Cloud Streaming Services

Console Guide

Product Documentation

Contents

Console Guide
Console Overview

Last updated：2024-10-14 11:32:49

To help you quickly get started with the CSS console, this document will introduce some frequently used CSS services. They are grouped into four modules based on user needs: Basic Services, Scenario-Specific Services, Data Center, and CSS Toolkit.

Basic Services

This module provides basic services of CSS. If you only want to use basic live streaming services, this is the right module for you.

Feature	Description
Overview	You can view live streaming value-added features, their application scenarios, and functional characteristics. You can view relevant data such as billing bandwidth/traffic trends, live streaming real-time data, and concurrent connection numbers. You can switch billing modes or change the time granularity as needed.
Domain Management	Add and manage your own acceleration domains and configure CNAME for them. Generate live streaming URLs. You can call the created recording, transcoding, screencapture, time shifting, watermarking, moderation, and callback templates for live stream domain names. You can configure live streaming domains with authentication, HTTPS protocol, acceleration regions, bandwidth caps, delayed playback, IP blacklists and whitelists, HTTP response headers, origin server information, and more.
Stream Management	You can manage live streams, primary and backup streams, stream history, and disabled streams. You can also disable and resume live streams.
Resource Package Management	You can view the usage of traffic and transcoding packages. Support automatic renewal of traffic and transcoding packages when they expire or are used up.

Live +

Live+ gathers various value-added services of Cloud Streaming Services, including transcoding, watermarking, screencapture, moderation, standby streams, subtitling, and relay. If you need to use related services, you can make

relevant configurations in this module.

Feature	Description
Feature Configuration	We provide configuration template services for various features required in live streaming, such as watermarking, recording, transcoding, screencapture, time-shifting, adaptive bitrate, callbacks, and DRM management. To reduce the complexity of page navigation, we have added a new process for binding templates to domain names.
LEB	Describes the product features of LEB and the steps for access guidance. LEB can be assessed in three steps and is smoothly compatible with LVB.
LVC	Online broadcasting can be realized through the CSS console. It supports custom screen layout, audio-video synchronous switching, program list, and automated broadcasting. This feature eliminates the need for heavy hardware, allowing users to conveniently and quickly use broadcasting services.
Pull and Relay	We offer the ability to pull live video or on-demand files from third-party platforms and push them to Cloud Streaming Services. You can directly perform operations such as mixing, recording, and more on the audio and video content. This feature allows for easy cross-platform distribution and the capability to convert on-demand content to live streaming.

Data Center

Data analysis provides users with professional data analysis services. You can query the consumption of traffic/bandwidth, transcoding, watermarking, relaying, and screencapture within a specific time granularity. Additionally, it offers log analysis functionality, making it convenient for users to monitor resources and obtain useful data.

Feature	Description
Billing Usage Statistics	You can query the billing items, including the related data generated by push and pull stream traffic/bandwidth, recording, time-shifting, screencapture, transcoding, and relaying.
Operation Analysis	You can view live streaming playback data analysis, user distribution, and origin server back-to-origin data, among other information.
Stream Data Query	You can query the data details of a single video stream, such as push, playback, live streaming records, callback events, etc., and export the data to your local machine.
Errors	You can query abnormal events that occur during live streaming push.

Stream Interruption Records	You can query the records and reasons for live streaming push interruptions.
Log Analysis	You can perform real-time collection, washing, analysis, and retrieval of live streaming access logs to quickly locate access faults.
SDK Quality Monitoring	You can query the push data information of the live SDK for the past 3 days.

CSS Toolkit

The Live Toolbox mainly provides some auxiliary features for ensuring live streaming processes and the use and management of live SDKs.

Feature	Description
Web Push	Quickly experience the Web push feature, with input sources including camera capture, screen sharing, and local file collection. It also supports multi-stream mixing, enabling push testing in various scenarios.
Address Generator	Provide the necessary information to splice push/playback URLs.
Self-Diagnosis	Quickly diagnose common live streaming push/playback issues. The diagnostic results are for reference only.
MLVB SDK	In conjunction with the Live SDK, you can add and manage official licenses and bind related resource packages.

Overview

Last updated：2024-11-08 16:05:33

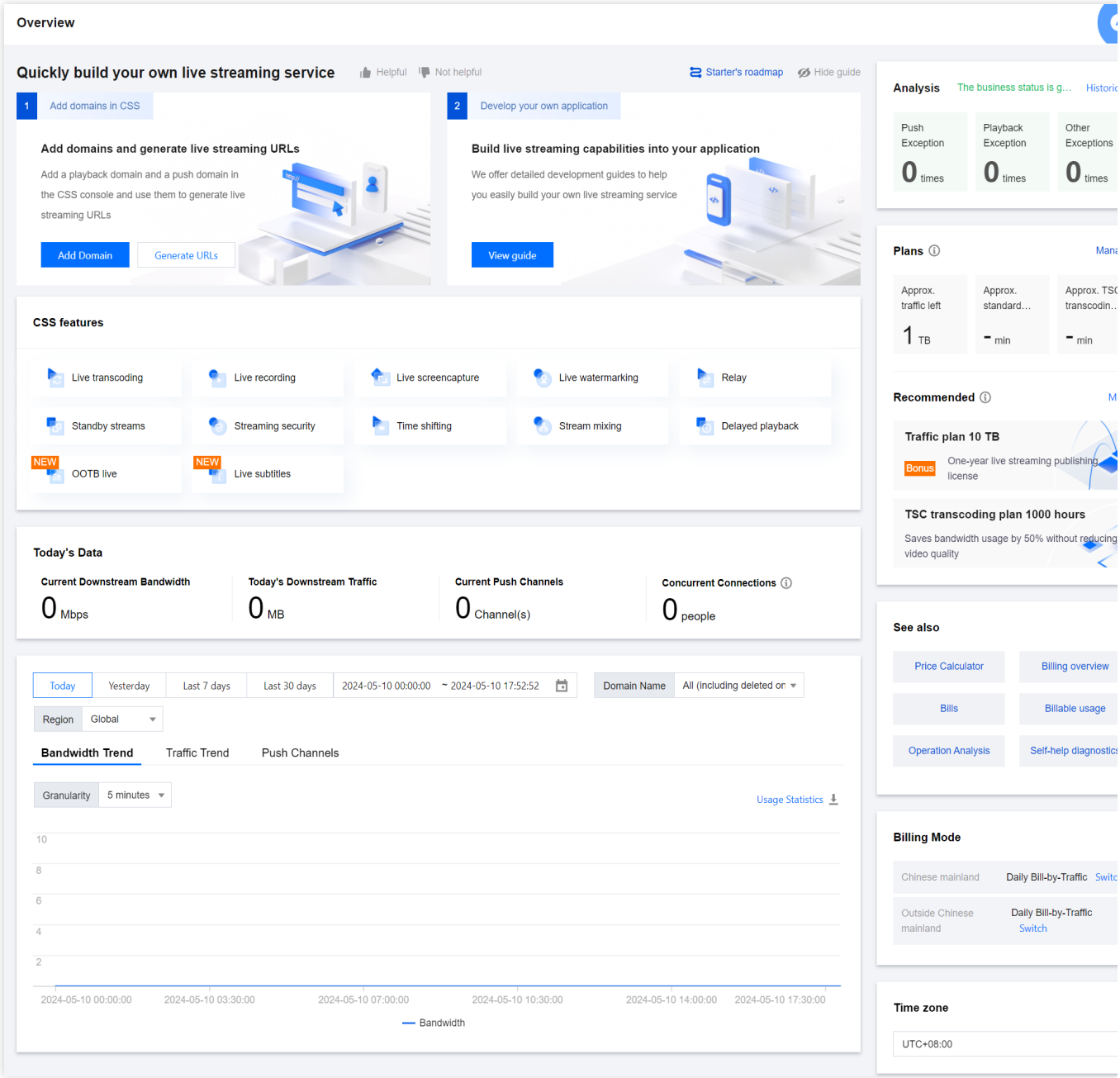
In the CSS console, you can manage domain name and streams, configure transcoding, recording, and acceleration, as well as push streams (web) and monitor resources.

Prerequisites

You have activated CSS.
You have logged in to the CSS console.

Overview

By clicking the Overview in the left sidebar, you can view relevant data, including real-time downstream bandwidth, today's downstream traffic, the current number of pushes, concurrent connections, and trends for billed bandwidth, billed traffic, and the number of pushes over the past 30 days. Additionally, you can view **Service Analysis** and **Plans** consumption details. You can switch **Billing Mode** or change the time granularity as needed. For beginner's guidance, you can click the **Guide** in the upper right corner to view instructions for getting started with CSS.



Today's Data

This section displays the downstream peak bandwidth, downstream traffic usage, the current number of push channels, and the number of concurrent connections of the day.

Item	Description
Current Downstream Bandwidth	The peak bandwidth consumed for acceleration by all playback domain names.
Today's Downstream Traffic	The total traffic consumed for acceleration by all playback domain names on the current day.

Current Push Channels	The number of current push channels.
Concurrent Connections	If the playback protocol is RTMP or FLV, **Concurrent Connections** indicates the number of online viewers. If the playback protocol is HLS, **Concurrent Connections** cannot be used as an indication of the number of online viewers.

Usage Trends

This section displays usage trends (**Bandwidth Trend**, **Traffic Trend**, and **Push Channels**) for today, yesterday, the last 7 days, and the last 30 days.

Item	Description
Bandwidth Trend	The sum of the peak bandwidth consumed for acceleration by all playback domain names in the query period.
Traffic Trend	The total traffic consumed for acceleration by all playback domain names in the query period.
Push Channels	The number of push channels under the selected domain names in the query period.

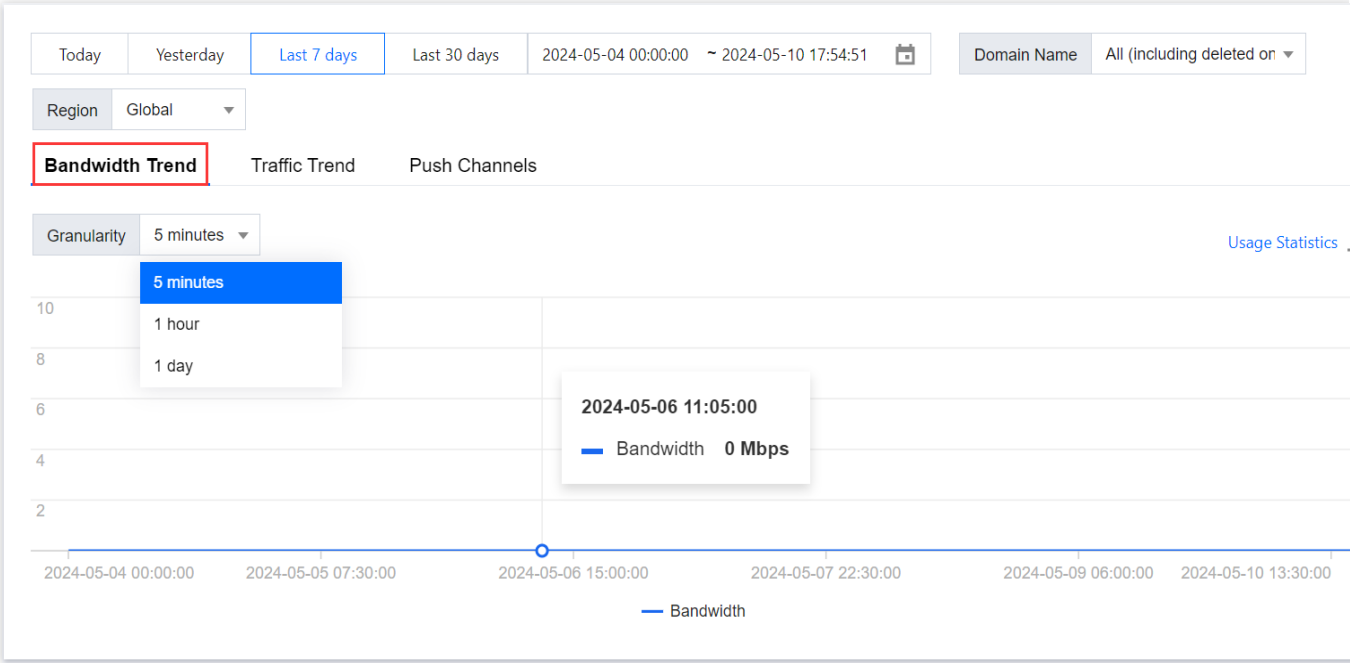
Changing the Granularity

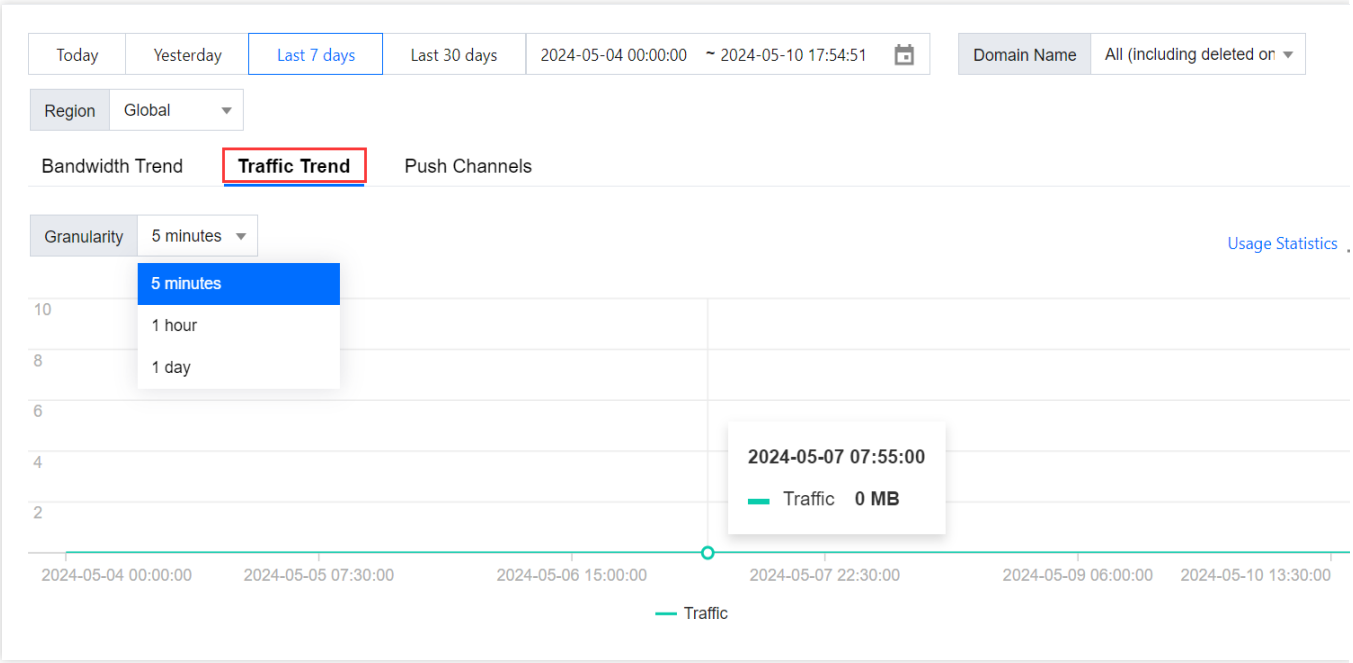
You can click the drop-down list box next to **Granularity** to change the granularity of the usage trend data.

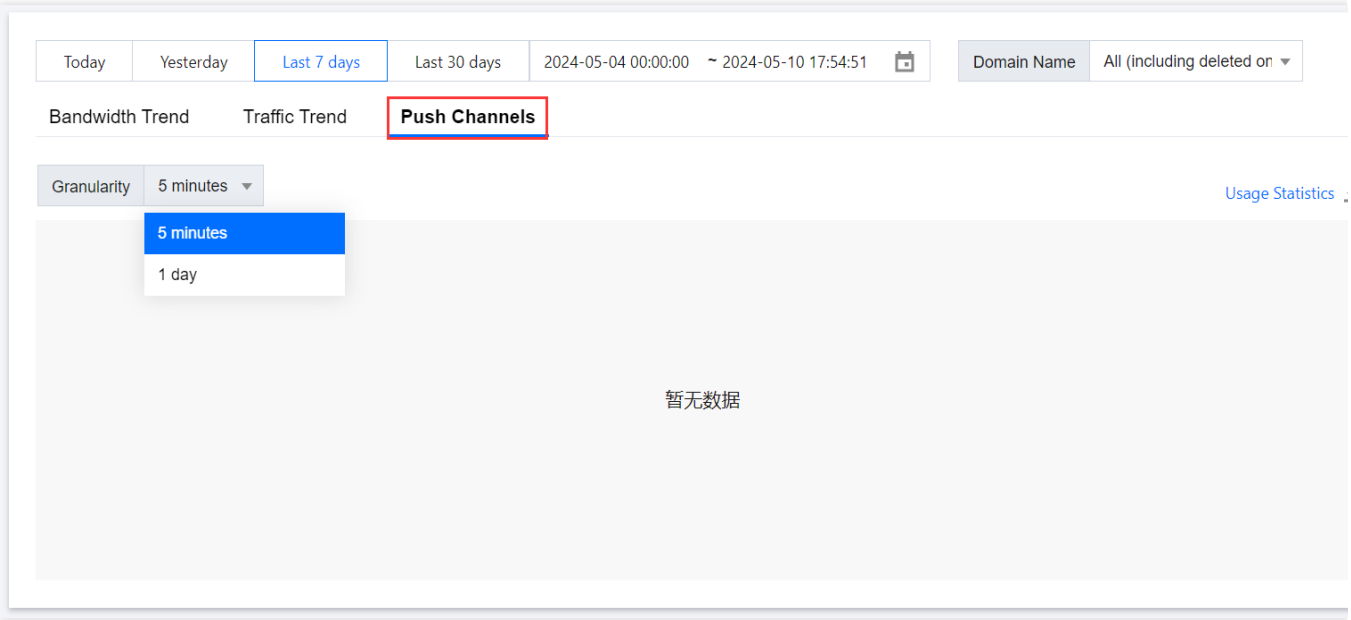
Bandwidth Trend

Traffic Trend

Push Channels


Today
Yesterday
Last 7 days
Last 30 days
2024-05-04 00:00:00 ~ 2024-05-10 17:54:51
Domain Name
All (including deleted on
Region
Global
Bandwidth Trend
Traffic Trend
Push Channels
Granularity
5 minutes
Usage Statistics
5 minutes
1 hour
1 day
10
8
6
4
2
2024-05-06 11:05:00
Bandwidth 0 Mbps
2024-05-04 00:00:00
2024-05-05 07:30:00
2024-05-06 15:00:00
2024-05-07 22:30:00
2024-05-09 06:00:00
2024-05-10 13:30:00
Bandwidth


Today
Yesterday
Last 7 days
Last 30 days
2024-05-04 00:00:00 ~ 2024-05-10 17:54:51
Domain Name
All (including deleted on
Region
Global
Bandwidth Trend
Traffic Trend
Push Channels
Granularity
5 minutes
Usage Statistics
5 minutes
1 hour
1 day
10
8
6
4
2
2024-05-07 07:55:00
Traffic 0 MB
2024-05-04 00:00:00
2024-05-05 07:30:00
2024-05-06 15:00:00
2024-05-07 22:30:00
2024-05-09 06:00:00
2024-05-10 13:30:00
Traffic



Business Analysis

Note:

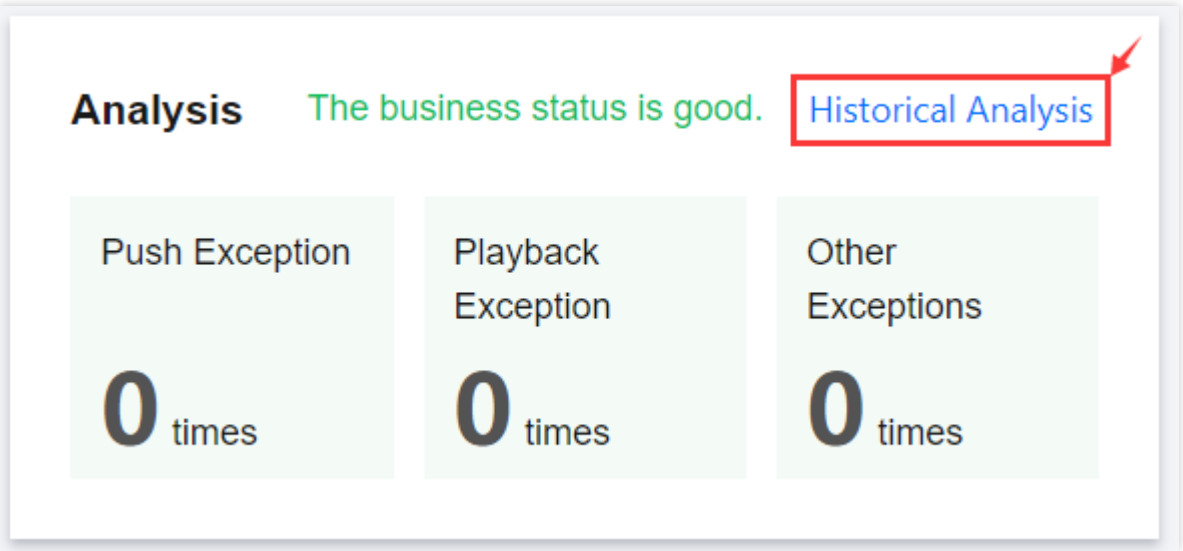
The real-time data statistics and reporting on the business analysis page may experience delay (about 1 hour).

Querying Business Analysis Data

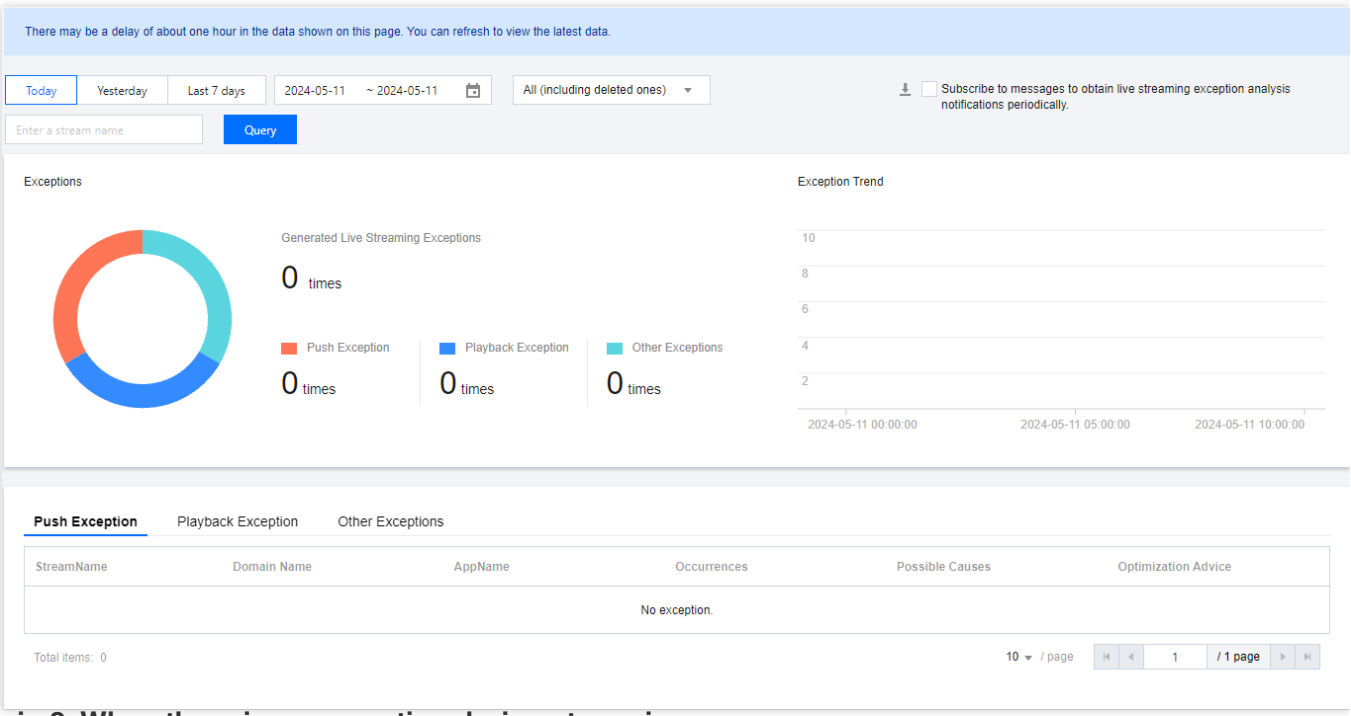
By default, the business analysis feature displays the current day's business usage data. It supports filtering by domain name and flow ID. Also, it supports querying data from the last 7 days.

Scenario 1: When the business status is good.

1.1 If the business condition is good, click **Historical Analysis** .

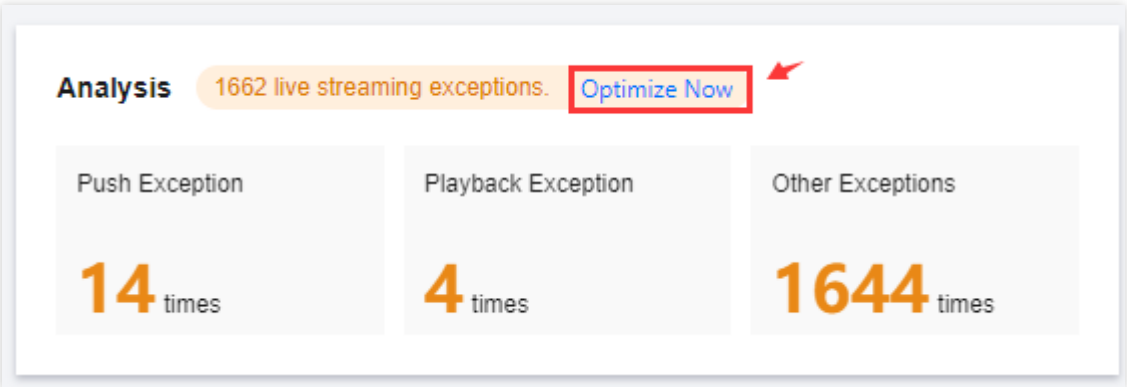


1.2 Navigate to the business analysis page to query relevant data.



Scenario 2: When there is an exception during streaming.

If there is an exception during streaming, click **Optimize Now** to enter the business analysis page.

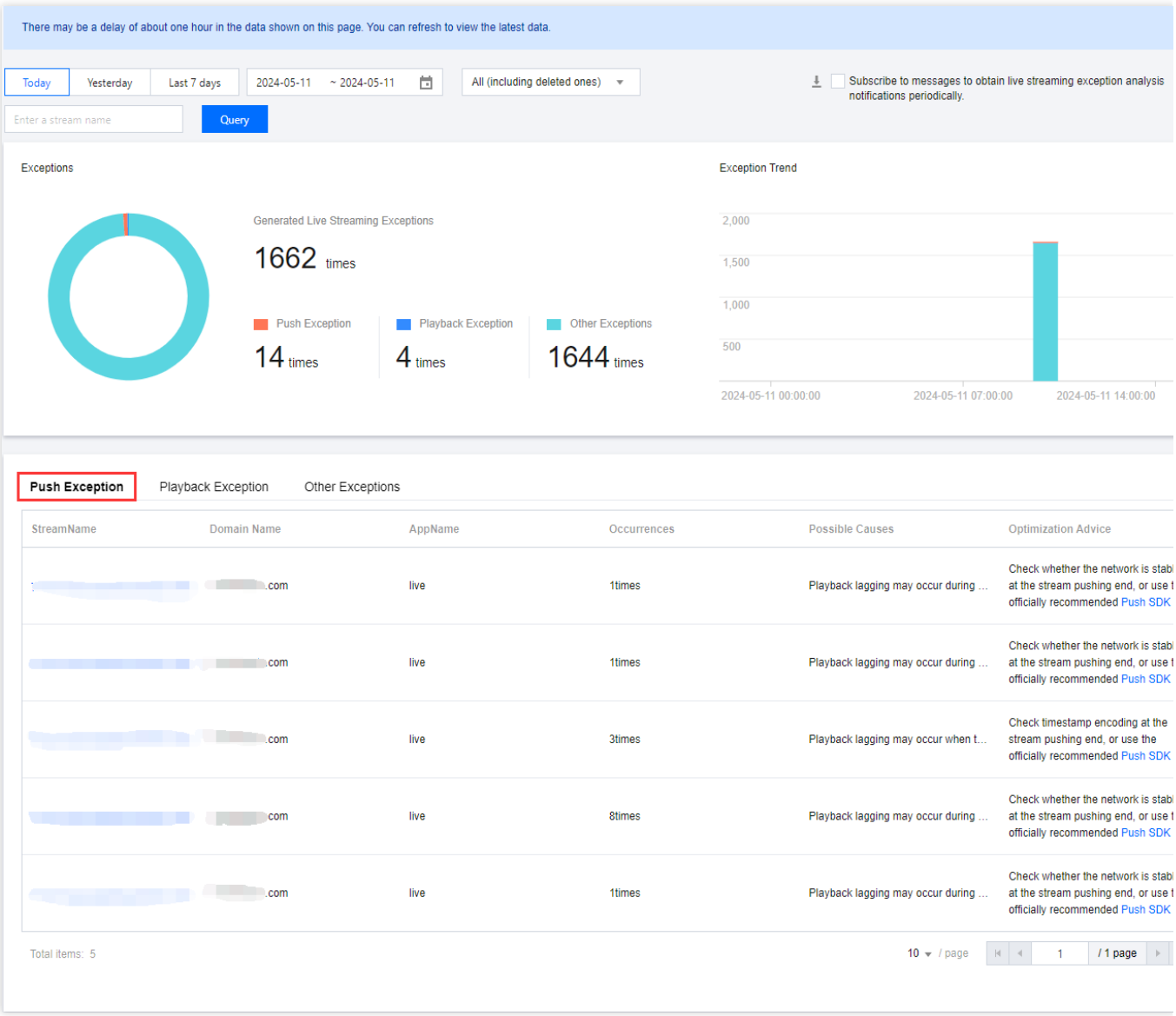


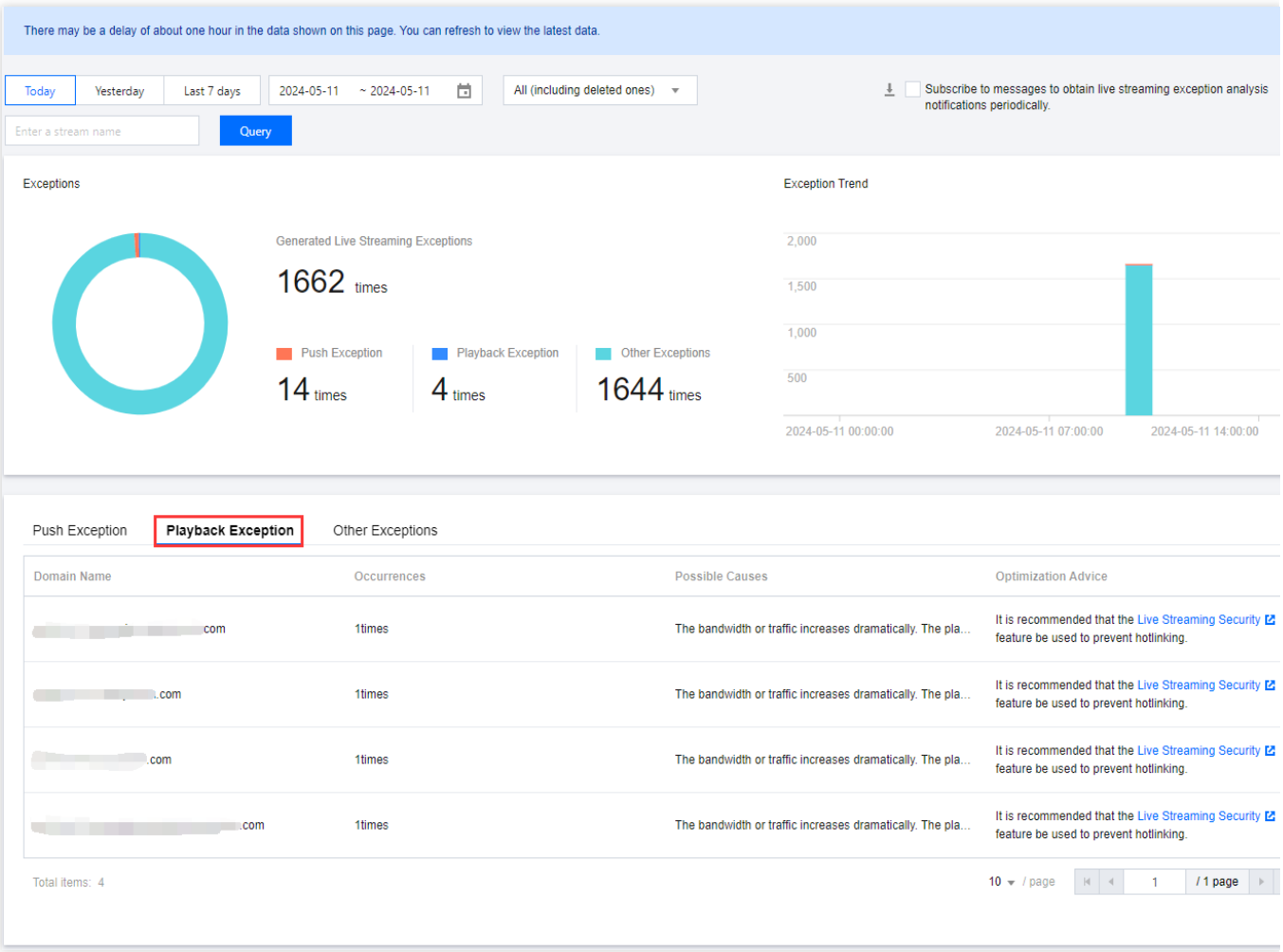
After entering the business analysis page, you can view information on the number of exceptions, exception trends, **Push Exception** , **Playback Exception** , and **Other Exceptions** . And understand the potential reasons for the exceptions and optimization suggestions.

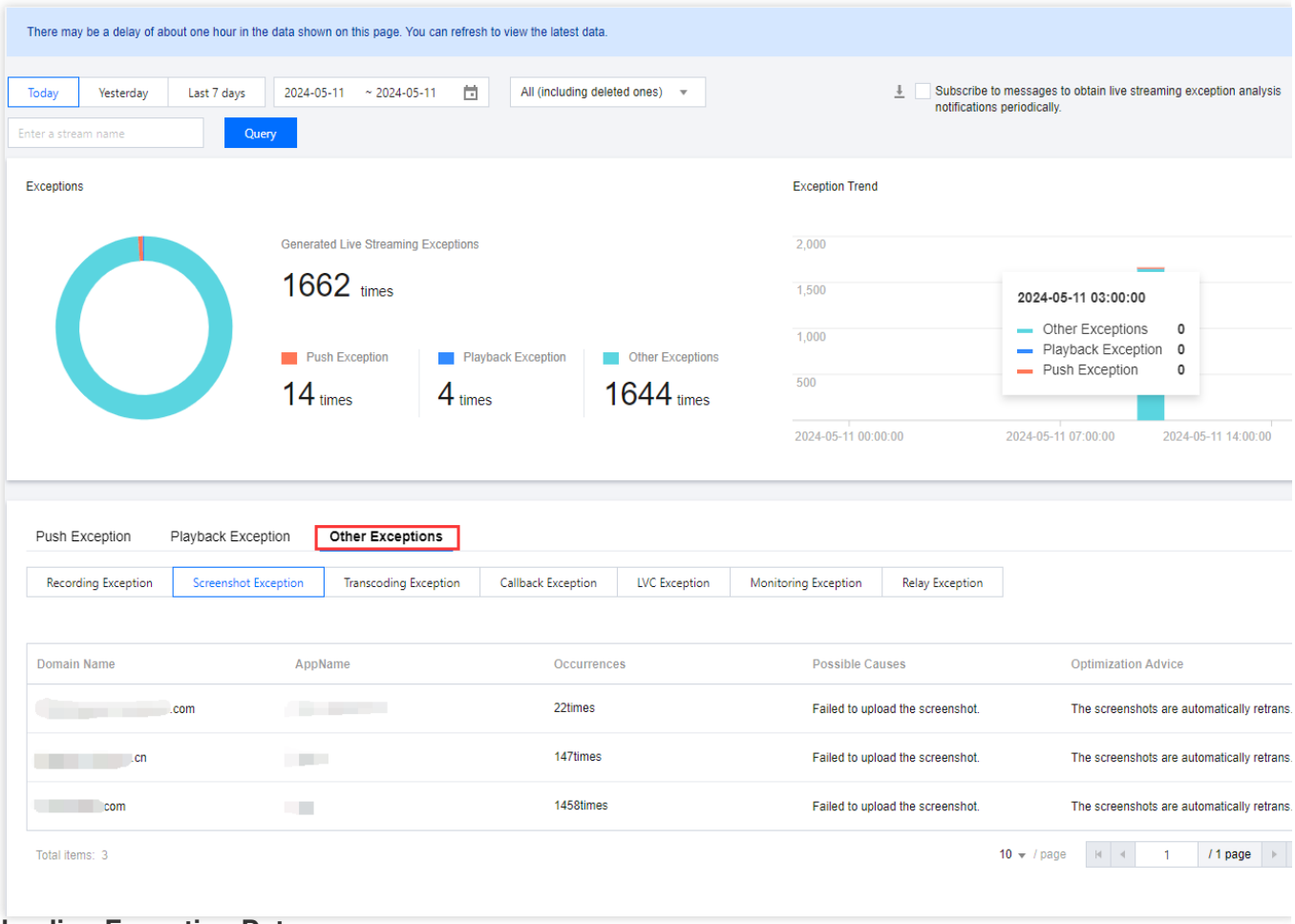
Push Exception

Playback Exception

Other Exceptions


There may be a delay of about one hour in the data shown on this page. You can refresh to view the latest data.
Today
Yesterday
Last 7 days
2024-05-11 ~ 2024-05-11
All (including deleted ones)
Subscribe to messages to obtain live streaming exception analysis notifications periodically.
Enter a stream name
Query
Exceptions
Generated Live Streaming Exceptions
1662 times
Push Exception
14 times
Playback Exception
4 times
Other Exceptions
1644 times
Exception Trend
2,000
1,500
1,000
500
2024-05-11 00:00:00
2024-05-11 07:00:00
2024-05-11 14:00:00
Push Exception
Playback Exception
Other Exceptions
StreamName
Domain Name
AppName
Occurrences
Possible Causes
Optimization Advice
.com
live
1times
Playback lagging may occur during ...
Check whether the network is stabl at the stream pushing end, or use t officially recommended Push SDK
.com
live
1times
Playback lagging may occur during ...
Check whether the network is stabl at the stream pushing end, or use t officially recommended Push SDK
.com
live
3times
Playback lagging may occur when t...
Check timestamp encoding at the stream pushing end, or use the officially recommended Push SDK
.com
live
8times
Playback lagging may occur during ...
Check whether the network is stabl at the stream pushing end, or use t officially recommended Push SDK
.com
live
1times
Playback lagging may occur during ...
Check whether the network is stabl at the stream pushing end, or use t officially recommended Push SDK
Total items: 5
10 / page
1
/ 1 page

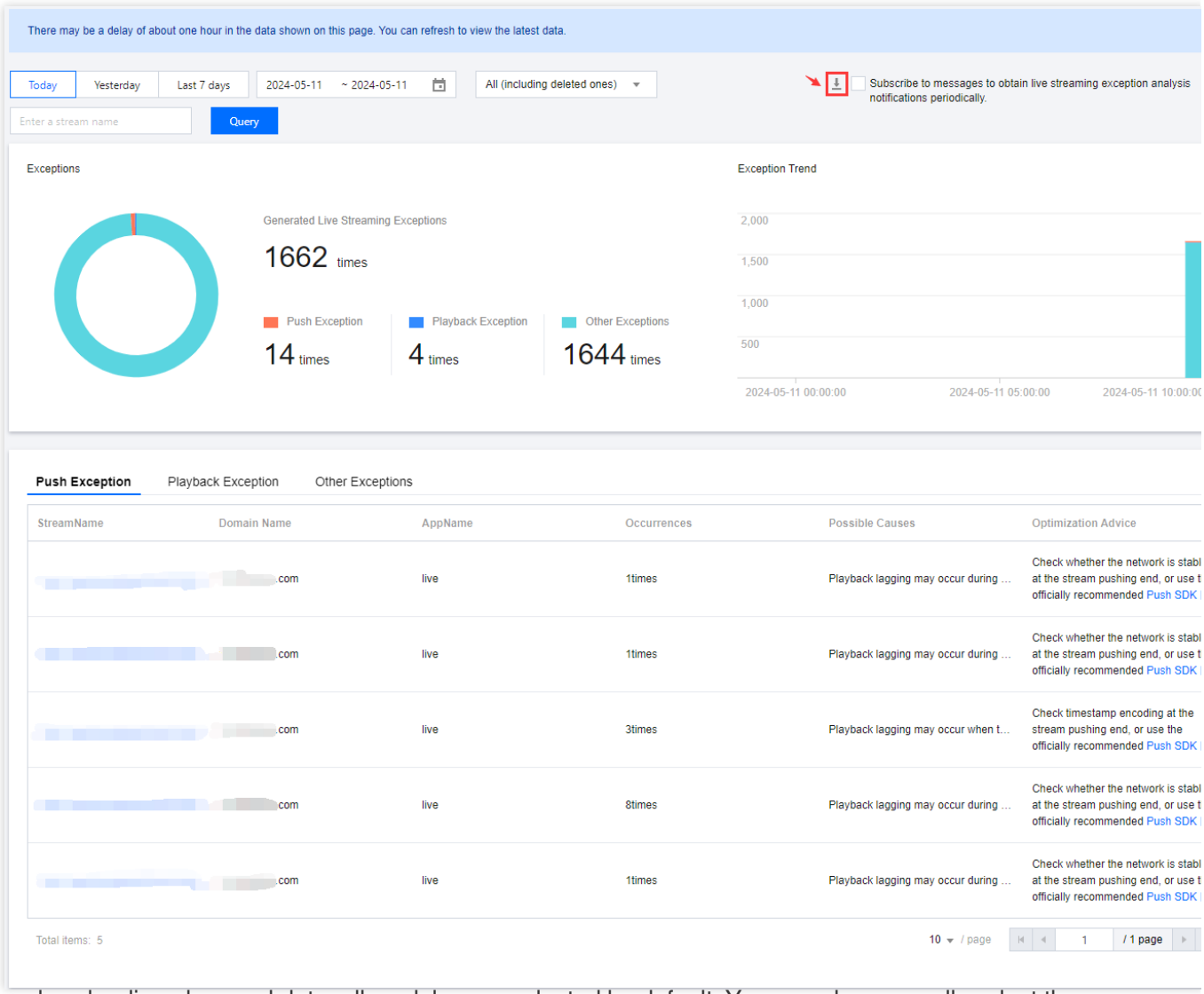

There may be a delay of about one hour in the data shown on this page. You can refresh to view the latest data.
Today
Yesterday
Last 7 days
2024-05-11 ~ 2024-05-11
All (including deleted ones)
Subscribe to messages to obtain live streaming exception analysis notifications periodically.
Enter a stream name
Query
Exceptions
Generated Live Streaming Exceptions
1662 times
Push Exception
14 times
Playback Exception
4 times
Other Exceptions
1644 times
Exception Trend
2,000
1,500
1,000
500
2024-05-11 00:00:00
2024-05-11 07:00:00
2024-05-11 14:00:00
Push Exception
Playback Exception
Other Exceptions
Domain Name
Occurrences
Possible Causes
Optimization Advice
1times
The bandwidth or traffic increases dramatically. The pla...
It is recommended that the Live Streaming Security feature be used to prevent hotlinking.
Total items: 4
10 / page
1
/ 1 page



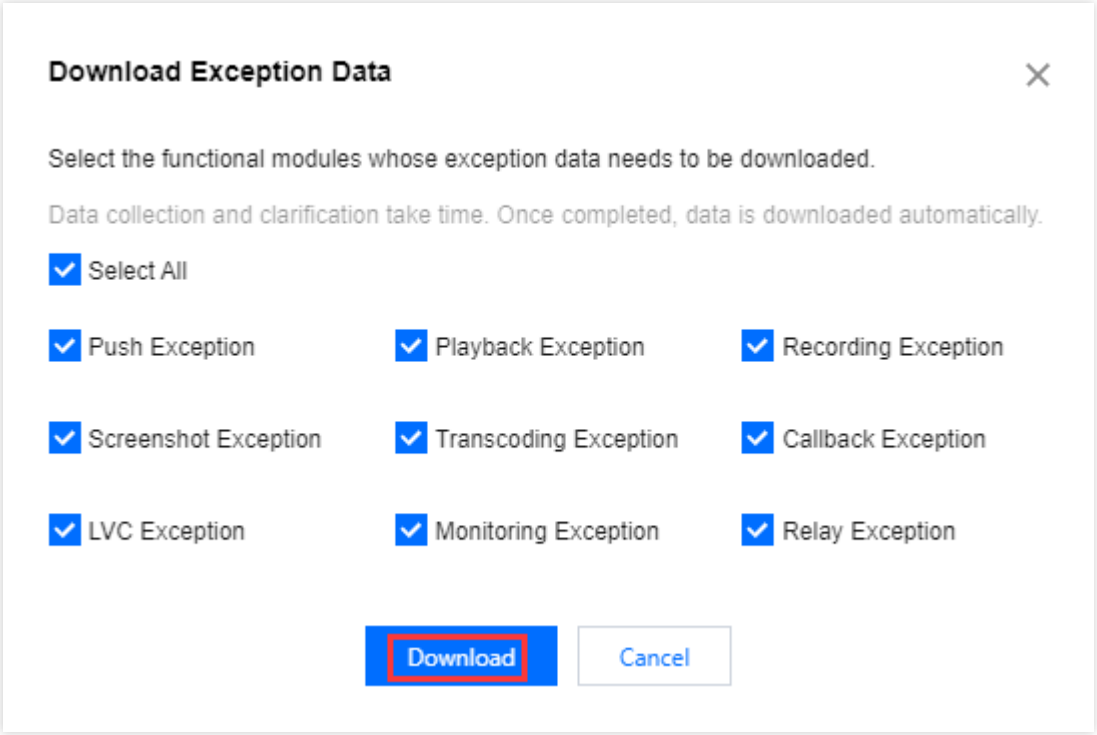
Downloading Exception Data

1. Based on your actual business needs, you can click

to download the business analysis report. This PDF document contains the streaming exception result information detected within the last 7 days. You can review and analyze it.

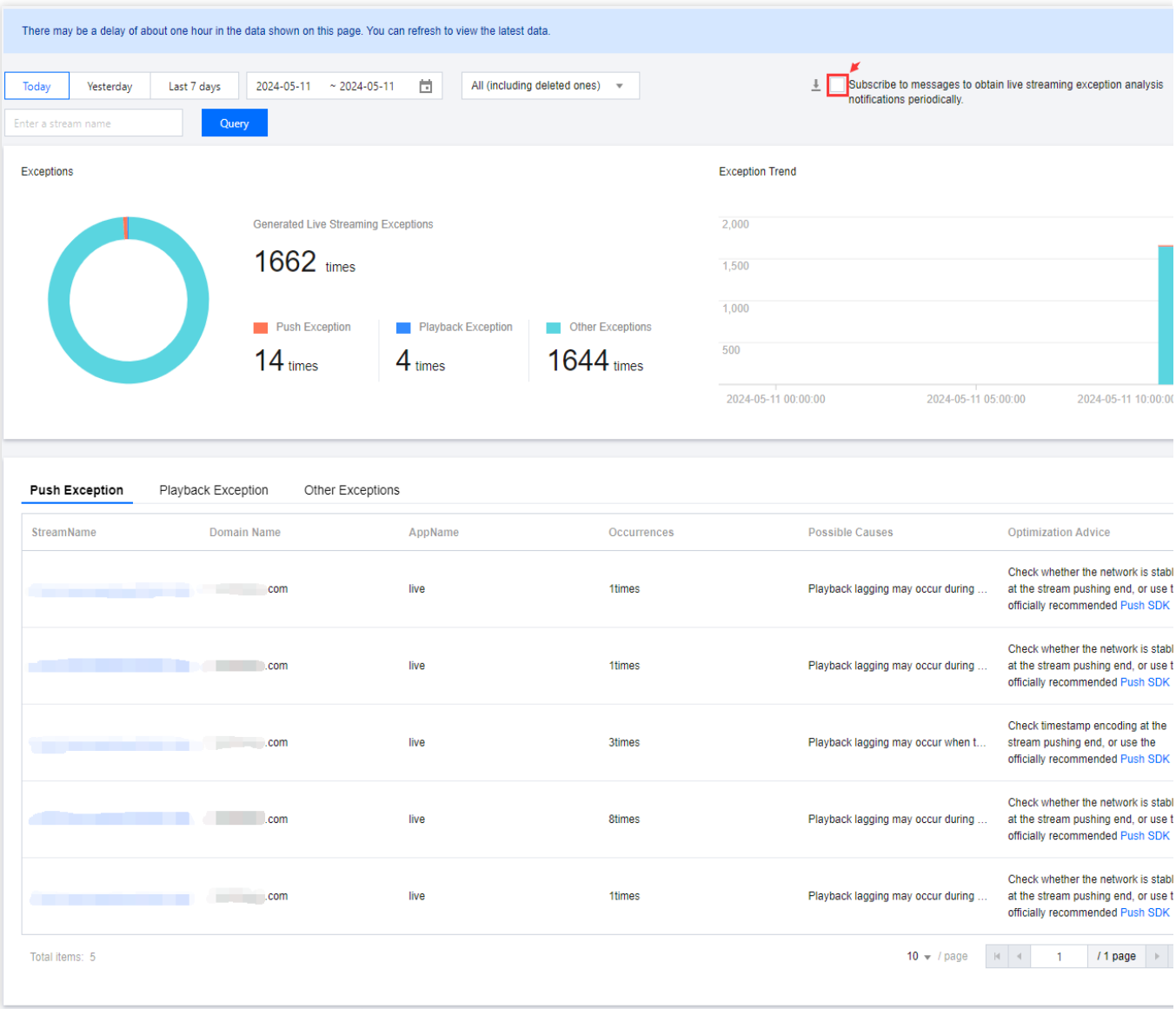


2. When downloading abnormal data, all modules are selected by default. You can also manually select the necessary modules.

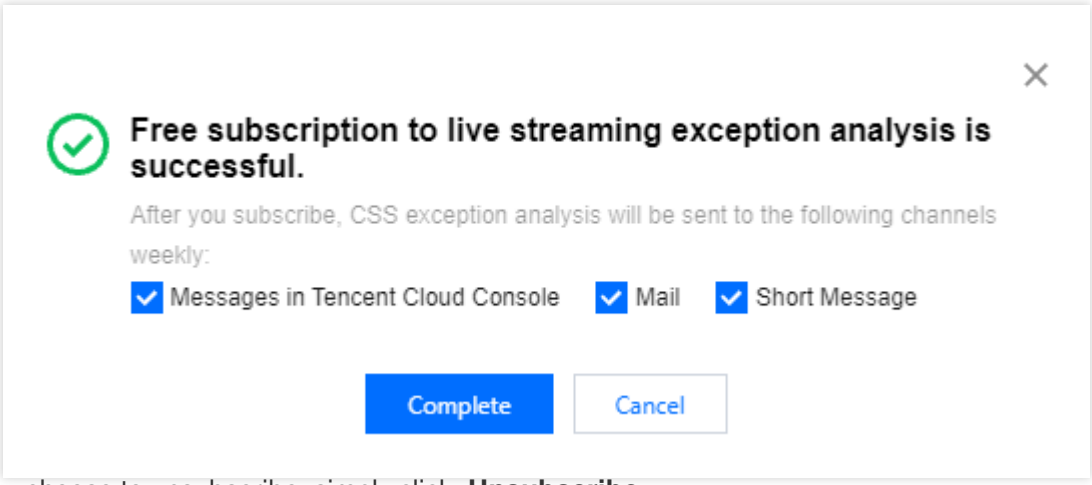


Streaming Exception Analysis Free Subscription

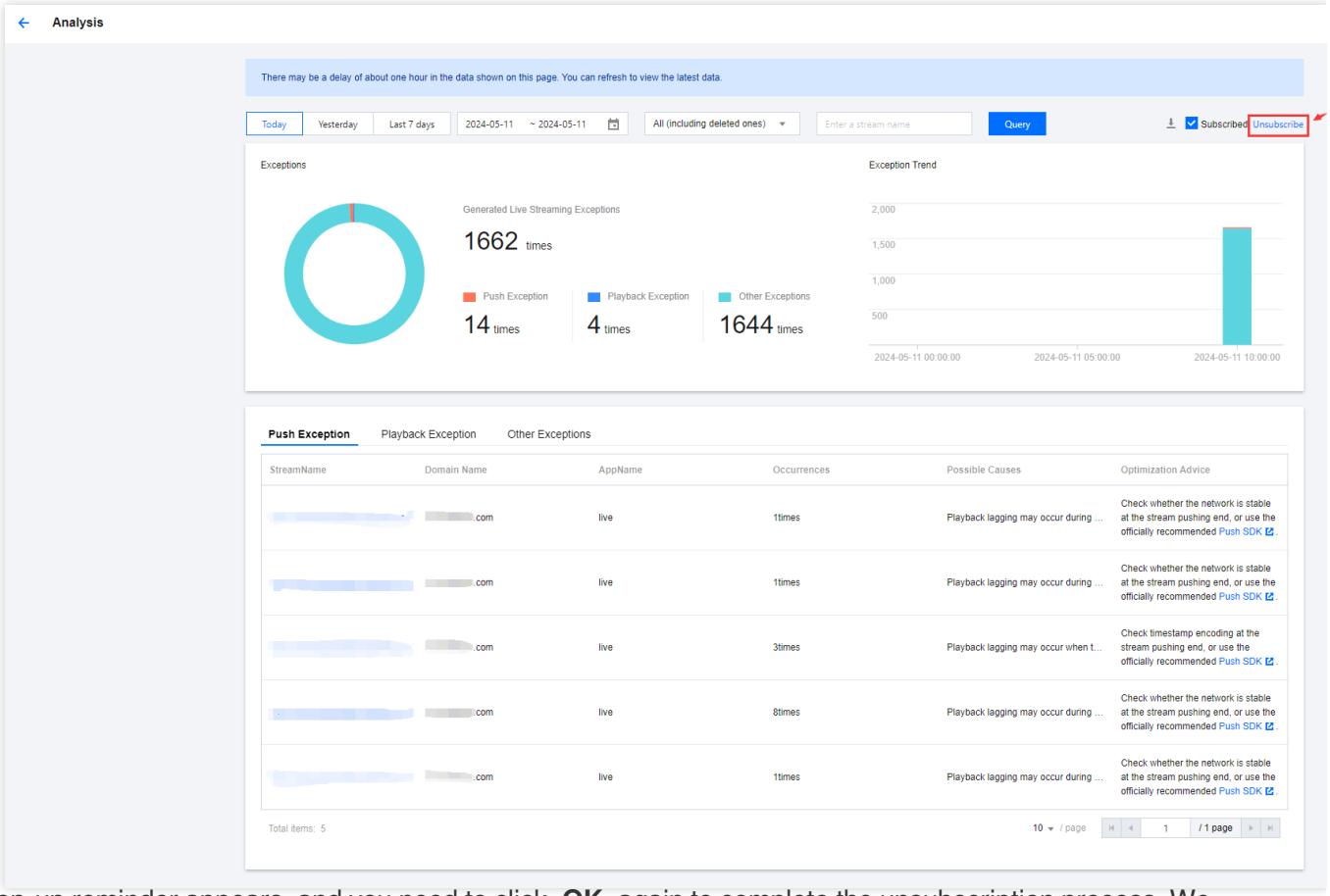
1. We offer a message subscription service. Based on your actual business needs, simply check the subscription option to regularly receive streaming exception analysis notifications.



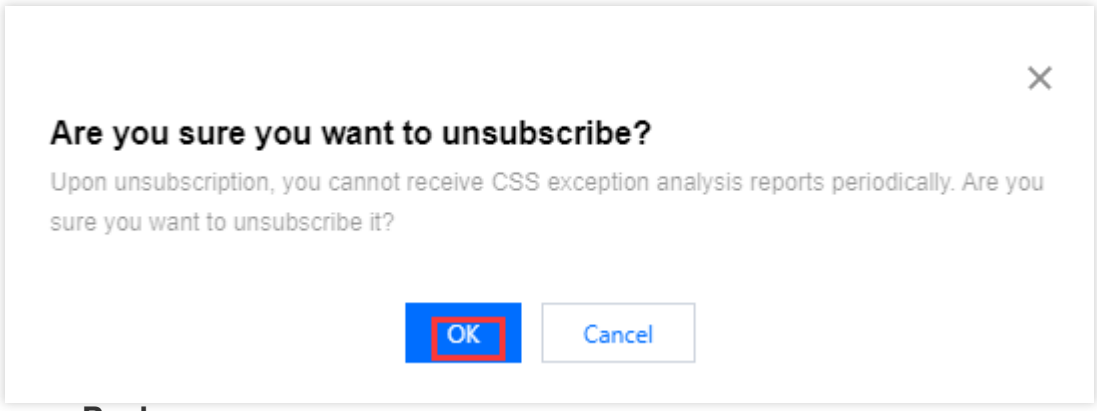
2. Once subscribed, we will send your CSS business exception analysis to the following channels on a weekly basis: message center, email, and SMS.



3. If you choose to unsubscribe, simply click **Unsubscribe** .



4. A pop-up reminder appears, and you need to click **OK** again to complete the unsubscription process. We recommend keeping your subscription active to regularly receive streaming exception analysis notifications.



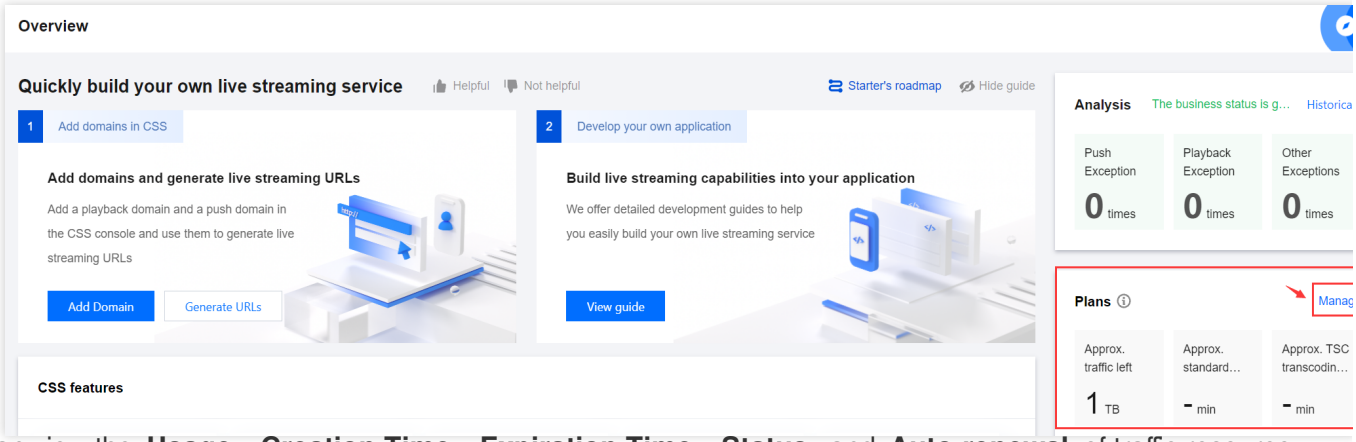
Resource Package

Note:

The remaining amount of resource packages displayed on the overview page is not real-time data. The update time coincides with the settlement time of the account statement.

Viewing Resource Package Consumption Details

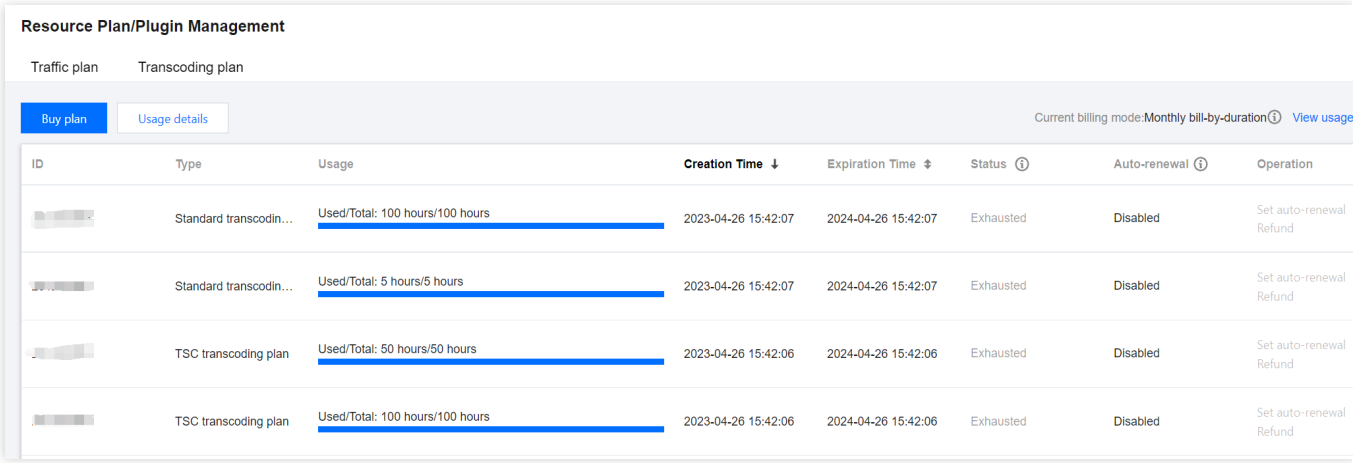
Click **Manage** on the right to enter the Resource Package/Plugin Management page.



You can view the **Usage** , **Creation Time** , **Expiration Time** , **Status** , and **Auto-renewal** of traffic resource packages/transcoding resource packages.

Auto-renewal (renew automatically when it is exhausted or expired) is supported for streaming traffic resource packages and streaming transcoding resource packages (including standard transcoding and top speed codec transcoding). For details, see Renewal documentation.

Purchasing Traffic Resource Package: Click Buy under the traffic package statistics, and you will enter the CSS Traffic Resource Package Purchase Page to purchase related packages.



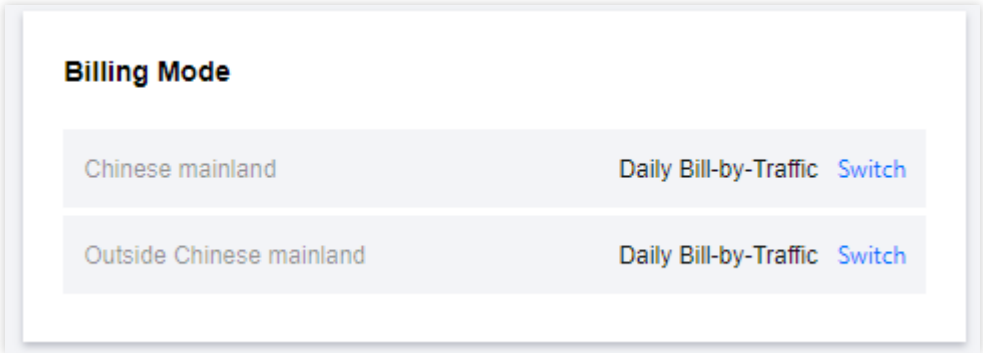
Note:

For information on billing prices, see Billing Overview.

Billing

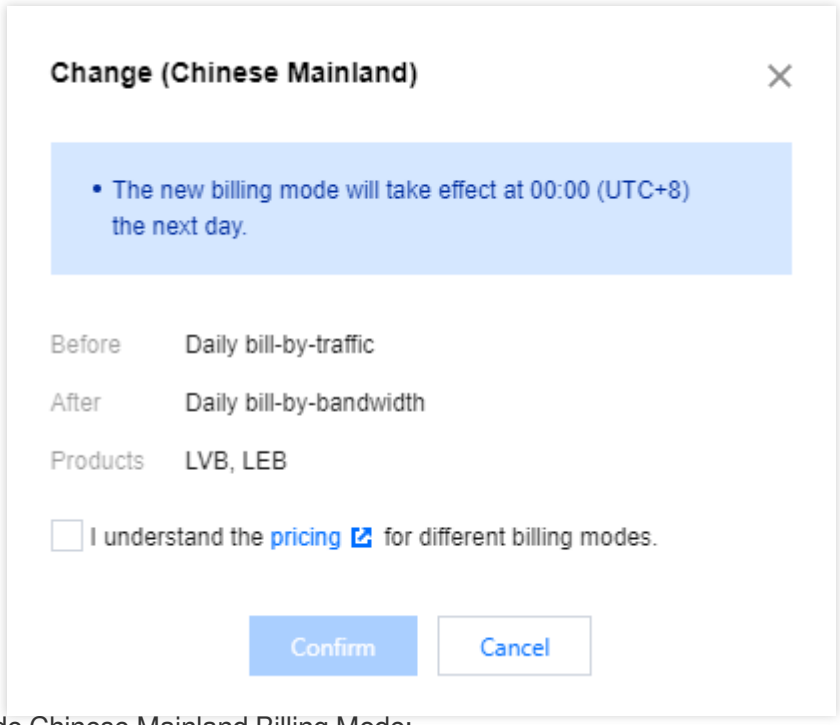
Switching Billing Mode

Based on your actual business needs, if your current billing mode is daily bill-by-traffic or daily bill-by-bandwidth, you can click **Switch** to change the billing mode.

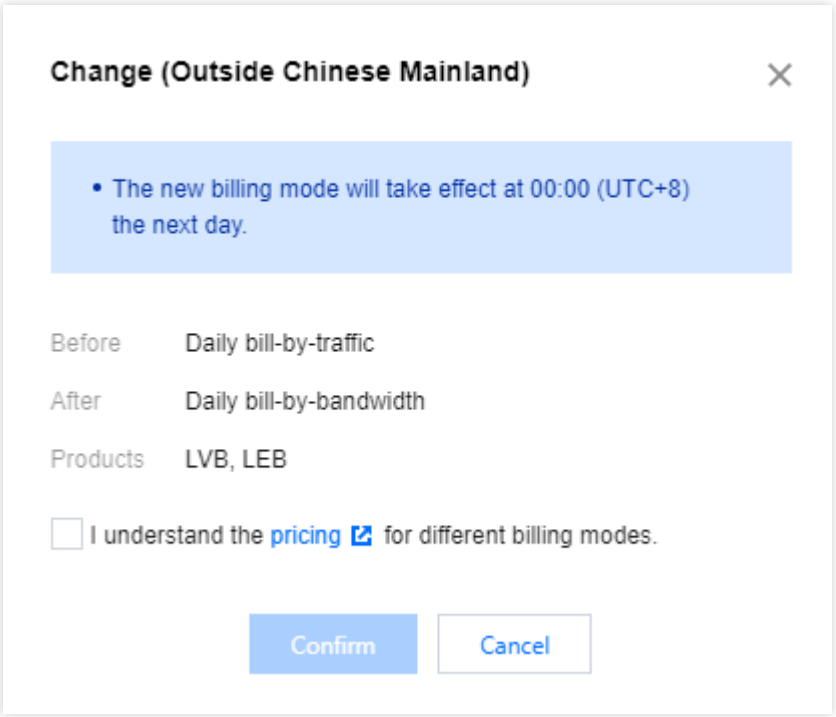


To view billing switch reminders, click **Confirm** to complete the switch of billing mode. For more detailed information on billing changes, see Changing Billing Modes.

Chinese Mainland Billing Mode:



Outside Chinese Mainland Billing Mode:


Change (Outside Chinese Mainland)
• The new billing mode will take effect at 00:00 (UTC+8) the next day.
Before
Daily bill-by-traffic
After
Daily bill-by-bandwidth
Products
LVB, LEB
I understand the pricing for different billing modes.
Confirm
Cancel

Domain Management
Adding Domain Names
Adding Your Own Domain

Last updated：2025-04-10 17:24:47

To use the CSS Service, at least two domain names are needed: one as the push domain name and one as the playback domain name. The push domain name and the playback domain name cannot be the same. However, they can be distinguished by second-level domain names, not limited to two subdomains. For example, `a.example.com` can be used as the push domain name and `b.example.com` can be used as the playback domain name for push and pull services.

Prerequisites

You have activated CSS.

Adding Your Own Domain

1. Log in to the CSS console and select **Domain Management** on the left sidebar.
2. Click **Add Domain** and complete the following settings in the pop-up window:
2.1 If you need to add a **push domain**: Enter the domain name and select the domain type as **Push Domain**.
2.2 If you need to add a **playback domain**: Enter the domain name, select the domain type as **Playback Domain**, and choose the acceleration region, with the default being **Chinese mainland**.
2.3 Tags are used to classify and manage resources from different dimensions. If the existing tag does not meet your requirements, you can also go to the Tag Console for unified tag management.
2.4 Click on **Add domain**.

Note:
The domain name can be up to **45** characters long and cannot contain uppercase letters.
By default, you can add up to 100 domains under each Tencent Cloud account. If you you need to add more than 100 domains, please submit a ticket to raise the limit.
You can change the acceleration region of a domain added. On the **Domain Management** page, click the name of the domain or click **Manage** on the right. Select the **Advanced Configuration** tab, click **Edit** in the **Region configuration** area, select the acceleration region again in the pop-up window, and click **Save**.

Verifying Your Domain

To make sure that a domain can only be added by its owner, you need to verify your ownership of a domain before you can add it in the CSS console. For example, to add `a.test.com`, you need to verify your ownership of `test.com`. You don't need to verify again when adding domains with the same parent domain, such as `b.test.com`. You can verify a domain either by adding a DNS record or by uploading an HTML file. If a previously added domain is not verified, when you add a domain with the same parent domain, verification is still required.

DNS record

You can verify your ownership of a domain by adding a DNS record at your DNS provider. If you use Tencent Cloud's DNS service, follow the steps below to add a DNS record.

1. Log in to the DNSPod console.
2. Select **DNS** > **My Domains** on the left sidebar and click the parent domain of the domain you want to add.
3. On the **Record Management** page, click **Add Record**.
4. Enter the following information:

Parameter	Description
Host	Enter "cssauth".
Record Type	Select "TXT".
Record Value	CSS assigns a unique record value for each domain. You can view it in the CSS console when adding your domain.

5. Click **Confirm**. The TXT record will take effect in about five minutes.
6. Click **Verify and add domain**. If the verification succeeds, you can proceed to the next step.

HTML file

You can also verify your domain by uploading an HTML file.

1. When asked to verify your domain in the CSS console, select **HTML file**.
2. Download the file.
3. Upload the file to the root directory of the second-level domain.
4. Confirm that the file is accessible at `http://second-level domain/second-level domain_cssauth.html`.
5. Click **Verify and add domain**. If the verification succeeds, you can proceed to the next step.

Note:

After finishing the **Basic settings**, you can proceed to the **CNAME configuration** step. For more information about CNAME configuration, see Configuring CNAME for Domain Name.

Configuring CNAME

Last updated：2024-08-27 10:34:59

After the domain is connected to CSS, the system will automatically assign a CNAME domain for you (the CNAME suffix for the push domain is `.tlivepush.com` , and the CNAME suffix for the playback domain is `.txlivecdn.com`). which you can view in Domain Management. To make your domain accessible, you need to add a CNAME record at your DNS service provider. You can use CSS only after the configuration takes effect.

Notes

CNAME resolution is required for both playback and push domains.
For detailed directions on how to add a CNAME record, please consult your DNS service provider.
CNAME configuration generally takes effect in about 15 minutes. If you configure multiple levels of CNAMEs, CSS will be unable to track the resolution result. If your domain can be accessed, then the CNAME configuration is successful.
If CNAME configuration fails to take effect after a long time, refer to Domain Configuration to troubleshoot the issue.

Prerequisites

You have registered a domain.
You have verified the domain and added it in Domain Management of the CSS console. You haven't added a CNAME record for the domain (the icon in the **CNAME** column is

).

Directions

This document explains how to set up CNAME DNS with non-Tencent Cloud providers. The method is for reference only, and if it doesn't match the actual configuration, follow the information from your DNS service provider. After setting up the CNAME for your domain name, you can verify whether the CNAME has been successfully configured for your domain name by using the method described in Verify Whether the CNAME is Effective .

Non-Tencent Cloud Configuration Method

The general steps for setting up CNAME DNS with non-Tencent Cloud providers are as follows:
1. Log in to your DNS service provider's management console.

2. Find the domain name management or DNS management feature and go to the DNS settings page for the domain name where you need to configure the CNAME.
3. Add a new DNS record. Select the record type as `CNAME` .
4. Set the host record, DNS route, record value, and other relevant parameters.
5. Save the DNS record.

When setting a CNAME record, usually the following parameters need to be considered:

Record type: Select `CNAME` .

Host record: Enter the subdomain name or domain name prefix. If the playback domain name is `play.myqcloud.com` , then add `play` ; if you need to directly resolve the primary domain name `myqloud.com` , then enter `@` ; if you need to resolve a wildcard domain name, then enter `\\*` .

DNS route: It is recommended to select the " `Default` " type to adapt to different network environments.

Record value: (Enter the target domain name you want to point the subdomain name to) The CNAME value of the corresponding domain name on the domain name management page of the CSS console, formatted as `domain.txlivecdn.com` .

TTL: Set the DNS cache time. The smaller the value is, the faster the record changes take effect globally. Generally, you can use the default value or set a short time, such as 600 (10 minutes).

Note:

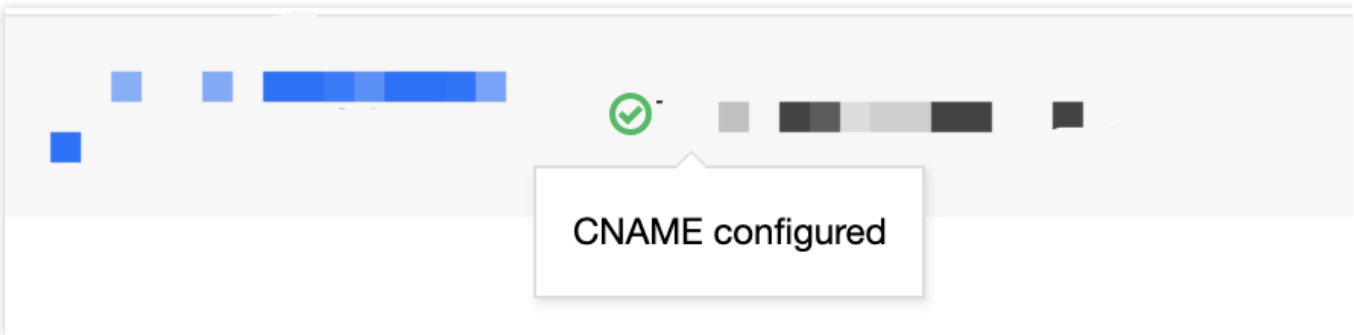
The above method is for reference only for non-Tencent Cloud providers. See the documentation and guidelines provided by your DNS service provider for the actual configuration.

Verifying CNAME Records

A new CNAME record generally takes effect within 30 minutes. The exact time needed varies with provider. You can check whether a record has taken effect using the following methods.

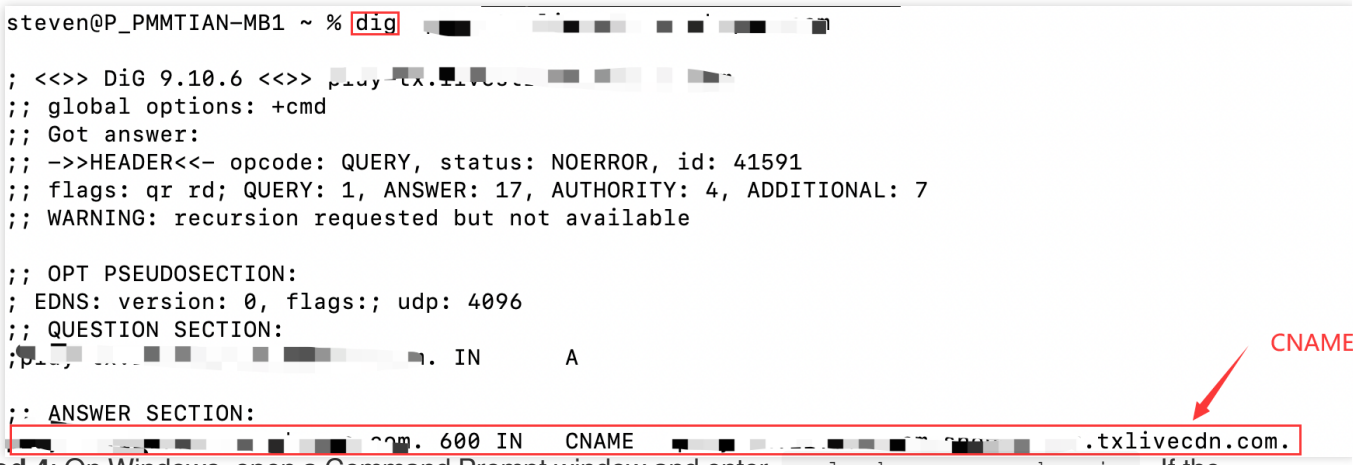
Method 1: Go to Domain Management of the CSS console. If the icon in the **CNAME** column is

, CNAME configuration is successful.



Method 2: When you add your domain in the CSS console, after completing the basic settings, in the **CNAME configuration** step, you can view the CNAME status of the domain.

Method 3: On Linux/macOS, run the `dig` command (`dig your domain`). If the first row displays the destination domain provided by CSS, CNAME configuration is successful.



Method 4: On Windows, open a Command Prompt window and enter `nslookup your domain` . If the destination domain name provided by CSS is displayed, CNAME configuration is successful.

Note:

If CNAME configuration fails to take effect after a long time, refer to Domain Configuration to troubleshoot the issue.

Managing Domain Names

Last updated：2025-03-28 17:49:52

On the Domain Management page of the Cloud Streaming Services (CSS) console, you can perform a series of operations on your domain names according to your business needs, including enabling, disabling, and deleting the domain names.

Disabling a Domain Name

If you do not want to use a live streaming domain name temporarily, you can disable it. Here are the steps to disable a domain name:

Note:

After a live streaming domain name is disabled, the domain name information will still be retained in the system, but the live streaming services will no longer process requests for the domain name. This means users will no longer be able to initiate live streaming push and playback through the domain name. Additionally, ongoing streaming or playback will not be interrupted.

1. Log in to theCSS console and select **Domain Management**. In the domain name list, find the domain name you want to disable and click **Disable**.

2. In the pop-up window, click **Confirm** to disable the live streaming domain name.

3. In the Status column on the Domain Management page, you can see that the current status of the domain name has changed to **Disabled**. The domain name has been successfully disabled and cannot be used for live streaming push and playback.

Enabling a Domain Name

If you need to re-enable a disabled domain name, follow these steps:

1. Log in to the CSS console and select **Domain Management**. In the domain name list, find the domain name you want to re-enable and click **Enable**. Live streaming services will be resumed for the domain name.

2. In the Status column on the Domain Management page, you can see that the current status of the domain name has changed to **Enabled**. You can use this domain name again for live streaming push and playback.

Deleting a Domain Name

Note:

Deletion is irreversible. When you delete a domain name, all its configurations will be permanently deleted.

You can still view the usage data of deleted domain names.

If you need to delete a domain name, follow these steps:

1. Log in to the CSS console and select **Domain Management**. In the domain name list, find the domain name you want to delete and click **Delete**.

2. In the pop-up window, click **Confirm** to delete the domain name from your CSS console.

Push Domain Name Management
Push Configuration

Last updated：2024-10-10 17:28:28

To protect your live streaming content, push authentication is enabled for push domains by default. You can use the address generator on the details page of a push domain to generate a push URL, which you can use to push streams (upload live videos) to the CSS platform.

Must-Knows

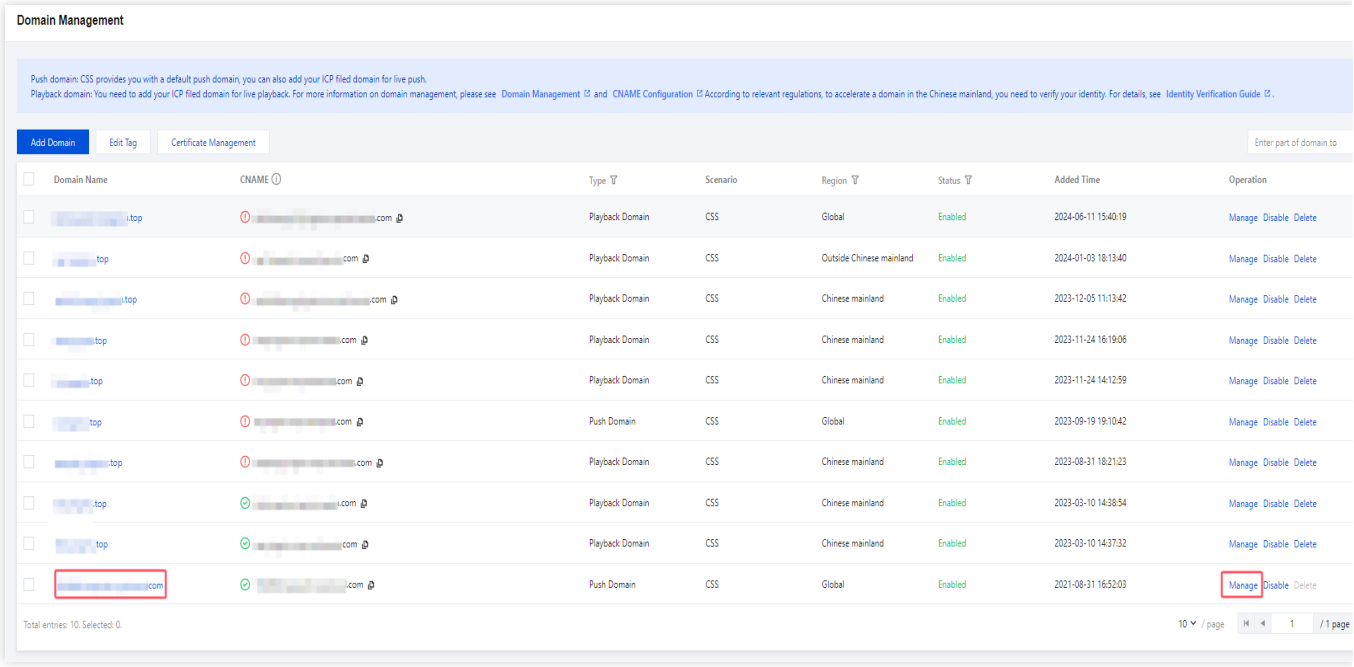
CSS provides a test domain name `xxxx.tlivepush.com` . You can use it to push streams for test purposes, but the test domain should not be used in production environments.
A push URL is valid before the expiration time you specify. After it expires, you need to generate a new URL.

Prerequisites

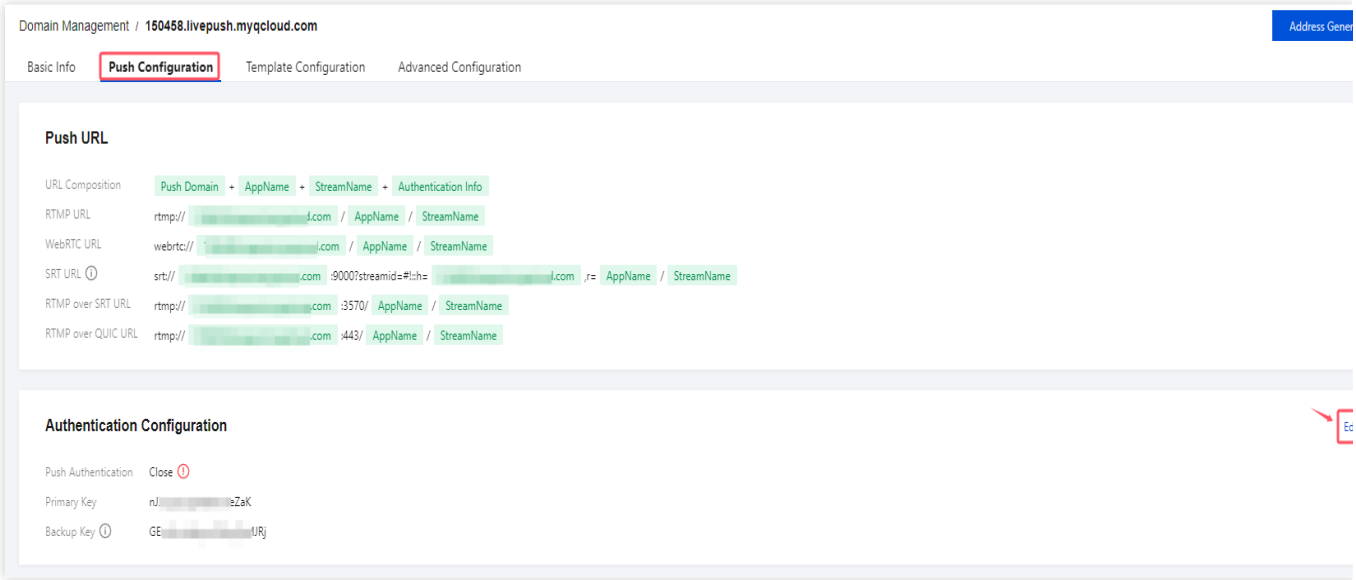
You have activated CSS.

Authentication Configuration

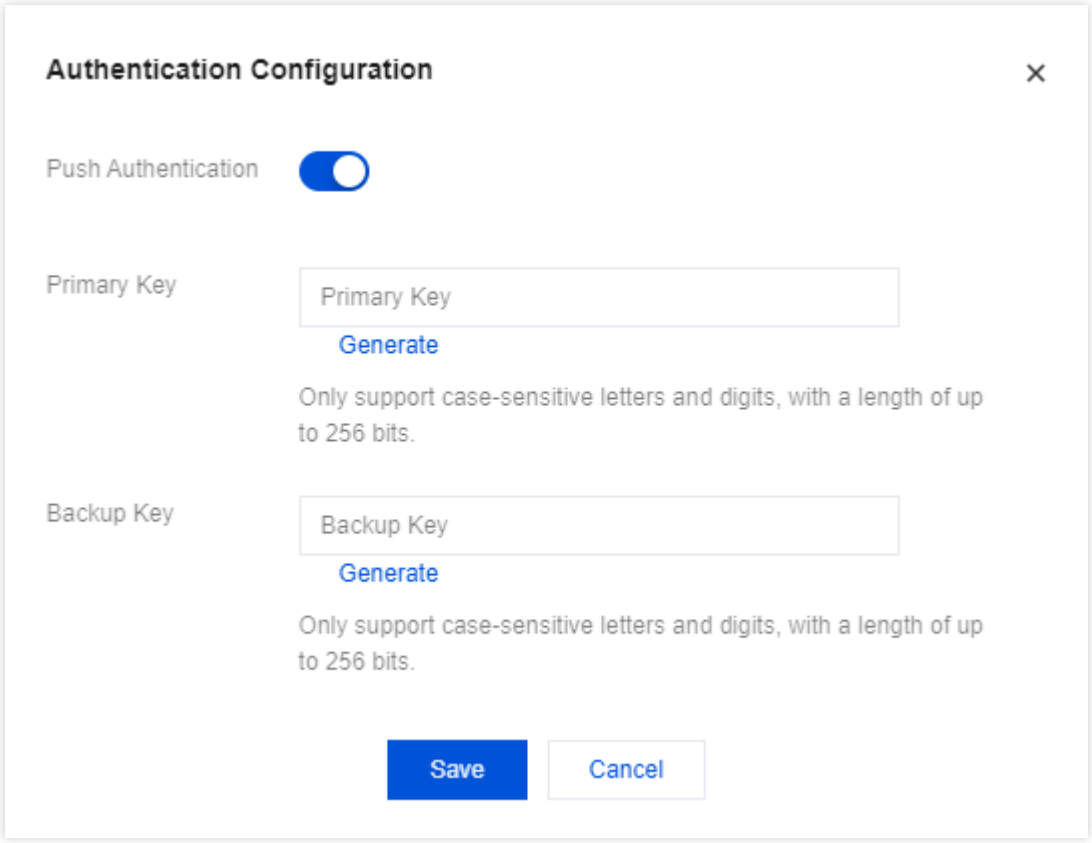
1. Go to Domain Management, click the target **push domain name** or click **Manage** to enter the domain details page.



2. Click **Push Configuration** and, in the **Authentication Configuration** area, click **Edit**.



3. In the pop-up window, toggle on **Push Authentication**.
4. Enter the primary key and backup key, and click **Save**.



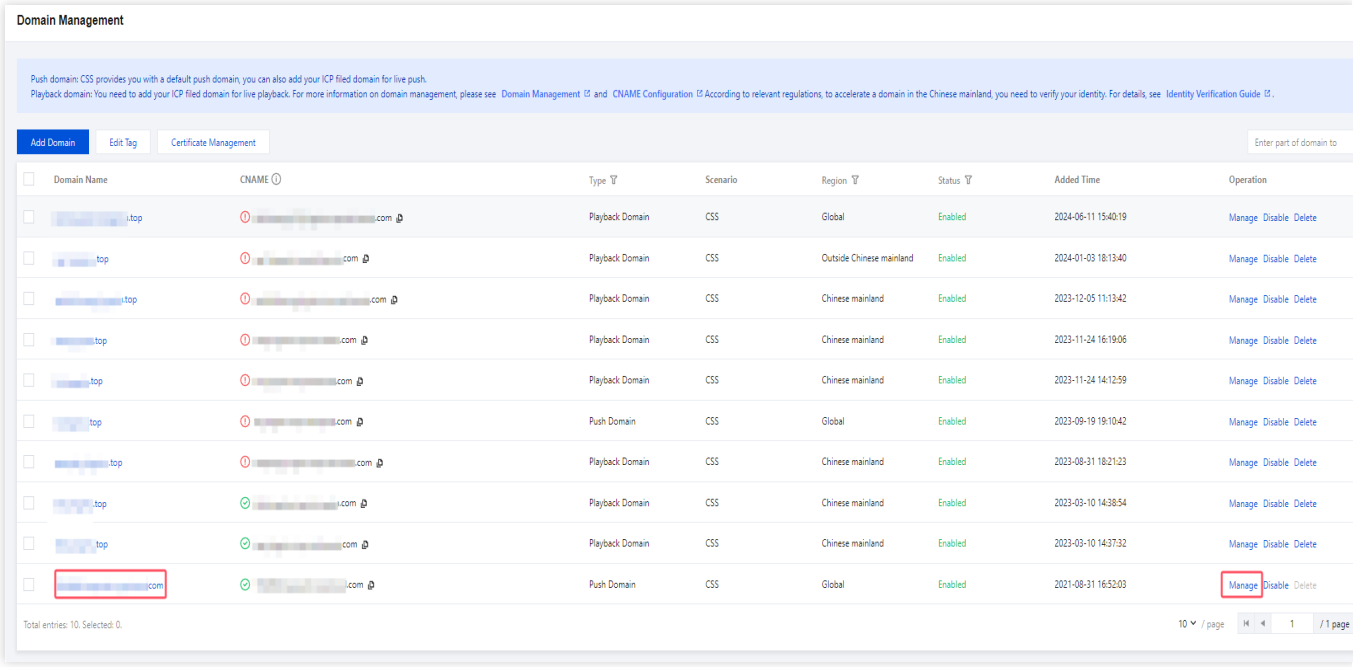
Note:

The primary key is required and the backup key is optional. Entering both allows you to switch to the other key when one key is disclosed.

Push Address Generator

Directions

1. Go to Domain Management, click the target domain name or click **Manage** on its right to enter the details page.



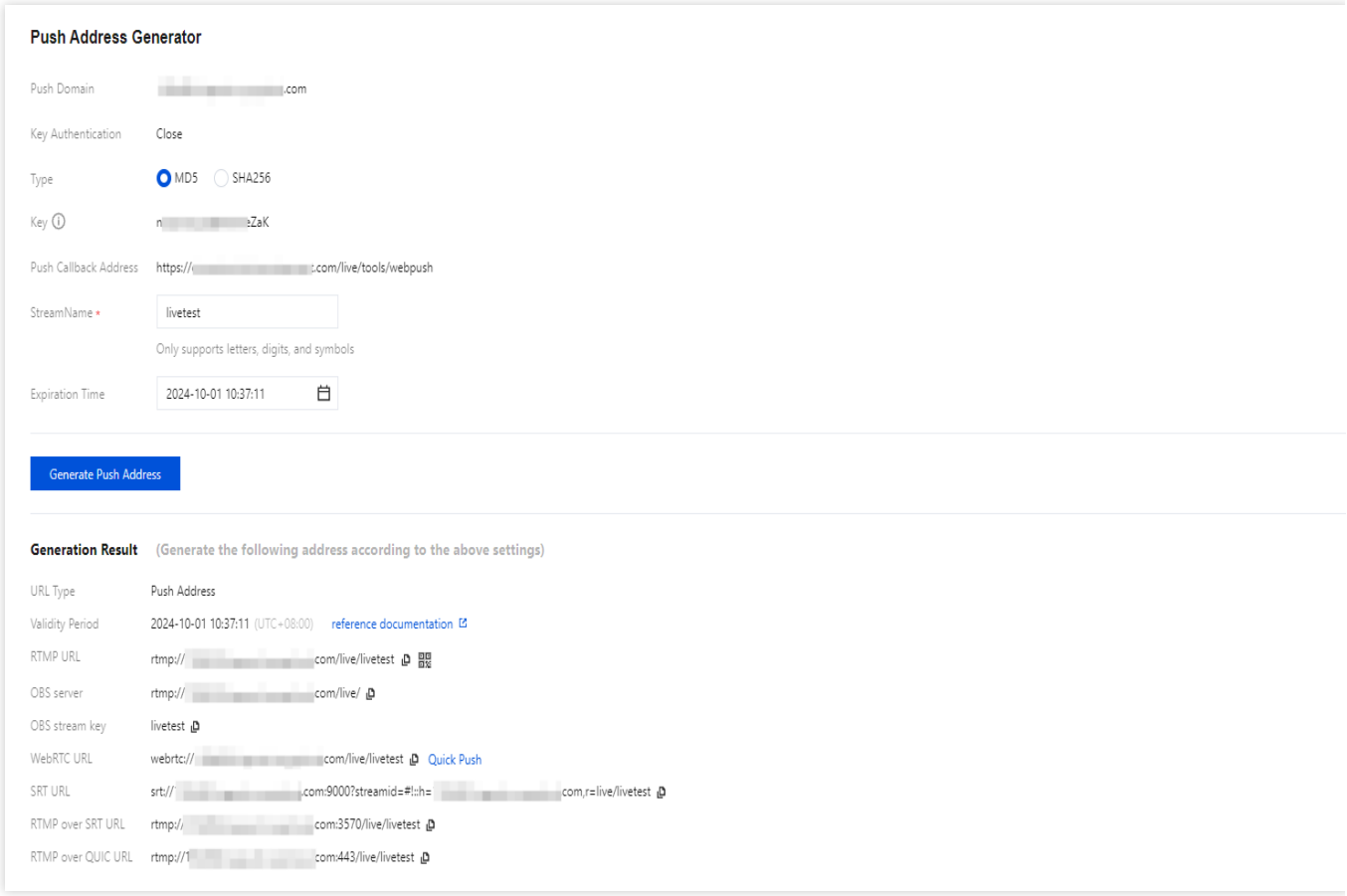
2. Select **Push Configuration** and, in **Push Address Generator**, complete the following settings:

2.1 You need to choose an encryption type based on your security requirements and performance considerations. The encryption type can be either **MD5** or **SHA256**, with **MD5** being the default option.

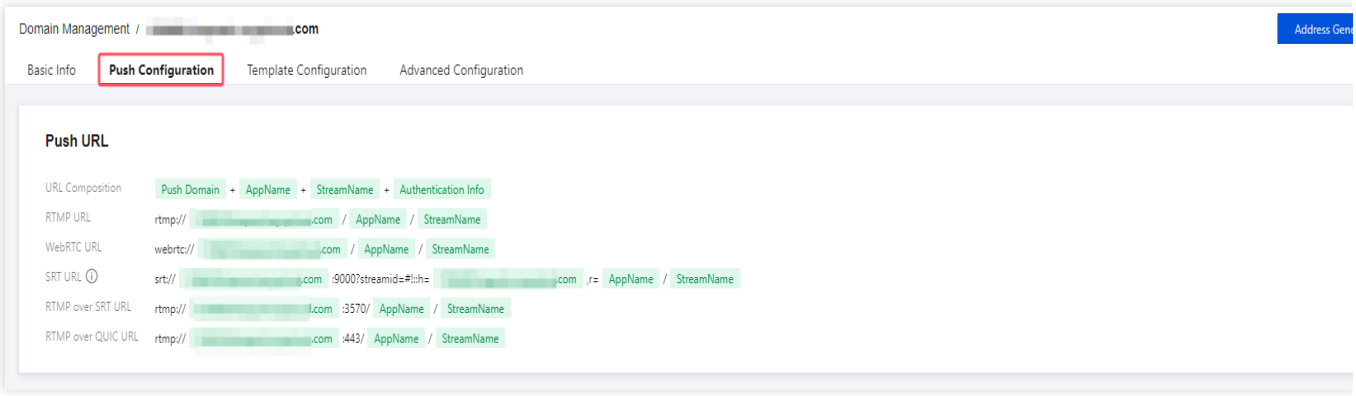
2.2 Enter a custom stream name (`StreamName`).

2.3 Select an expiration time, such as `2024-10-01 10:37:11` .

2.4 Click **Generate Push Address** to generate a push URL containing the `StreamName` .



3. If you haven't enabled authentication for your push domain, then you will also find RTMP, WebRTC, SRT, and RTMP over SRT URLs in the **Push URL** area. Replace `StreamName` in your playback URL with the stream name used for push, and you can use the URL to play the stream.



Push URL format

An RTMP push URL looks like this:

```
rtmp://domain/AppName/StreamName?
txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)
```

Parameter description

`domain` : The push domain name.

`AppName` : The live streaming application name, which is `live` by default and is customizable.

`StreamName` : The custom stream name used to identify a live stream.

`txSecret` : The authentication string generated after push authentication is enabled.

`txTime` : The expiration timestamp for the push URL.

Note:

If you have enabled authentication, `txTime` indicates the expiration time of the URL.

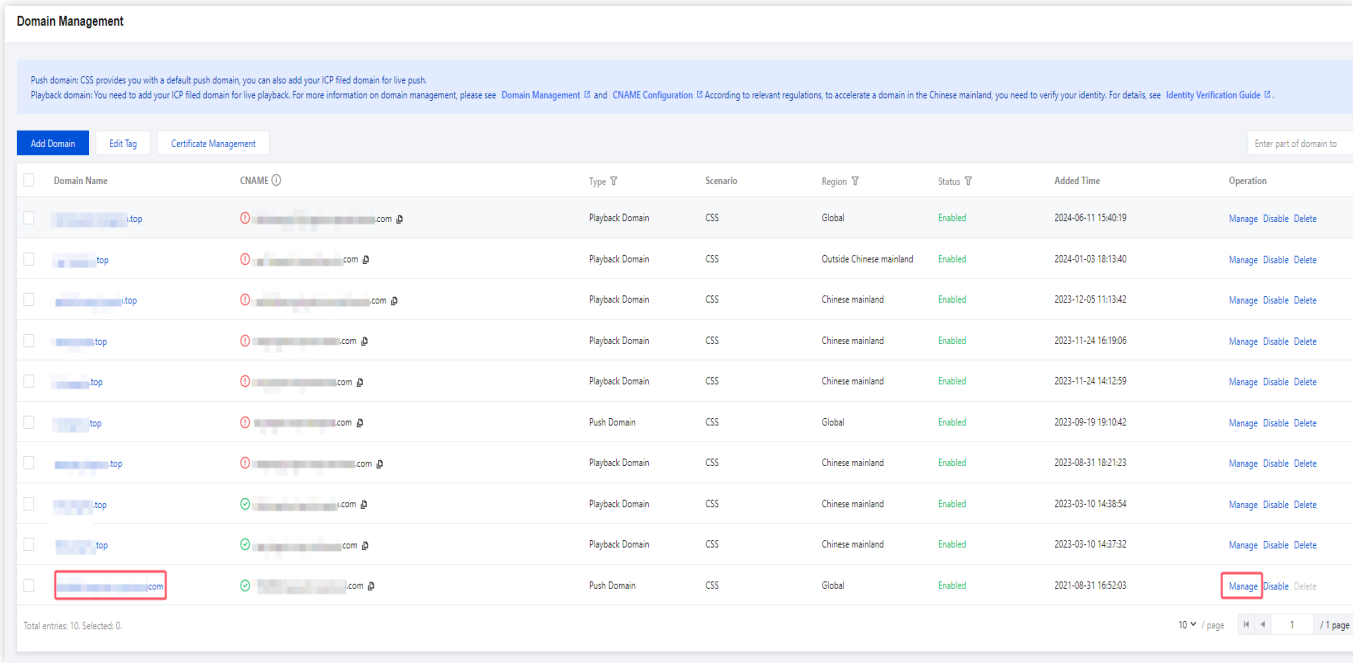
For the sake of convenience, the console allows you to specify the URL expiration time in human-readable format. **If you enable authentication, when generating push URLs, the system will convert it to a hex timestamp (the value of `txTime`).**

As long as you start push or playback before the expiration time and the stream is not interrupted, the push or playback can continue even after the URL expires.

Sample Code of Push URL

We offer sample code in PHP, Java, and Go for generating push URLs. To view the code, follow the steps below:

1. Log in to the CSS console and click Domain Management.
2. Click a push domain name or click **Manage** on the right to enter its details page.



3. Select **Push Configuration** and scroll down to find **Push Address Sample Code**.

4. Click the tab to view the sample code for PHP, Java, or Go.

PHP

Java

GO

```
/**
* Get the push URL
* If you do not pass in the authentication key and URL expiration time, a URL witho
* @param domain: Your push domain name.
*        streamName: A unique stream name to identify the push URL.
*        key: The authentication key.
*        time:   The URL expiration time (example: 2016-11-12 12:00:00).
* @return String url
*/
function getPushUrl($domain, $streamName, $key = null, $time = null){
    if($key && $time){
          $txTime = strtoupper(base_convert(strtotime($time),10,16));
          //txSecret = MD5( KEY + streamName + txTime )
          $txSecret = md5($key.$streamName.$txTime);
          $ext_str = "?".http_build_query(array(
                "txSecret"=> $txSecret,
                "txTime"=> $txTime
          ));
    }
    return "rtmp://".$domain."/live/".$streamName . (isset($ext_str) ? $ext_str : "
}

echo getPushUrl("123.test.com","123456","69e0daf7234b01f257a7adb9f807ae9f","2016-09
```

```
package com.test;

import java.io.UnsupportedEncodingException;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

public class Test {

      public static void main(String[] args) {
            System.out.println(getSafeUrl("txrtmp", "11212122", 1469762325L));
      }

      private static final char[] DIGITS_LOWER =
            {'0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'a', 'b', 'c', 'd',

      /*
```

```
        * KEY+ streamName + txTime
        */
        private static String getSafeUrl(String key, String streamName, long txTime)
              String input = new StringBuilder().
                                append(key).
                                append(streamName).
                                append(Long.toHexString(txTime).toUpperCase()).toStri

              String txSecret = null;
              try {
                    MessageDigest messageDigest = MessageDigest.getInstance("MD5");
                    txSecret  = byteArrayToHexString(
                                messageDigest.digest(input.getBytes("UTF-8")));
              } catch (NoSuchAlgorithmException e) {
                    e.printStackTrace();
              } catch (UnsupportedEncodingException e) {
                    e.printStackTrace();
              }

              return txSecret == null ? "" :
                                new StringBuilder().
                                append("txSecret=").
                                append(txSecret).
                                append("&").
                                append("txTime=").
                                append(Long.toHexString(txTime).toUpperCase()).
                                toString();
        }

        private static String byteArrayToHexString(byte[] data) {
              char[] out = new char[data.length << 1];

              for (int i = 0, j = 0; i < data.length; i++) {
                    out[j++] = DIGITS_LOWER[(0xF0 & data[i]) >>> 4];
                    out[j++] = DIGITS_LOWER[0x0F & data[i]];
              }
              return new String(out);
        }
}
```

```
package a

import (
    "crypto/md5"
    "fmt"
```

```
    "strconv"
    "strings"
    "time"
)

func GetPushUrl(domain, streamName, key string, time int64)(addrstr string){
    var ext_str string
    if key != "" && time != 0{
        txTime := strings.ToUpper(strconv.FormatInt(time, 16))
        txSecret := md5.Sum([]byte(key + streamName + txTime))
        txSecretStr := fmt.Sprintf("%x", txSecret)
        ext_str = "?txSecret=" + txSecretStr + "&txTime=" + txTime
    }
    addrstr = "rtmp://" + domain + "/live/" + streamName + ext_str
    return
}
/*
*domain: 123.test.com
*streamName: streamname
*key: 69e0daf7234b01f257a7adb9f807ae9f
*time: 2022-04-26 14:57:19 CST
*/
func main(){
    domain, streamName, key := "123.test.com", "streamname", "69e0daf7234b01f257a7a
    //CST: ChinaStandardTimeUT, "2006-01-02 15:04:05 MST" must be const
    t, err := time.Parse("2006-01-02 15:04:05 MST", "2022-04-26 14:57:19 CST")
    if err != nil{
        fmt.Println("time transfor error!")
        return
    }
    fmt.Println(GetPushUrl(domain, streamName, key, t.Unix()))
    return
}
```

Related Operations

You can start pushing streams after the push URL is generated. For details, see Live Push.

Recording Configuration

Last updated：2024-07-26 14:44:12

The live recording feature is disabled by default. This document describes how to bind a recording template to a push domain to enable the recording feature, as well as how to unbind a template to disable the feature.

Use Limits

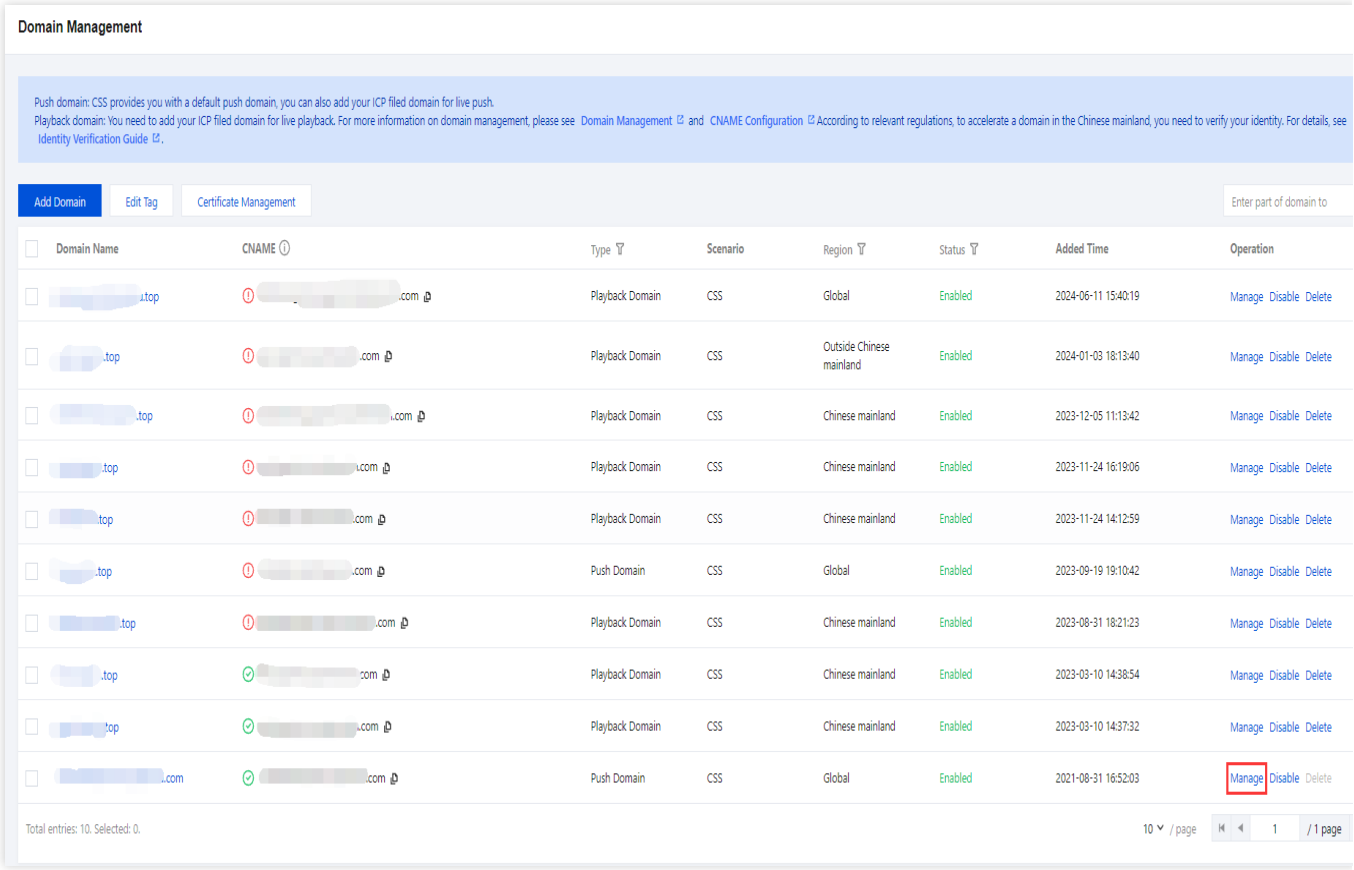
After enabling the recording feature, please make sure that your VOD or COS service is in normal status. If VOD or COS is not activated or is suspended due to overdue payments, live recording will fail. No recording files will be generated. Nor will fees be incurred.
A template takes effect about 5-10 minutes after it is bound to a domain.
After a template is successfully bound to a push domain, recording will be enabled for push addresses under that domain.
One domain can be bound with only one recording template. After binding, all streams under that domain will be recorded according to the template.
Mixed-stream recording does not support mixing streams inside the Chinese mainland with those outside. It will cause an error and playback will fail.

Prerequisites

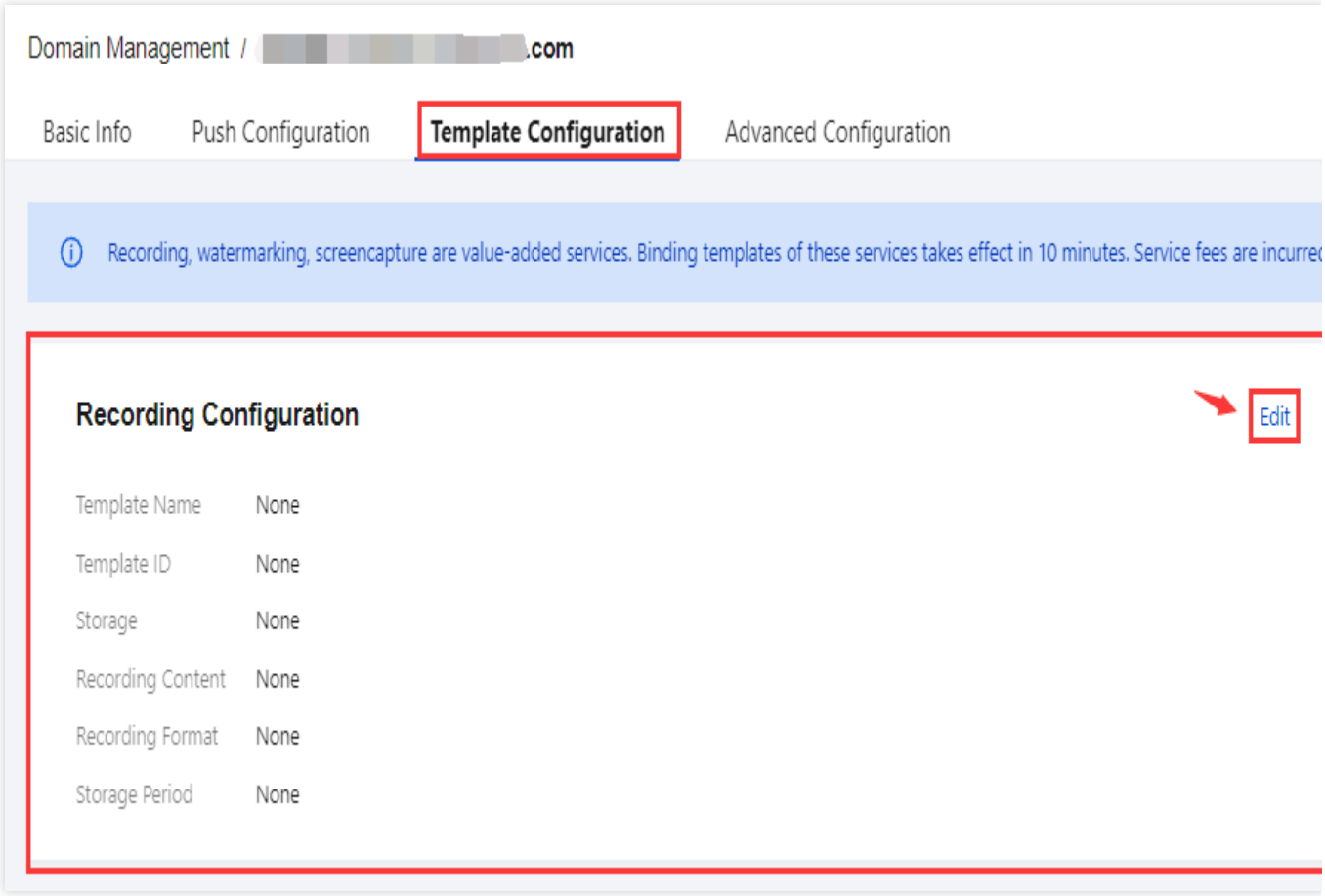
You have logged in to the CSS console and added a push domain.
You have created a recording template.

Binding a Recording Template

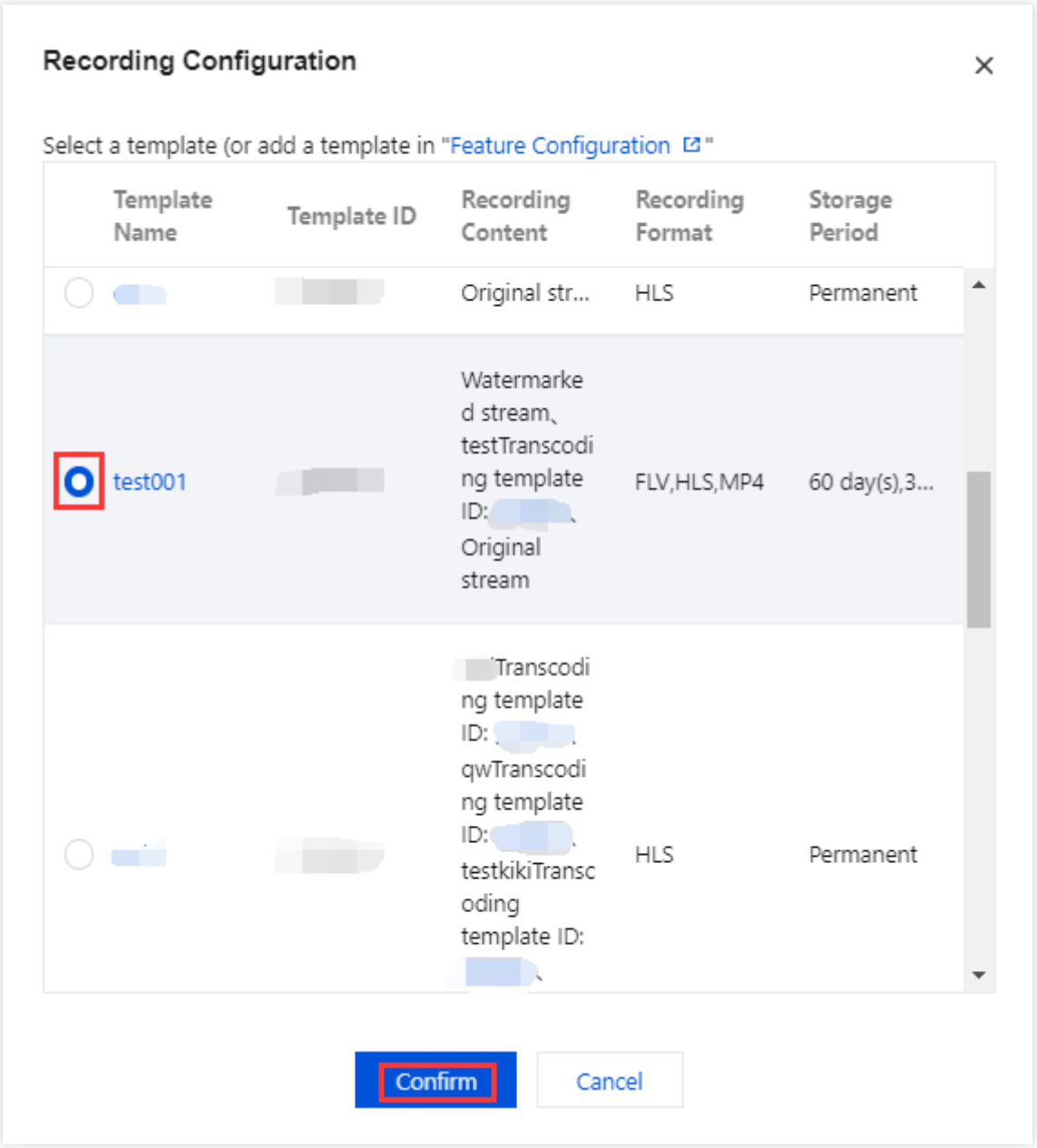
1. Go to Domain Management, and click the target **push domain** or click **Manage** to enter the domain details page.

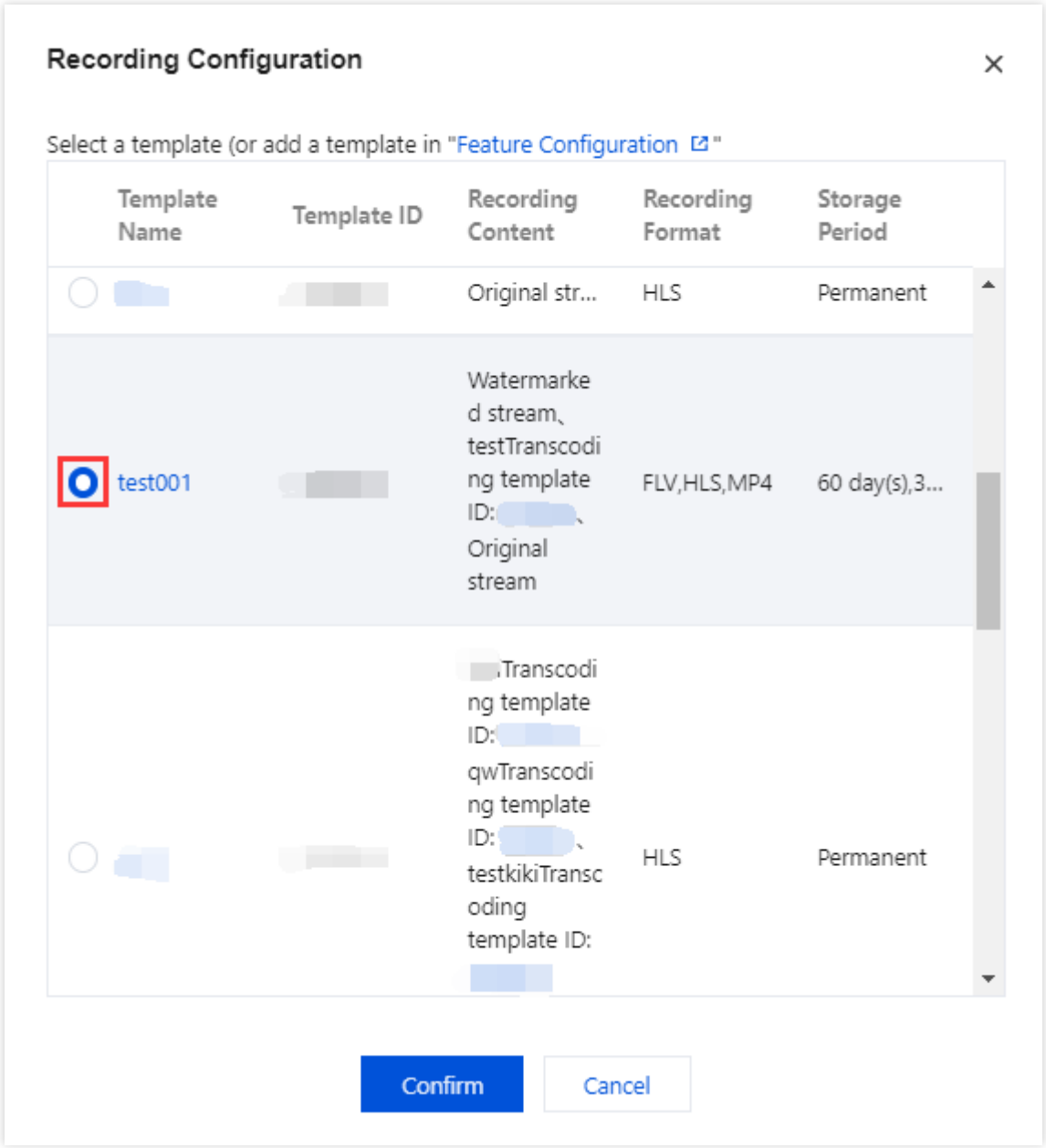


2. Select the **Template Configuration** tab and click **Edit** in the **Recording configuration** area.



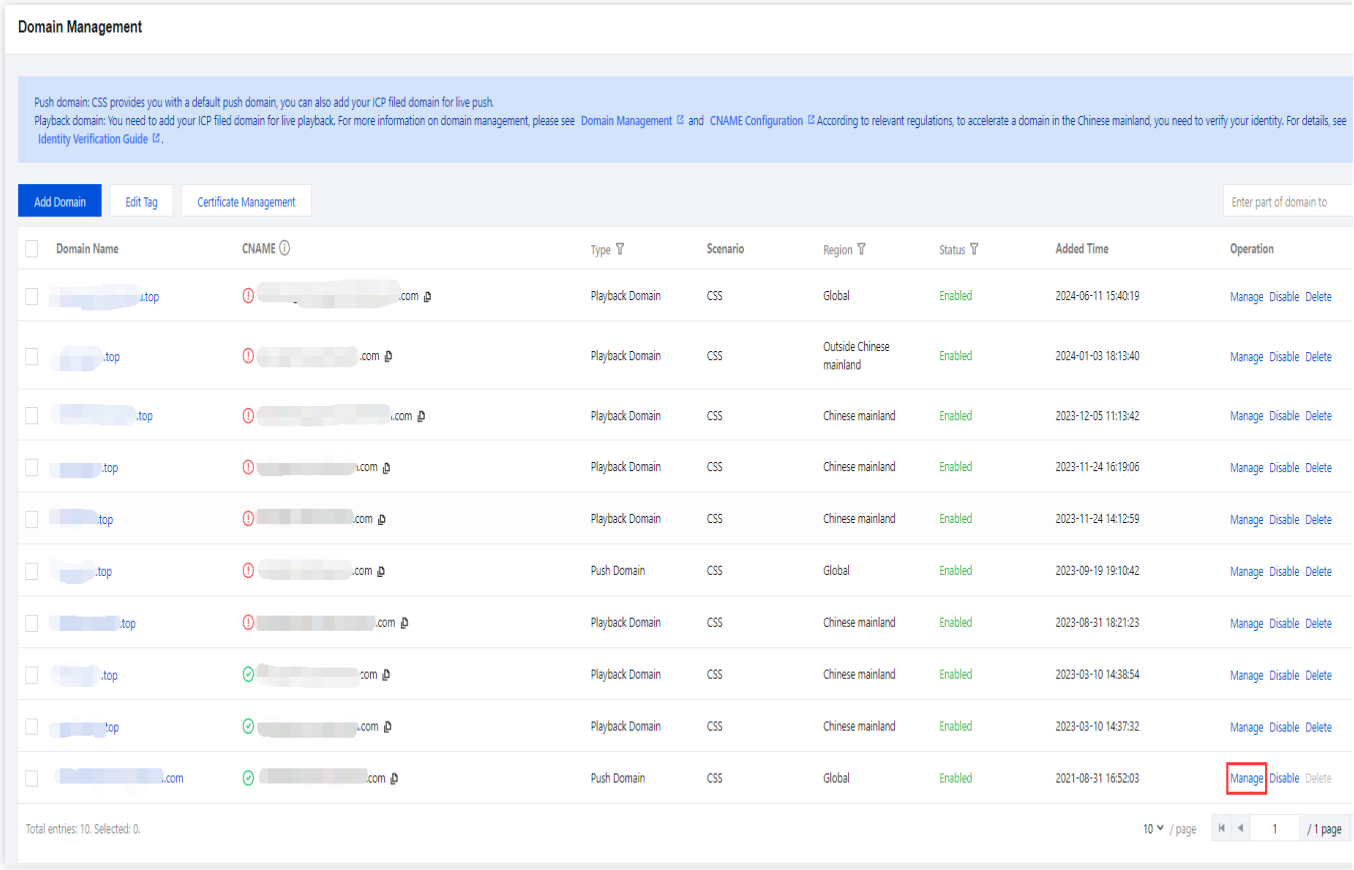
3. Select a recording template and click **Confirm**.


Recording Configuration
Select a template (or add a template in "Feature Configuration")
Template Name
Template ID
Recording Content
Recording Format
Storage Period
Original str...
HLS
Permanent
test001
Watermarked stream、testTranscoding template ID: 、Original stream
FLV,HLS,MP4
60 day(s),3...
Transcoding template ID: 、qwTranscoding template ID: 、testkikiTranscoding template ID: 、
HLS
Permanent
Confirm
Cancel

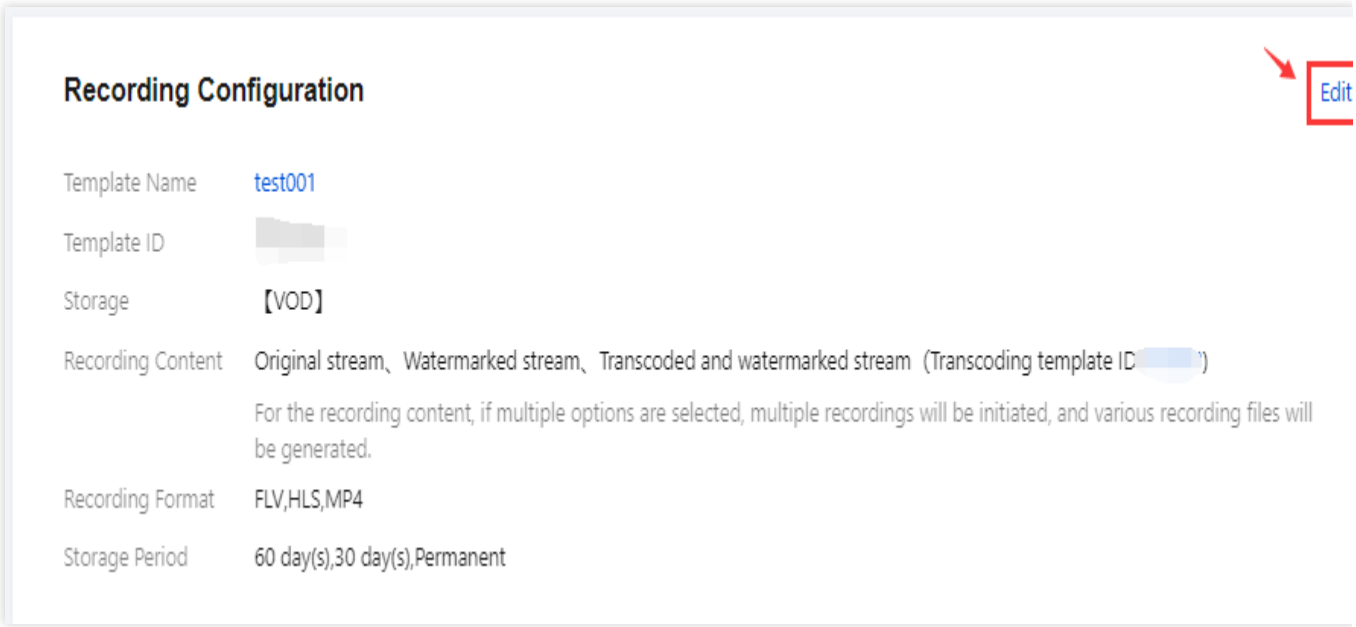


Unbinding a Recording Template

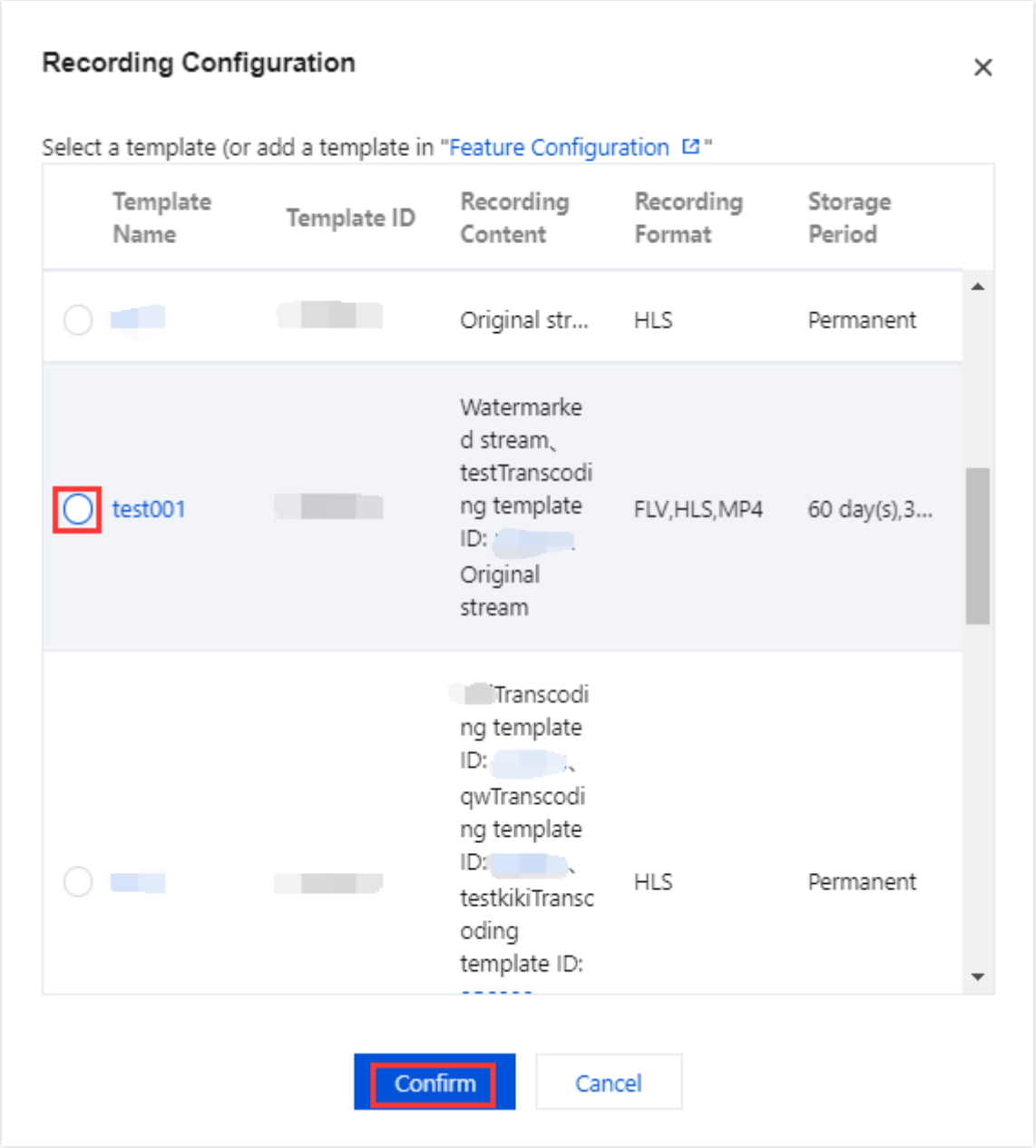
1. Go to Domain Management, and click the target **push domain** or click **Manage** to enter the domain details page.



2. Select the **Template Configuration** tab and click **Edit** in the **Recording configuration** area.



3. Unselect the template and click **Save**.



Note:

Unbinding a recording template will not affect ongoing live streams.

To cancel recording for ongoing streams, stop the streams and push them again.

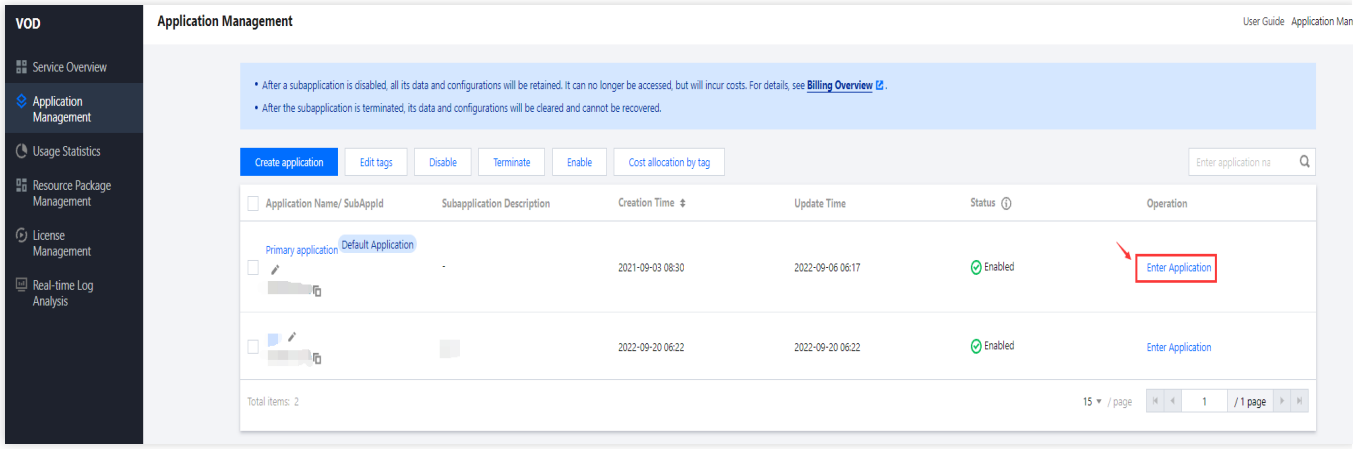
Obtaining Recording Files

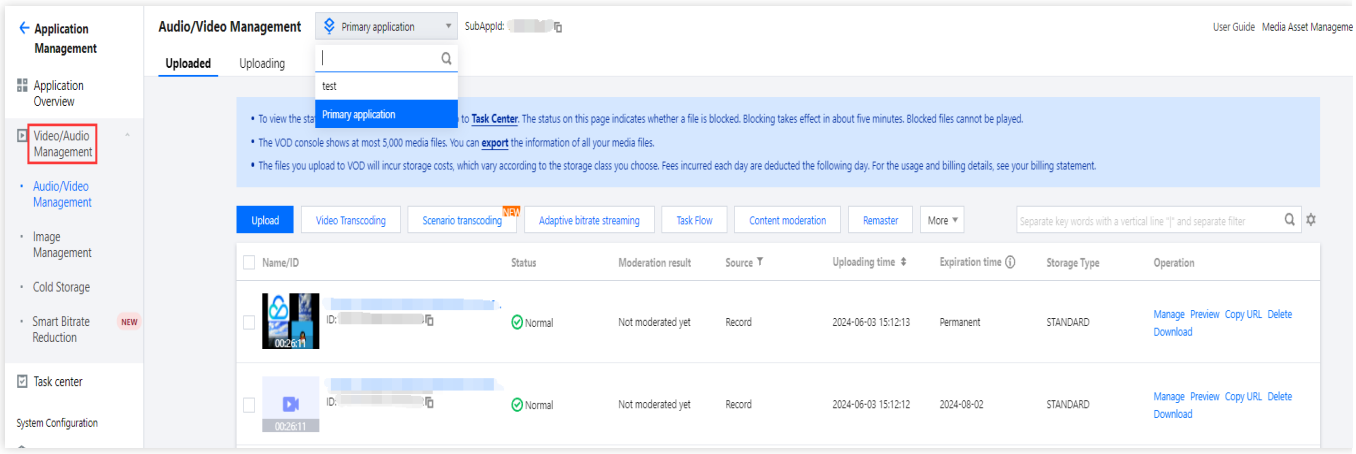
You can obtain recording files in the following ways:

Recording to VOD

From the VOD console

Log in to the VOD console, select the target subapplication, and click **Video/Audio Management** on the left sidebar. You can view all your recording files on this page.





From recording callbacks

If you have configured a recording callback address in the console or using an API, after a recording file is generated, a notification will be sent to the callback address configured. For details about the fields of the callback, see How to Receive Event Notification.

Note:

The recording callback method is recommended for its reliability and real-timeliness.

Using a VOD API

You can also call the SearchMedia API of VOD to query recording files.

Recording to COS

From the COS console

Log in to the COS console, click Bucket List on the left sidebar, and then click the target bucket. You will be able to find the recording files in the file list.

Time Shifting Configuration

Last updated：2024-05-07 19:04:45

This document shows you how to bind a time shifting template to a push domain to enable time shifting for the domain, as well as how to unbind a template to disable the feature. Time shifting is disabled by default.

Use Limits

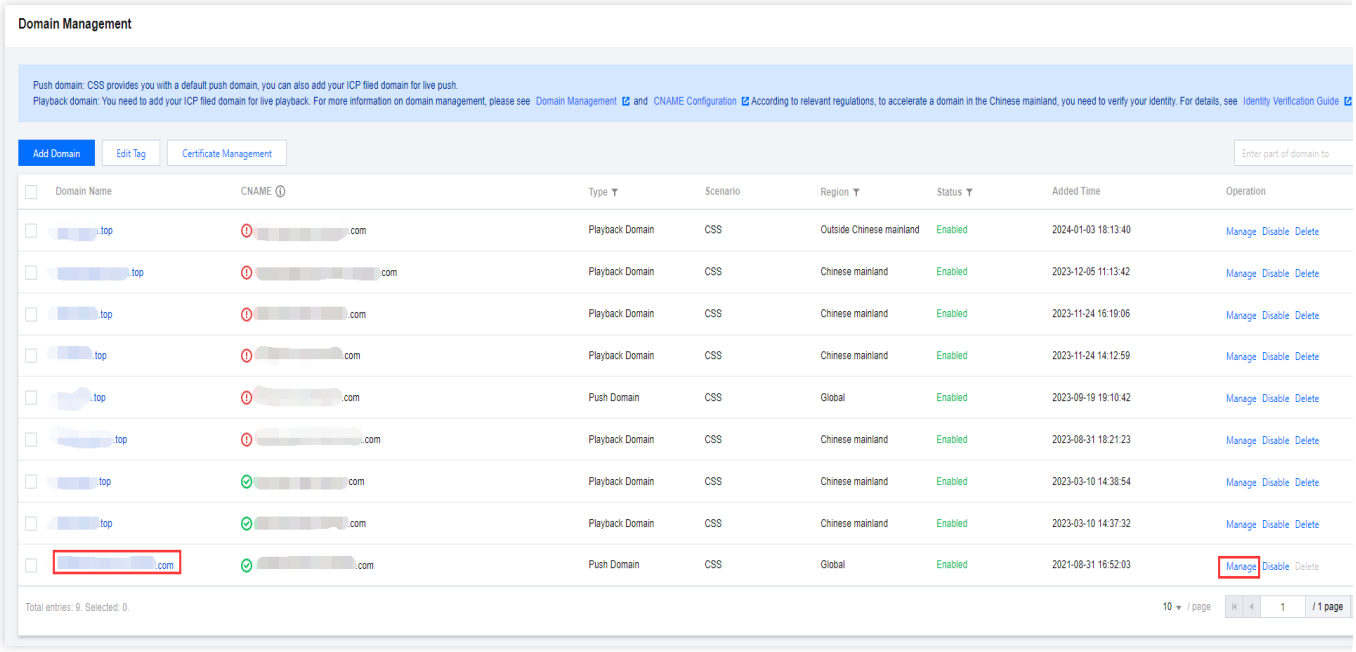
A template takes effect about 5-10 minutes after it is bound to a domain.
After a template is successfully bound to a push domain, time shifting will be enabled for push addresses under that domain.
One domain can be bound to only one time shifting template. After binding, time shifting will be enabled for all streams under the domain.

Prerequisites

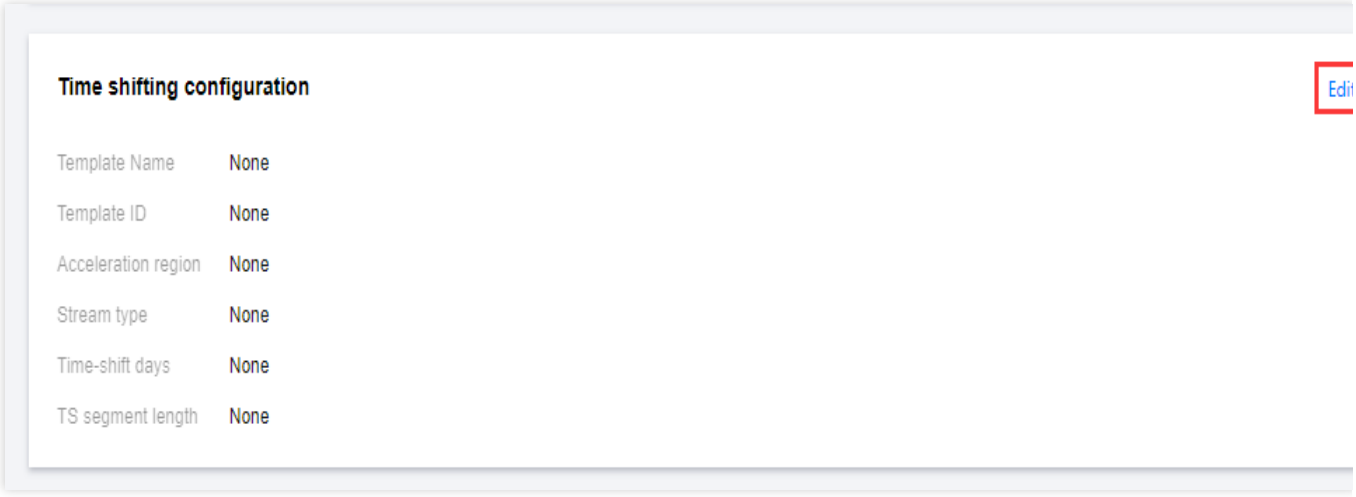
You have logged in to the CSS console and added a push domain.
You have created a time shifting template.

Binding a Time Shifting Template

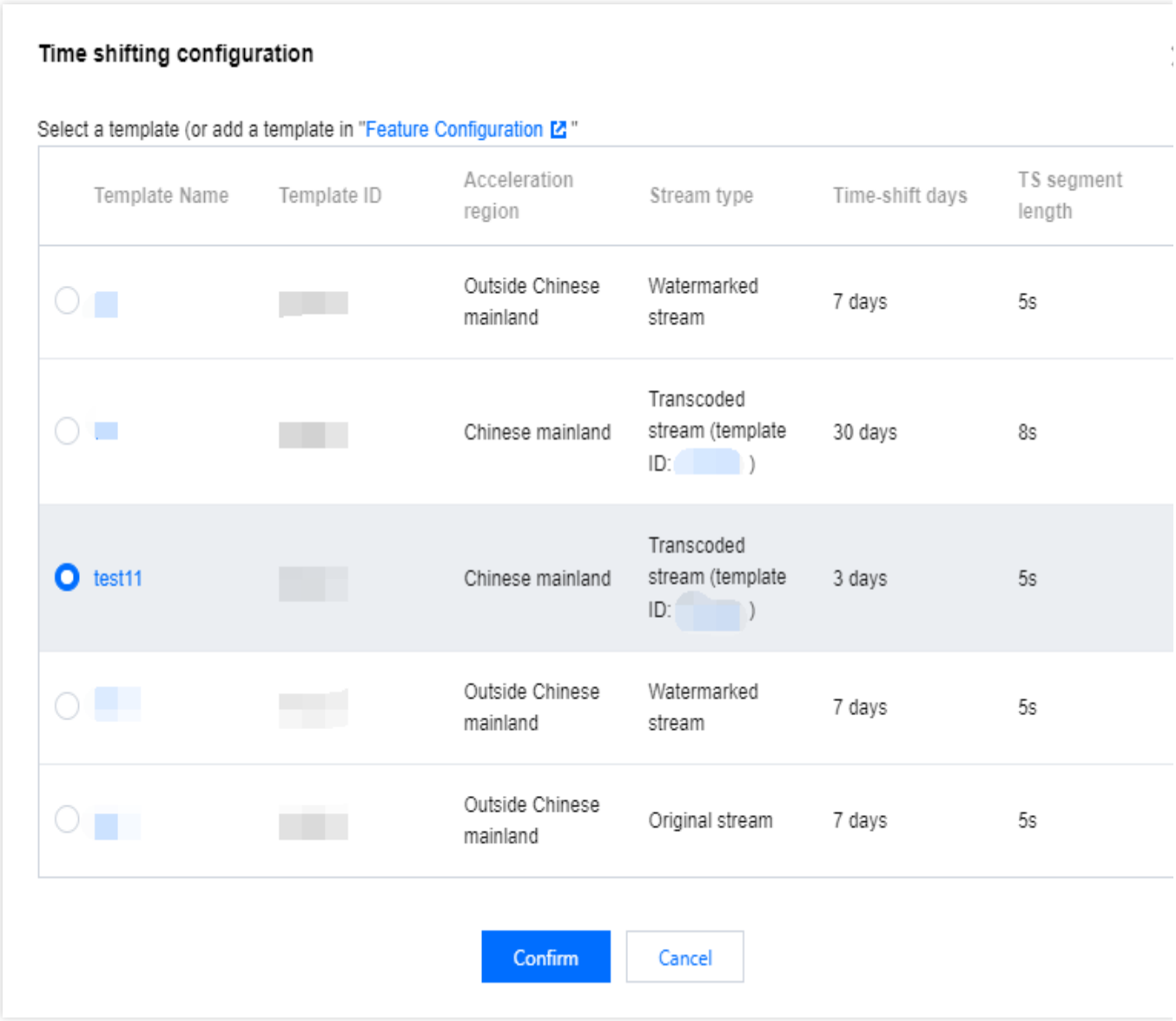
1. Go to Domain Management, and click the target **push domain** or click **Manage** to enter the domain details page.



2. Select the **Template Configuration** tab and click **Edit** in the **Time shifting configuration** area.

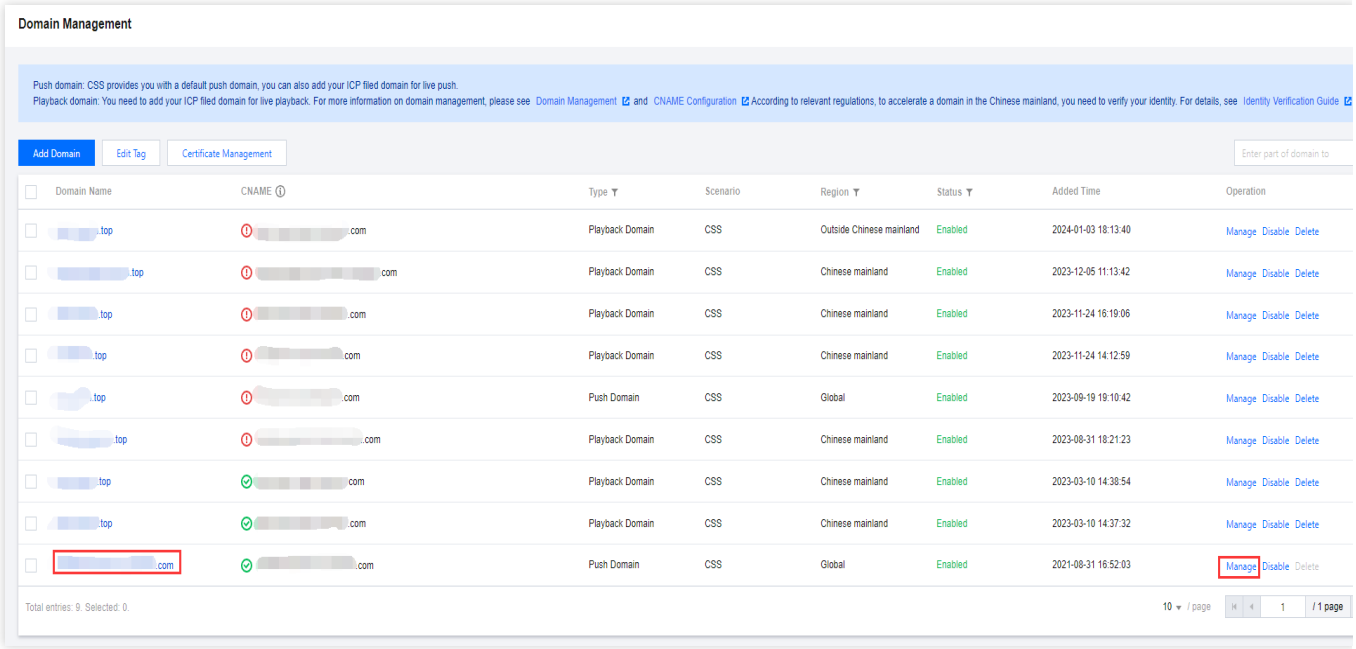


3. Select a time shifting template and click **Confirm**.



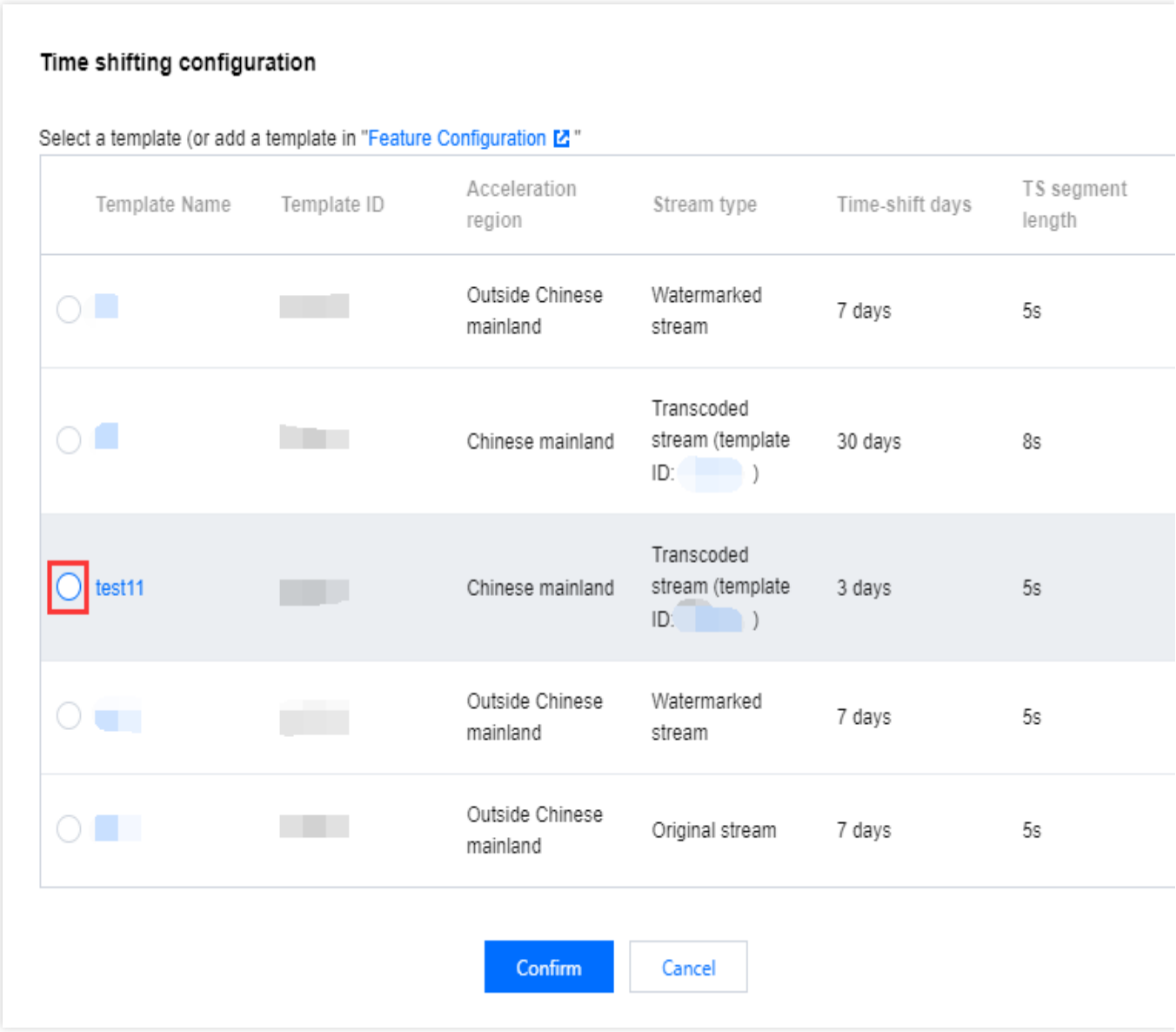
Unbinding a Time Shifting Template

1. Go to Domain Management, and click the target **push domain** or click **Manage** to enter the domain details page.



2. Select the **Template Configuration** tab and click **Edit** in the **Time shifting configuration** area.

3. Unselect the template and click **Save**.



Note:

Unbinding a time shifting template will not affect ongoing live streams.

Screencapture and Porn Detection Configuration

Last updated：2024-06-25 15:51:16

Live streaming push is set to have the screenshot feature turned off by default. This article will guide you on how to enable the screenshot feature on a specified push domain and establish a connection with a screenshot template, as well as how to unbind the template and disable the screenshot feature.

Notes

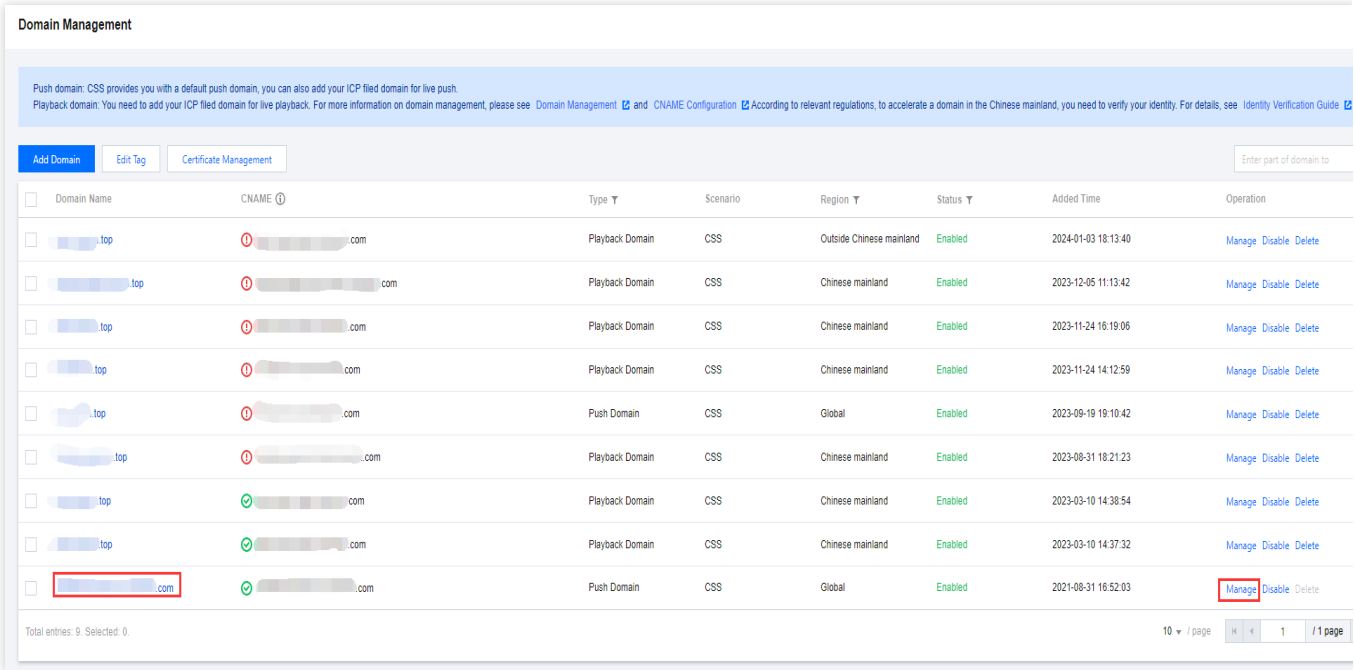
The template configuration will take effect in about **5 – 10 minutes**.
After completing the screenshot template configuration, you also need to configure the callback template to receive the screenshot results. For callback template configuration, please refer to Callback Configuration.
A domain can only be associated with one screenshot template. After the association, all streams under that domain will have screenshot tasks performed according to that template.

Prerequisites

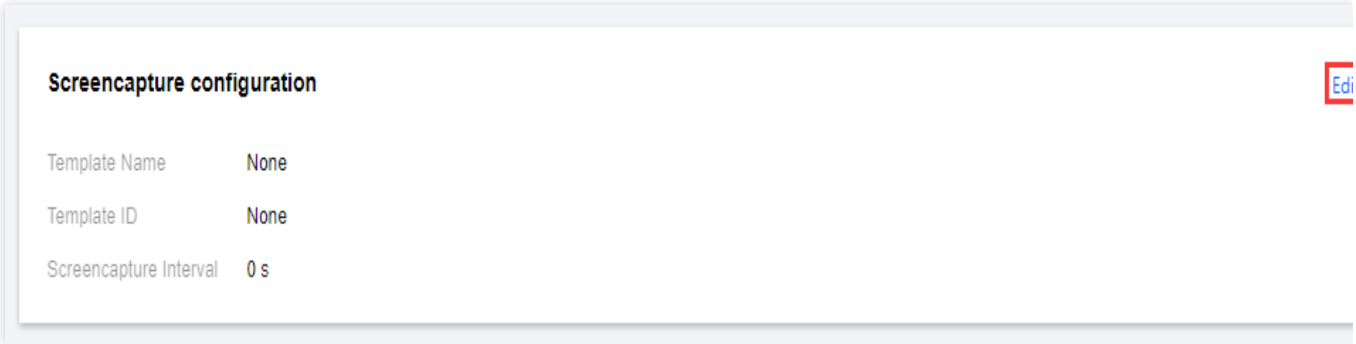
You have logged in to the CSS console and added a push domain name.
You have already created a Screenshot Template.

Bind Screencapture Template

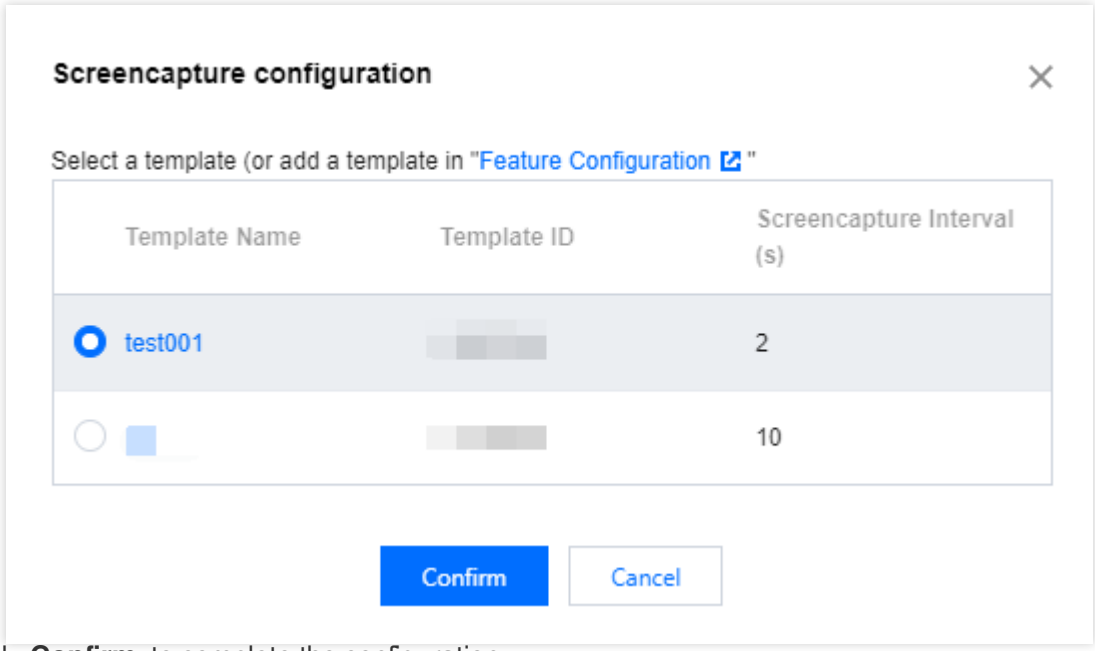
1. Go to Domain Management, and click the target push domain or click Manage to enter the domain details page.



2. Select the **Template Configuration**, and click on the **Edit** button in the upper right corner of the **Screenshot Configuration** tab.



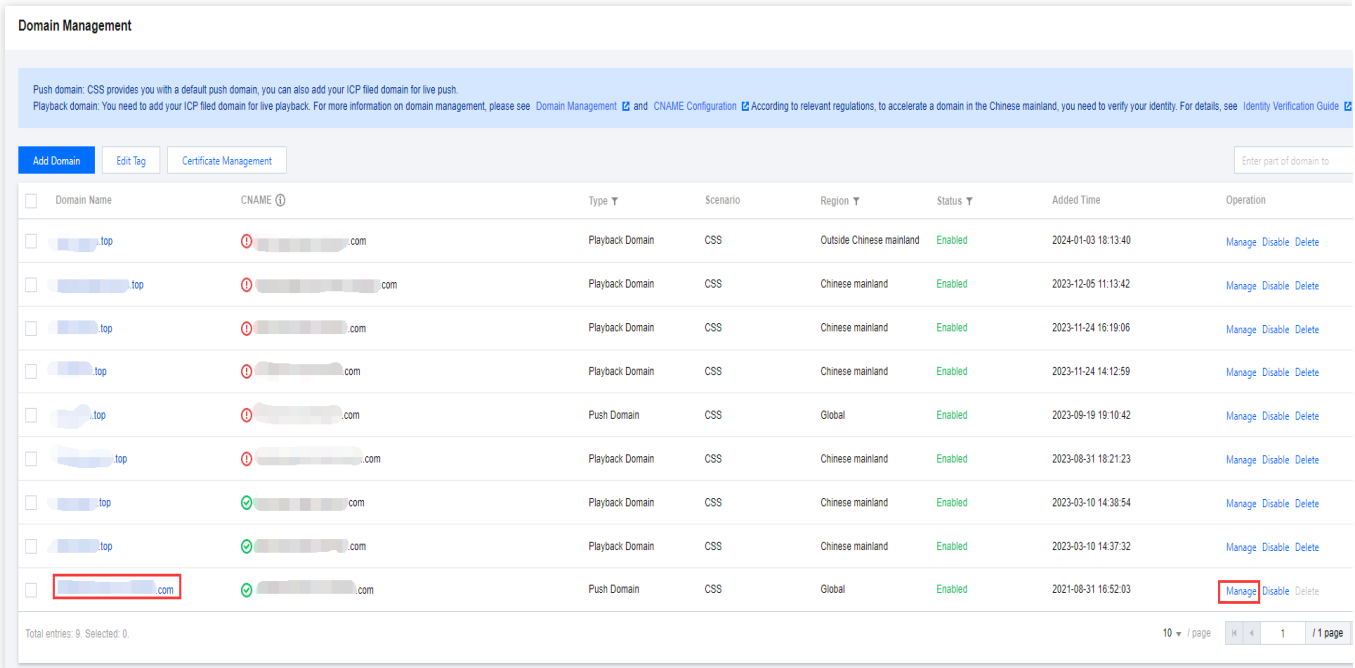
3. Select a screenshot configuration template based on your actual business needs.



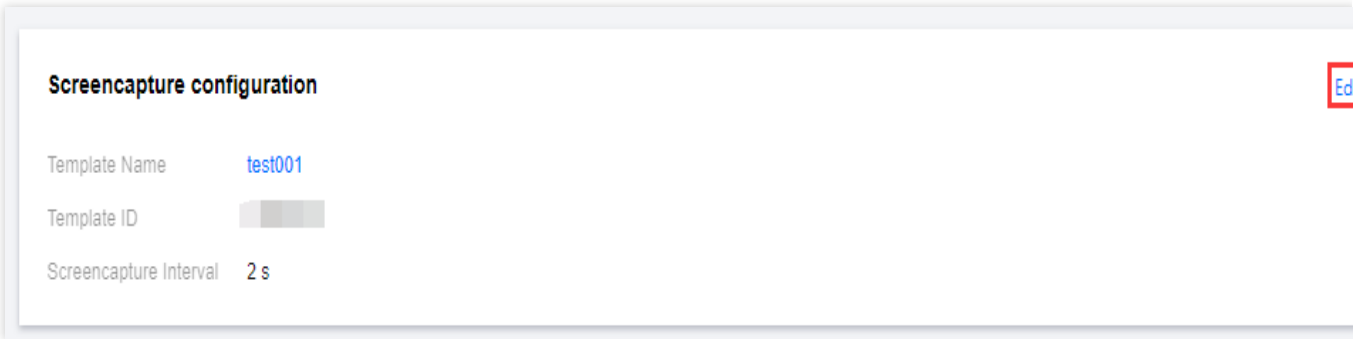
4. Click **Confirm** to complete the configuration.

Unbind screenshot template

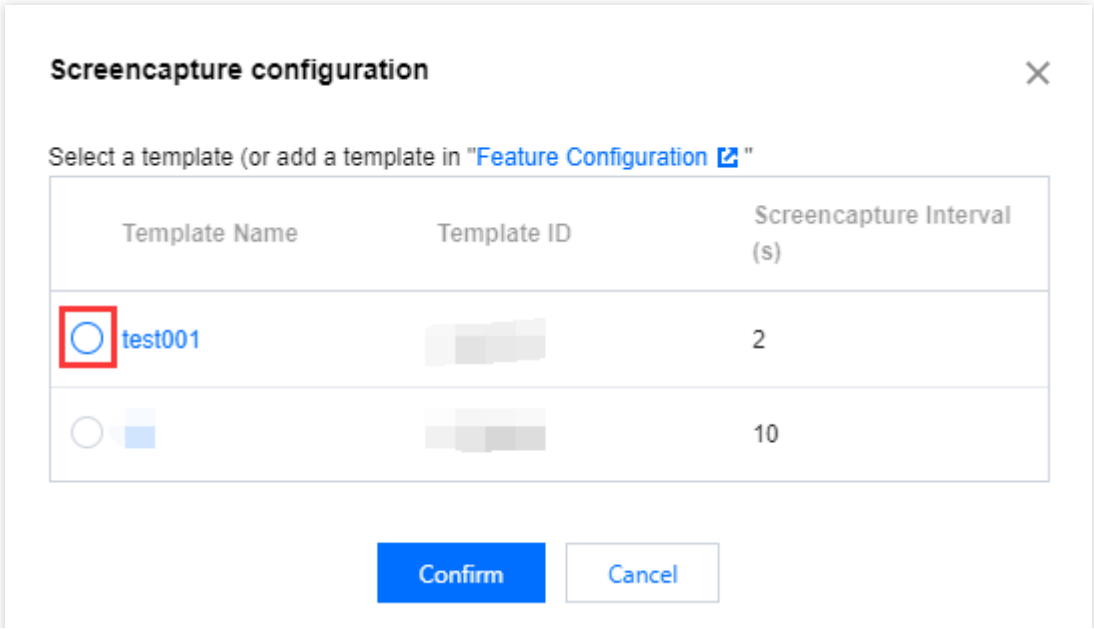
1. Go to Domain Management and click the push domain name to be configured or **Manage** to enter the domain name details page.



2. Select the**Template Configuration** tab, and click on the **Edit** button in the upper right corner of the **Screenshot Configuration** tab.



3. Based on your actual business needs, uncheck the corresponding template and click **Confirm** .



Watermark Configuration

Last updated：2024-06-18 14:40:42

The watermark feature is disabled by default for live push. This document describes how to bind/unbind a push domain name to/from a watermark template to enable/disable the watermark feature.

Notes

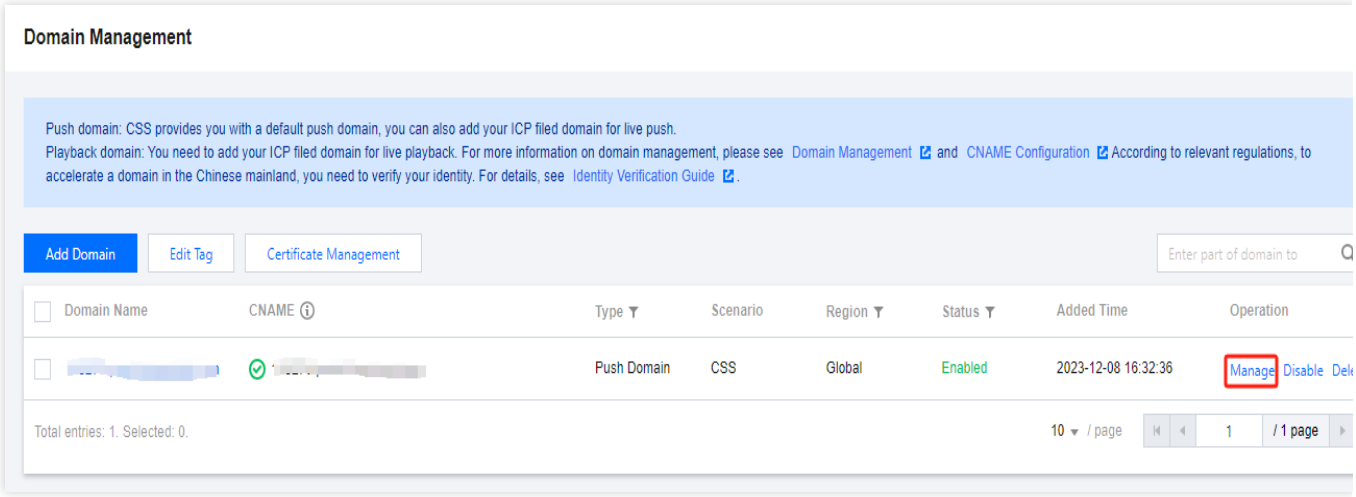
The template configuration will take effect in about 5–10 minutes.
After the template is bound successfully, the watermark feature will be enabled for push addresses under the specified push domain name.
One domain name can be bound to only one watermark template. After they are bound, all streams under the domain name will be watermarked according to this template.

Prerequisites

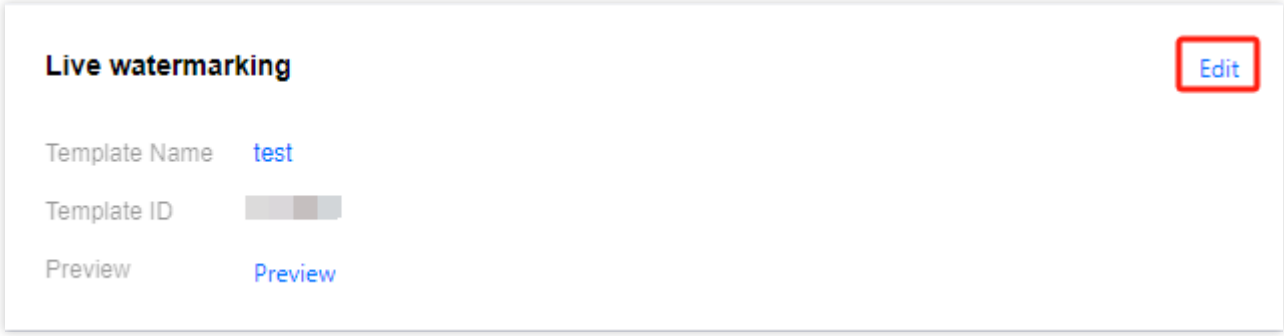
You have logged in to the CSS console and added a push domain name.
You have created a watermark template.

Binding Watermark Template

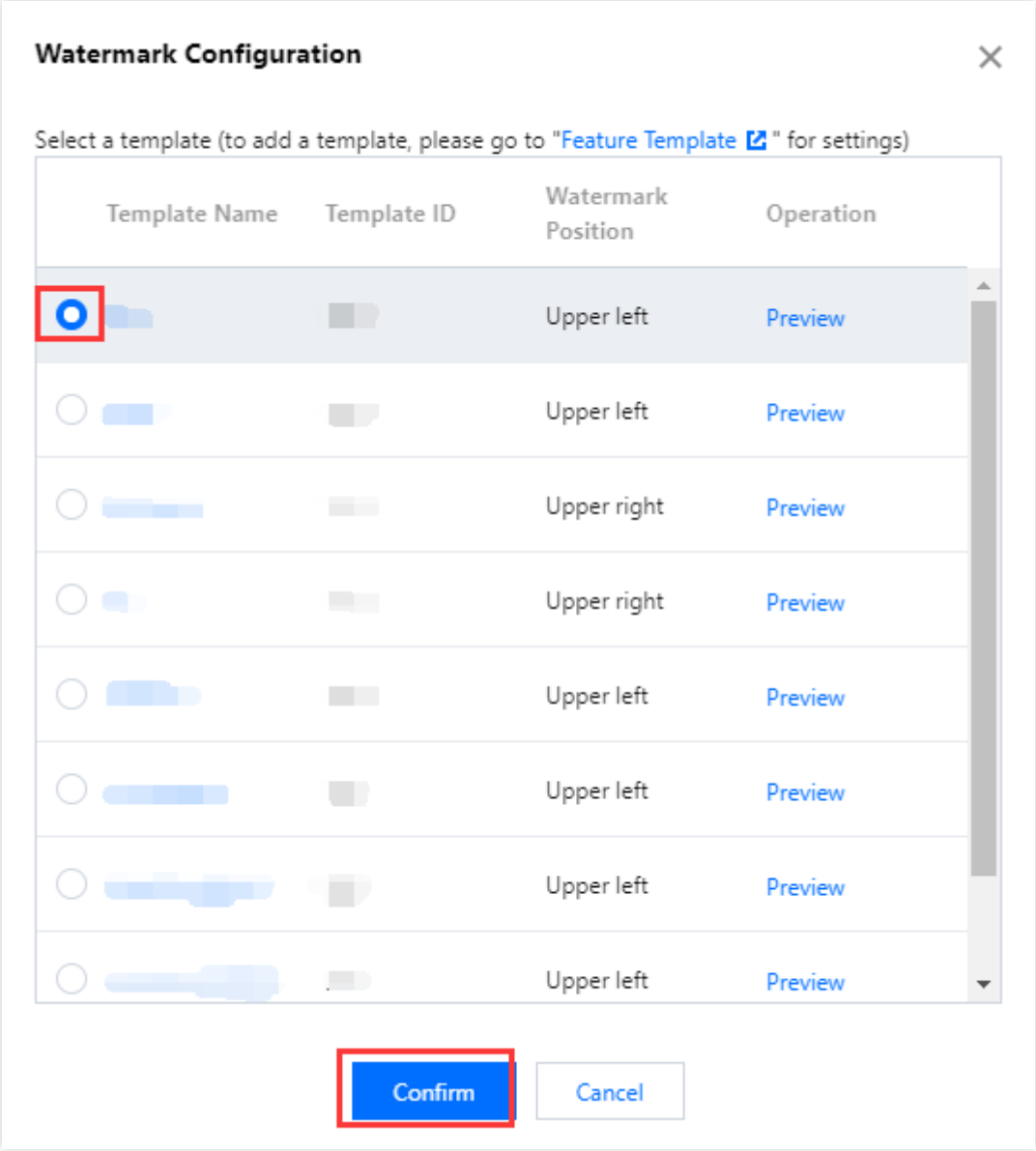
1. Go to **Domain Management** and click the **push domain name** to be configured or **Manage** to enter the domain name details page.



2. Click **Template Configuration** and, in the **Live Watermarking** area, click **Edit**.



3. Select a watermark template and click **Confirm**.

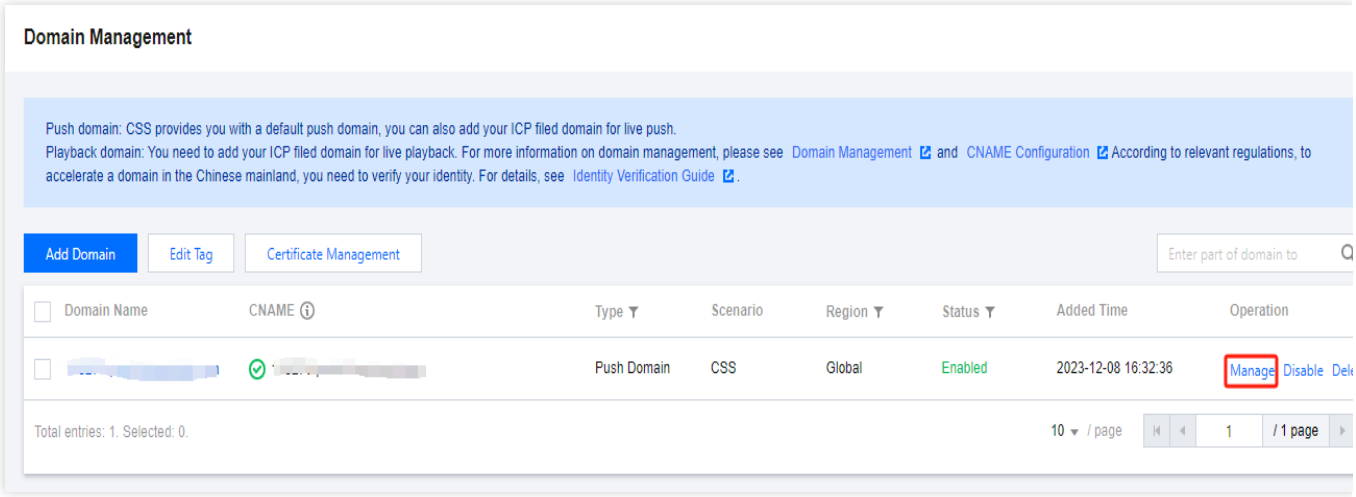


Note:

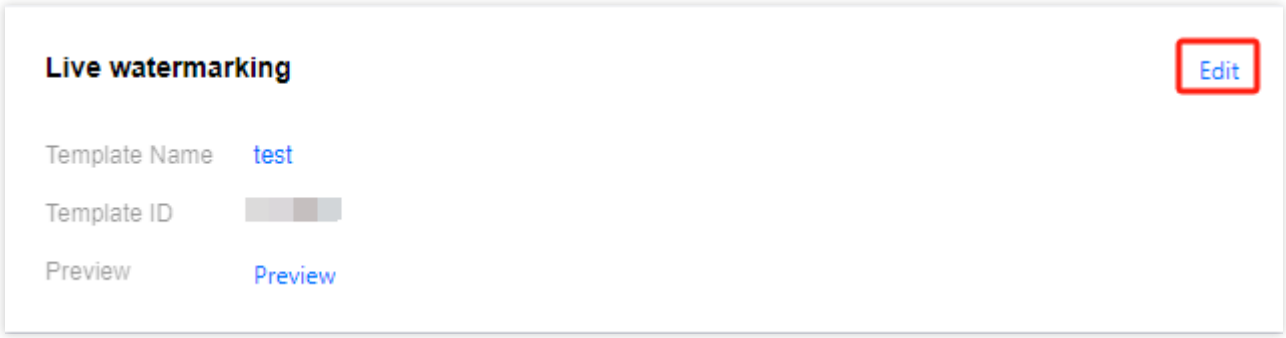
You can click **Preview** in the Operation column to view the watermark.

Unbinding Watermark Template

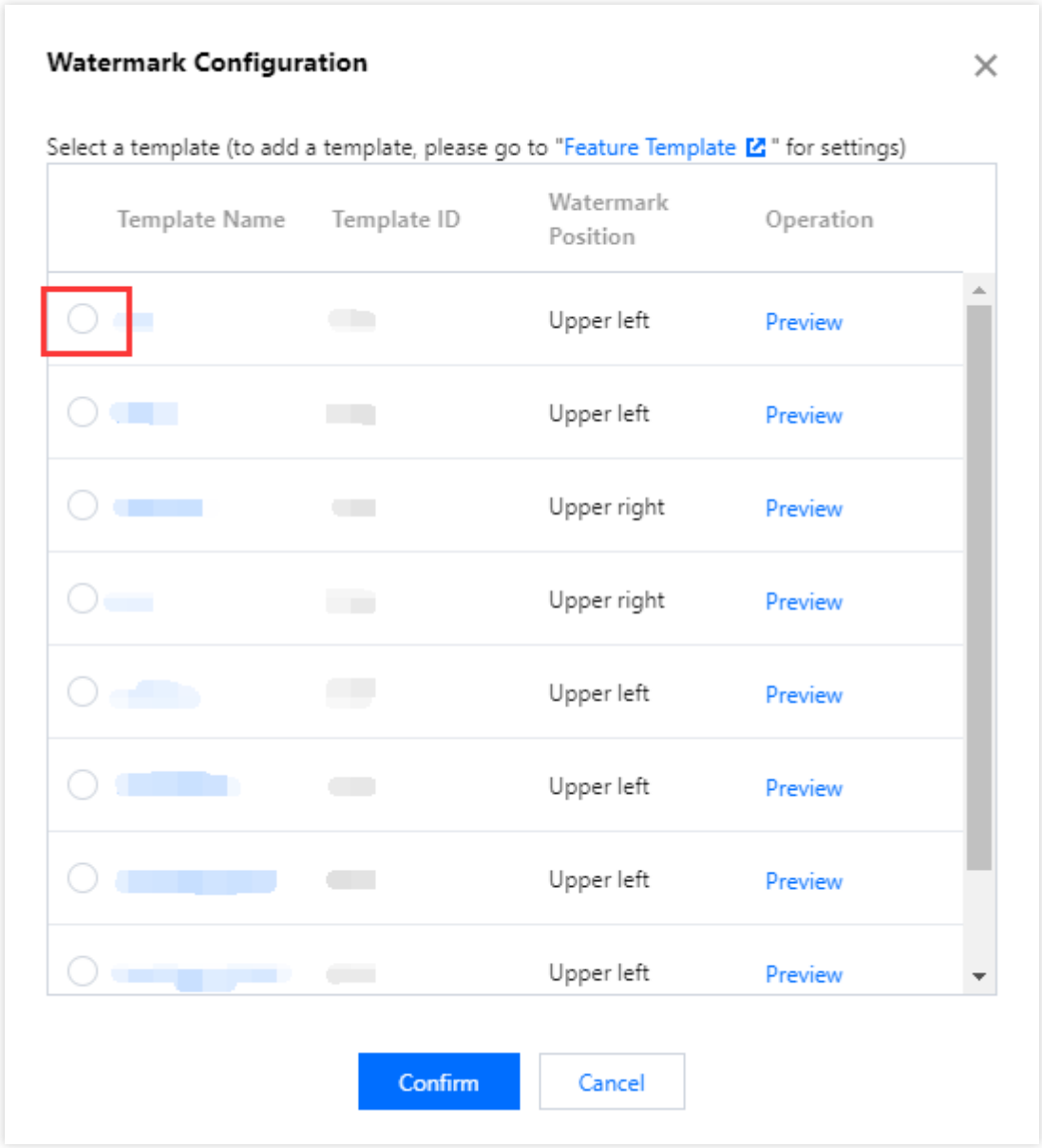
1. Go to **Domain Management** and click the **push domain name** to be configured or **Manage** to enter the domain name details page.



2. Select **Template Configuration** and click **Edit** in the **Live Watermarking** section.



3. Clear the target template and click **Confirm**.


Watermark Configuration
Select a template (to add a template, please go to "Feature Template " for settings)
Template Name
Template ID
Watermark Position
Operation
Upper left
Preview
Upper left
Preview
Upper right
Preview
Upper right
Preview
Upper left
Preview
Upper left
Preview
Upper left
Preview
Upper left
Preview
Confirm
Cancel

Callback Configuration

Last updated：2025-03-20 17:55:12

The callback feature is disabled by default for Cloud Streaming Services (CSS) push. After a push domain name is bound to a callback configuration, the callback feature will be enabled for all push addresses under this domain name. If a callback event is triggered by the configured template during live streaming, Tencent Cloud will send a request to the customer's server which is responsible for the response. After verification, the customer can obtain a JSON packet containing the callback information.
This document describes how to bind/unbind a push domain name to/from a callback template to enable/disable the callback feature.

Notes

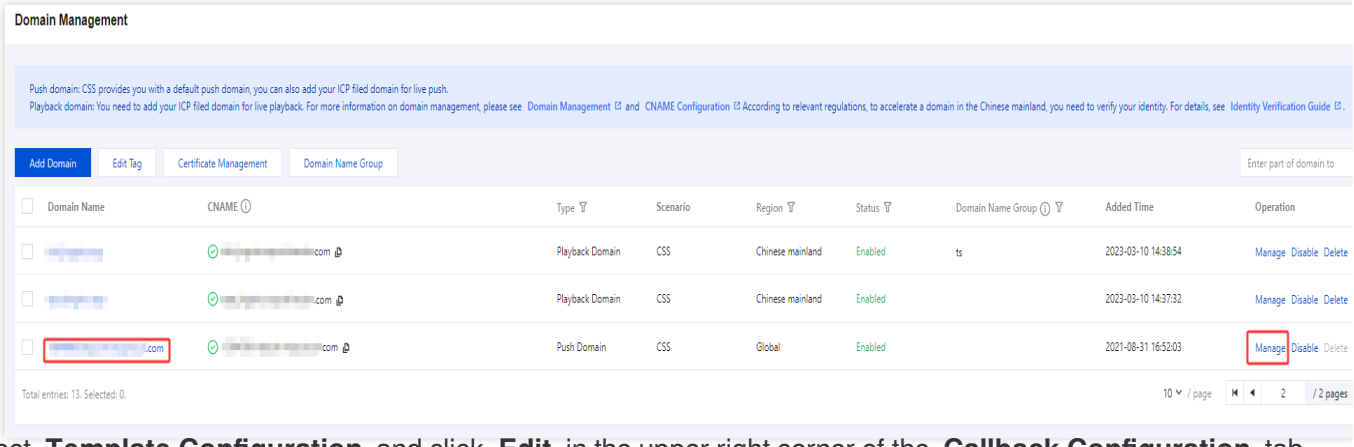
The template configuration will take effect in about 5–10 minutes.
When a CSS event is triggered after the callback feature is enabled, you can receive the event information through the event message notification.
The callback templates are managed at the domain name level in the console, and rules created by APIs cannot be canceled for the time being. If you bound a template to a specified stream through the callback APIs and want to unbind it, you need to call the DeleteLiveCallbackTemplate API.
One domain name can be bound to only one callback template. After binding, all streams under it will be called back according to this template.

Prerequisites

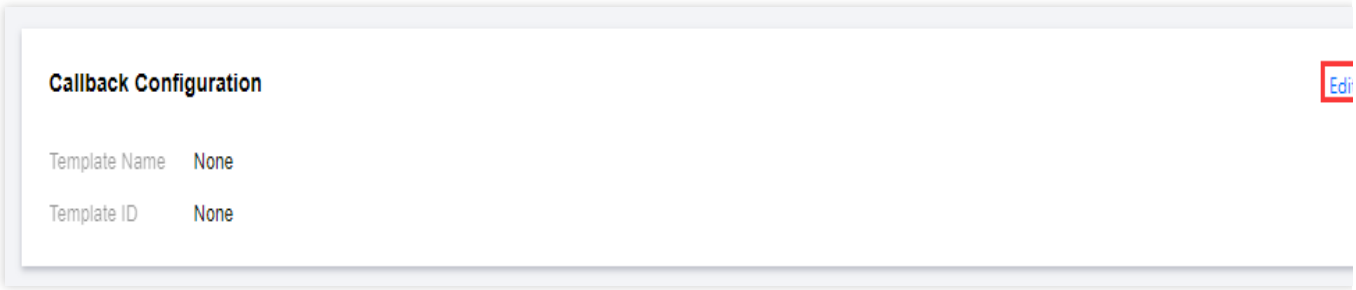
You have logged in to the CSS console and added a push domain name.
You have created a callback template.

Binding Callback Template

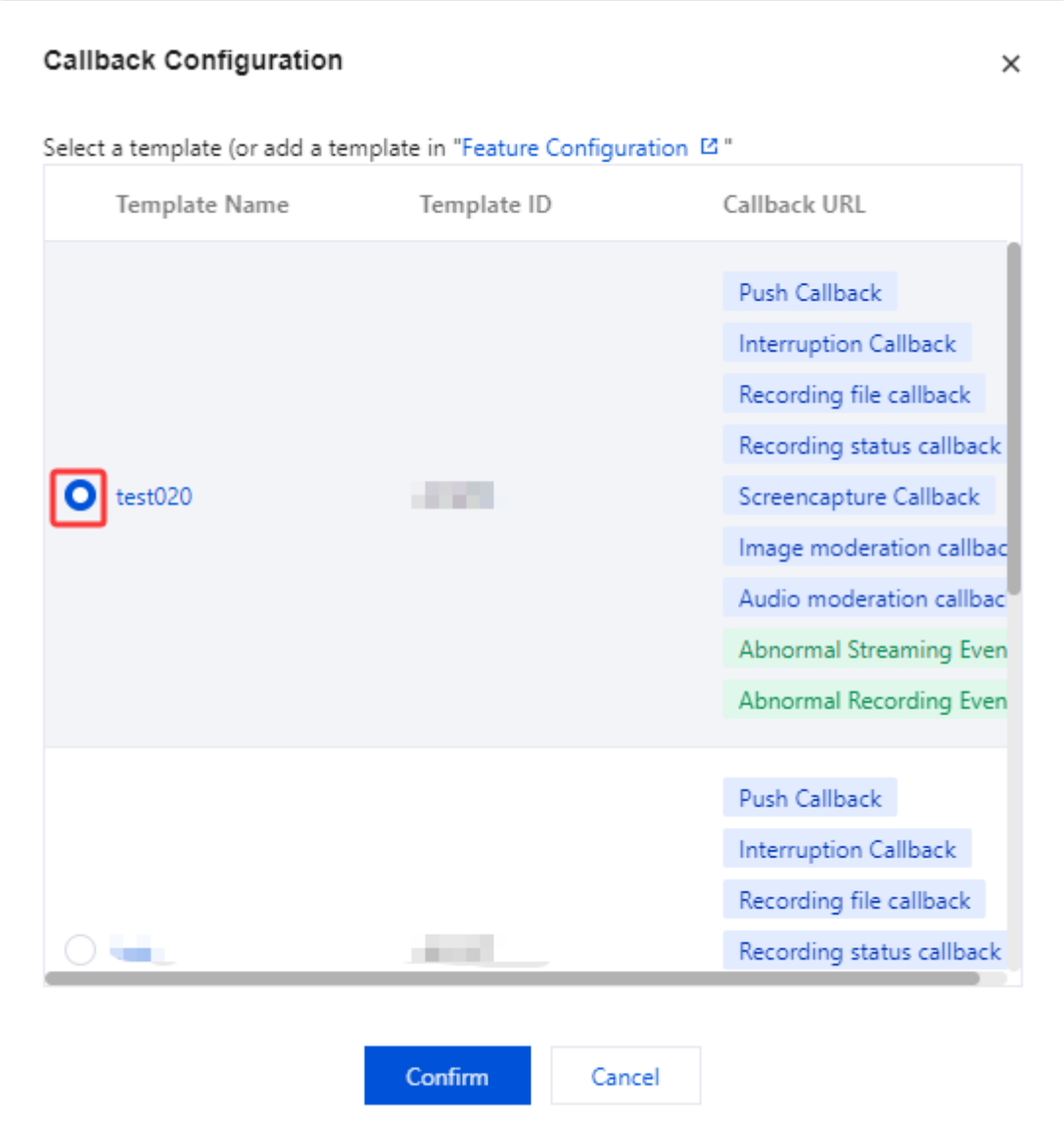
1. Go to Domain Management, and click the target **push domain name** or **Manage** to enter the domain details page.



2. Select **Template Configuration** and click **Edit** in the upper right corner of the **Callback Configuration** tab.

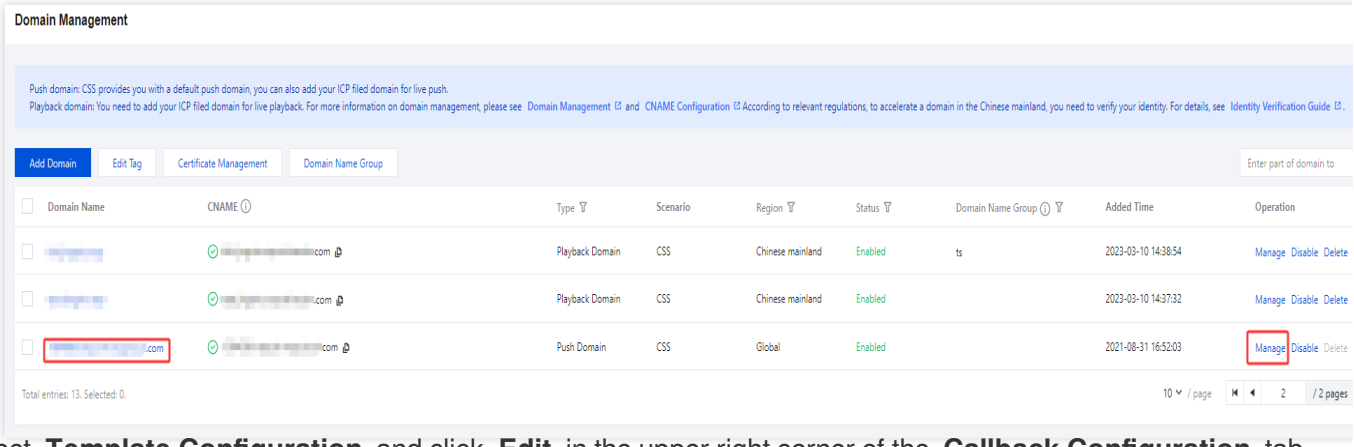


3. Select the corresponding callback template, and click **Confirm** .

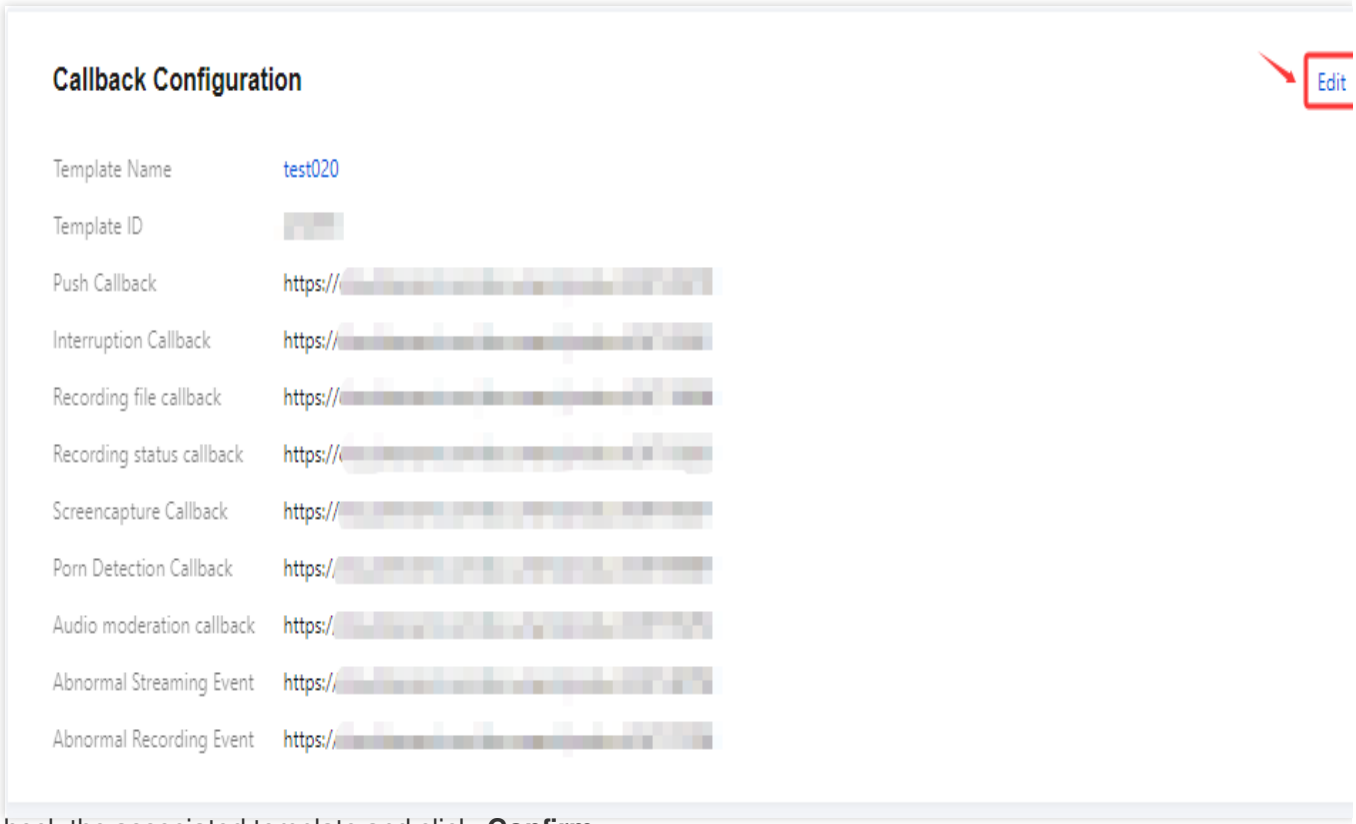


Unbinding Callback Template

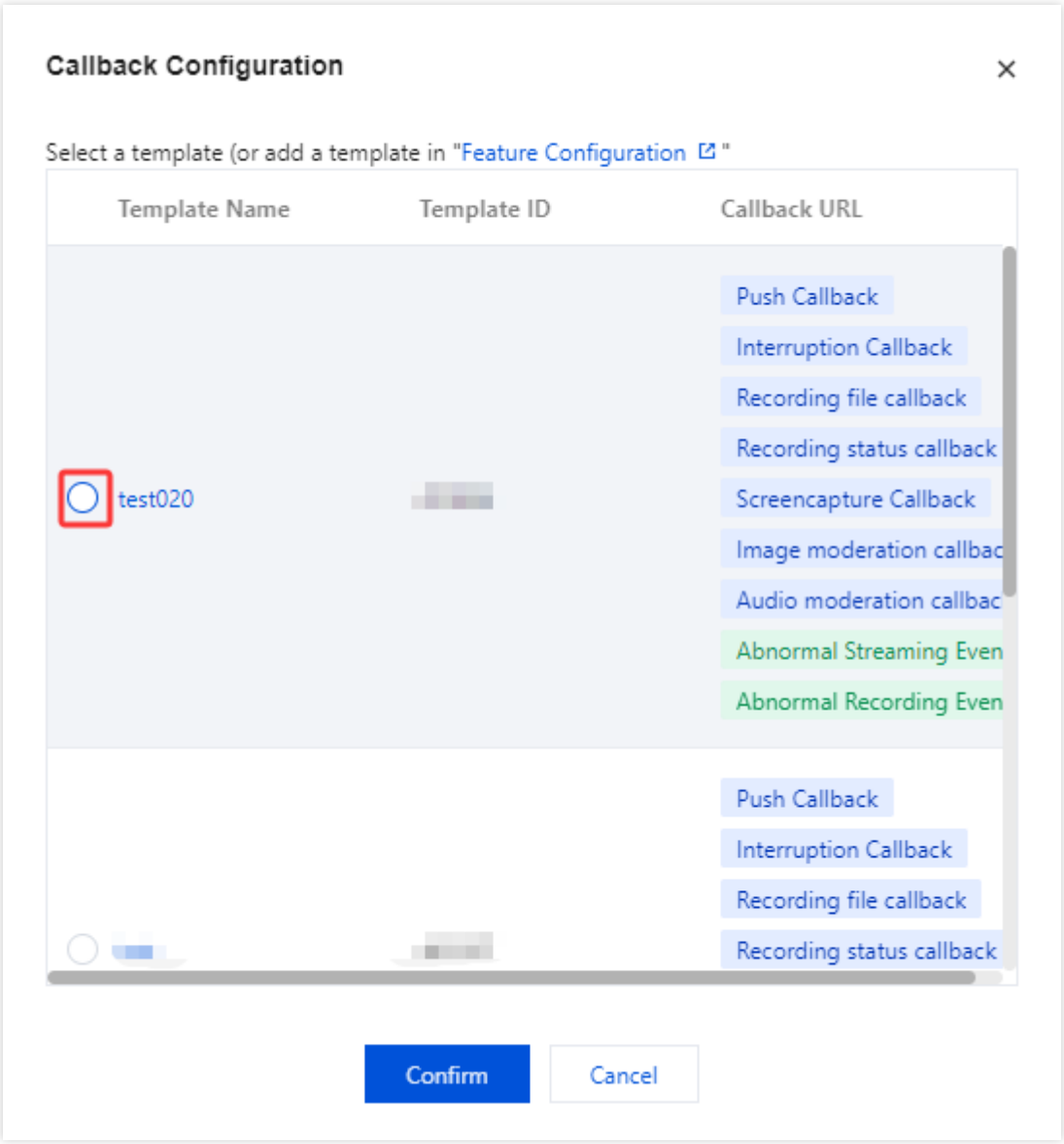
1. Go to Domain Management, and click the target **push domain name** or **Manage** to enter the domain details page.



2. Select **Template Configuration** and click **Edit** in the upper right corner of the **Callback Configuration** tab.



3. Uncheck the associated template and click **Confirm** .


Callback Configuration
Select a template (or add a template in "Feature Configuration ")
Template Name
Template ID
Callback URL
test020
Push Callback
Interruption Callback
Recording file callback
Recording status callback
Screencapture Callback
Image moderation callbac
Audio moderation callbac
Abnormal Streaming Even
Abnormal Recording Even
Push Callback
Interruption Callback
Recording file callback
Recording status callback
Confirm
Cancel

Standby Stream Configuration

Last updated：2024-05-07 19:04:45

This document shows you how to bind a standby stream template to a push domain to enable the standby stream feature for that domain, as well as how to unbind a template to disable the feature. The standby stream feature is disabled by default.

Notes

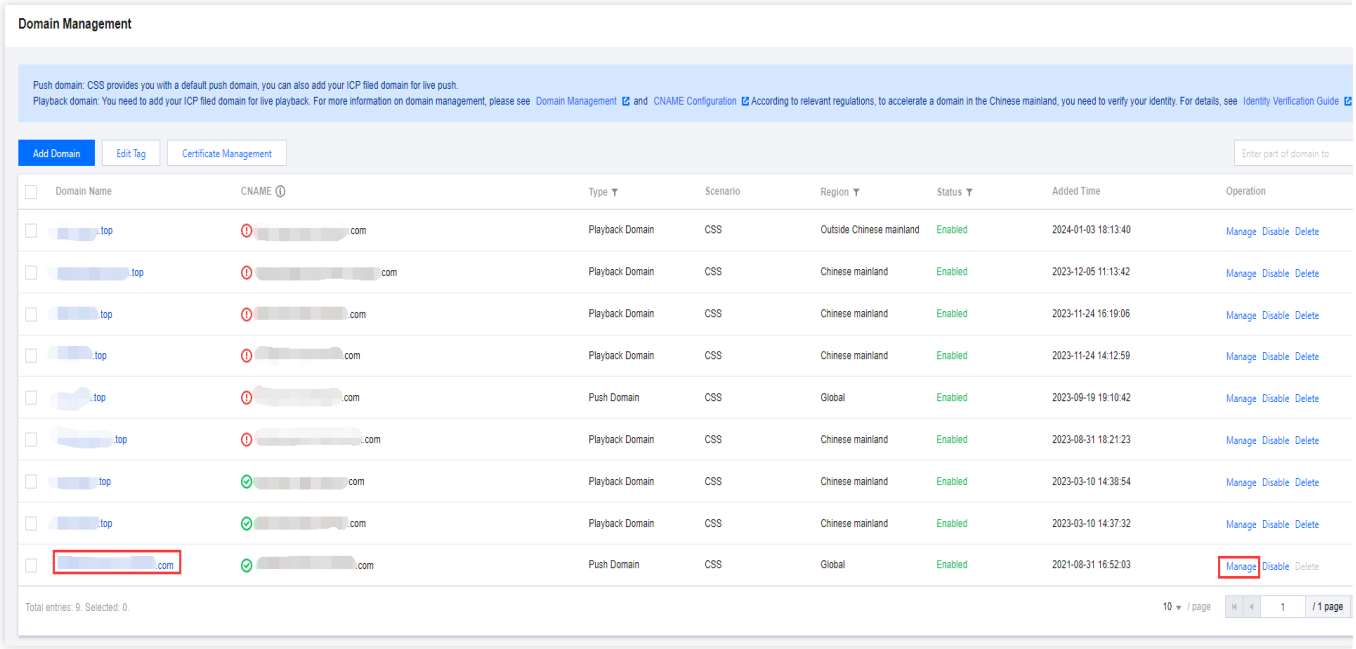
A template takes effect about 5-10 minutes after it is bound to a domain.
After a template is successfully bound to a push domain, the standby stream configured will take effect for all push addresses under that domain.

Prerequisites

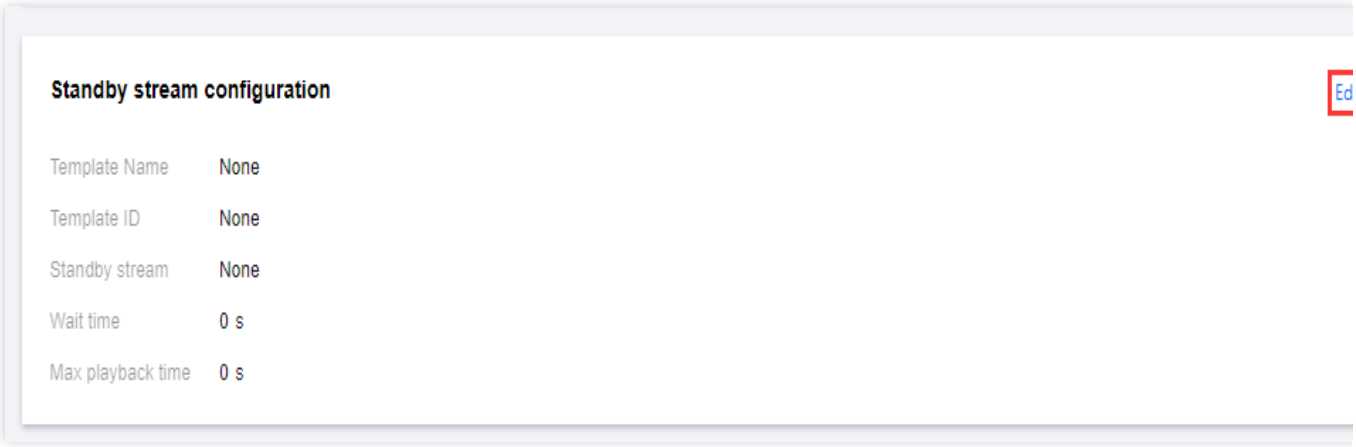
You have logged in to the CSS console and added a push domain.
You have created a standby stream template.

Binding a Standby Stream Template

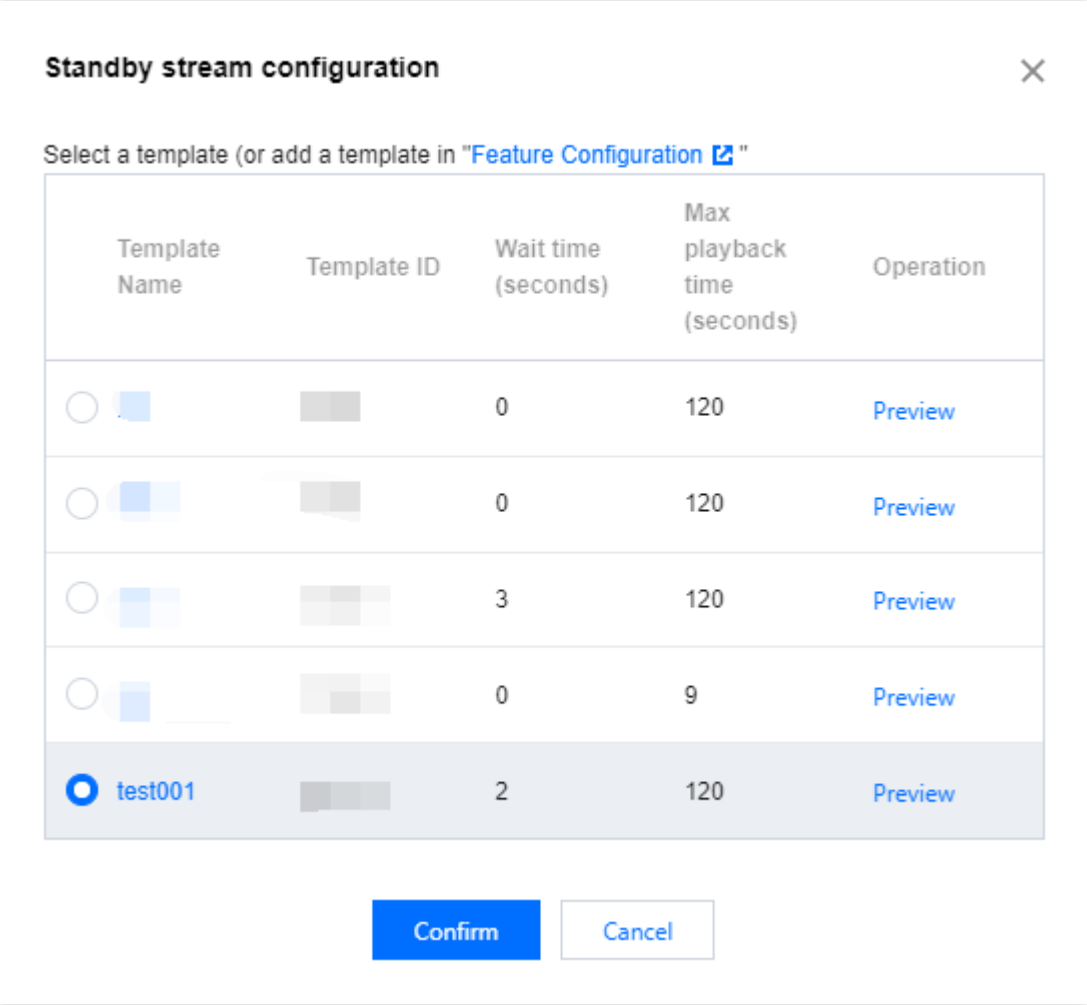
1. Go to Domain Management, and click the target **push domain** or click **Manage** to enter the domain details page.



2. Select the **Template Configuration** tab and click **Edit** in the **Standby stream configuration** area.



3. Select a standby stream template and click **Confirm**.

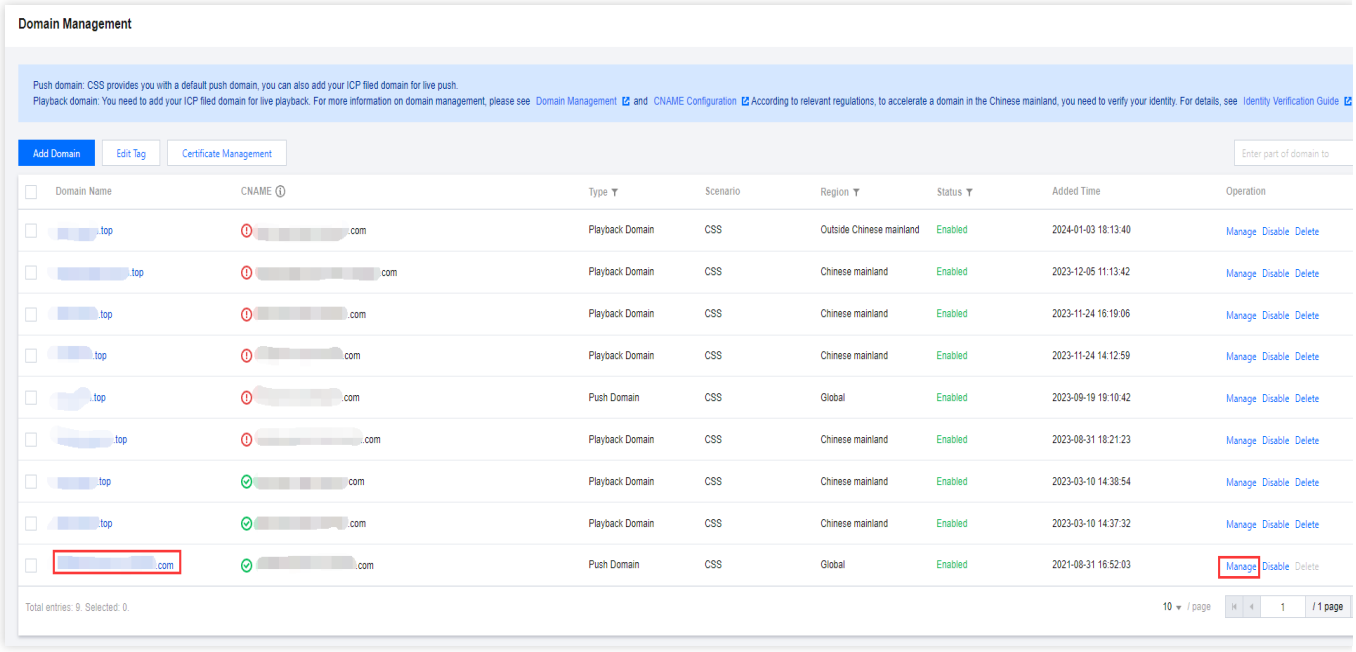


Note:

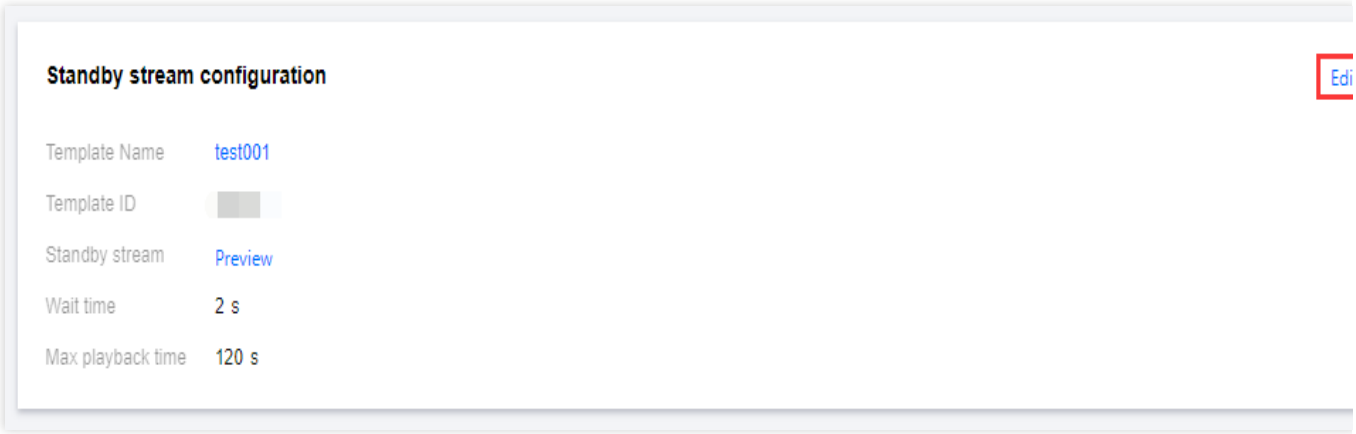
You can click **Preview** in the **Operation** column to preview the standby stream.

Unbinding a Standby Stream Template

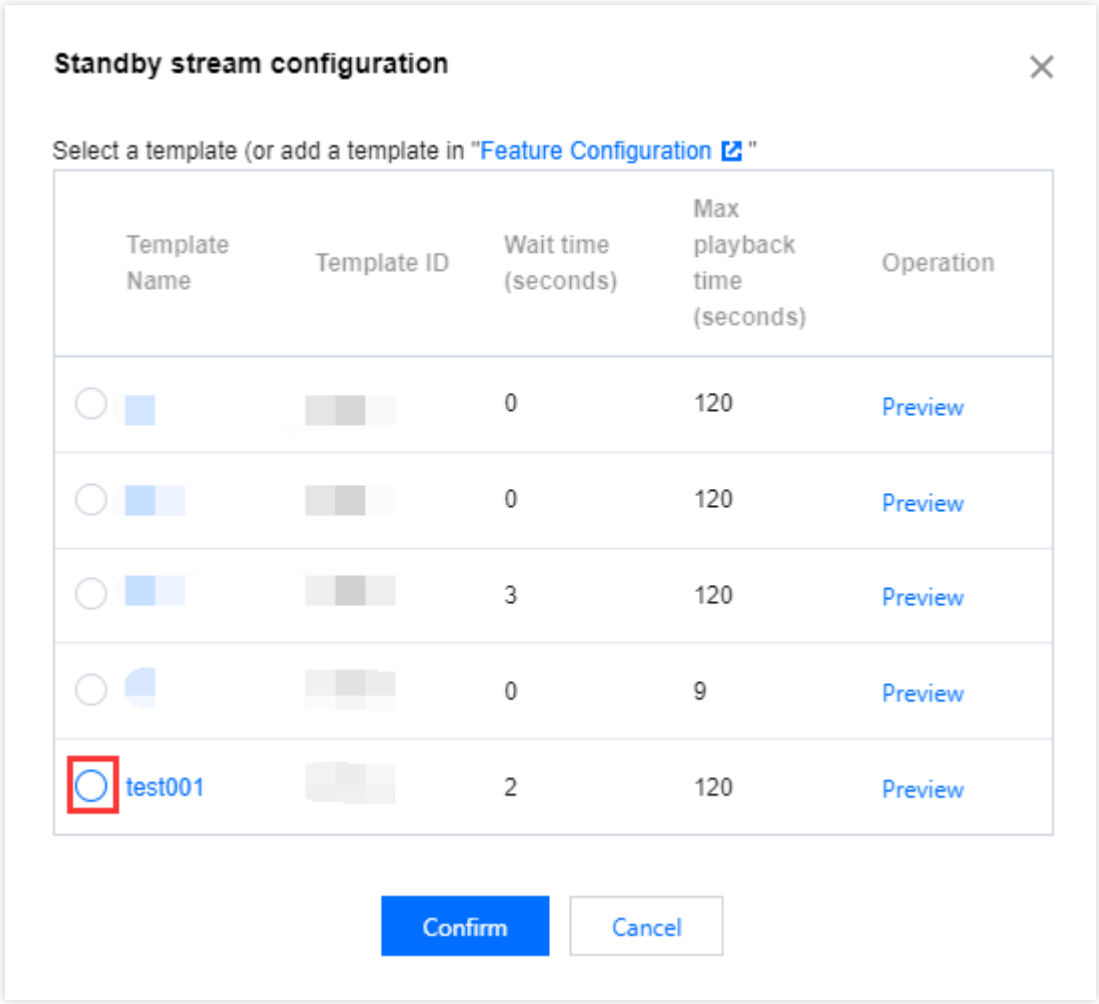
1. Go to Domain Management, and click the target **push domain** or click **Manage** to enter the domain details page.



2. Select the **Template Configuration** tab and click **Edit** in the **Standby stream configuration** area.



3. Unselect the template and click **Save**.


Standby stream configuration
Select a template (or add a template in "Feature Configuration ")
Template Name
Template ID
Wait time (seconds)
Max playback time (seconds)
Operation
0
120
Preview
0
120
Preview
3
120
Preview
0
9
Preview
test001
2
120
Preview
Confirm
Cancel

Latency Control

Last updated：2024-05-28 10:29:07

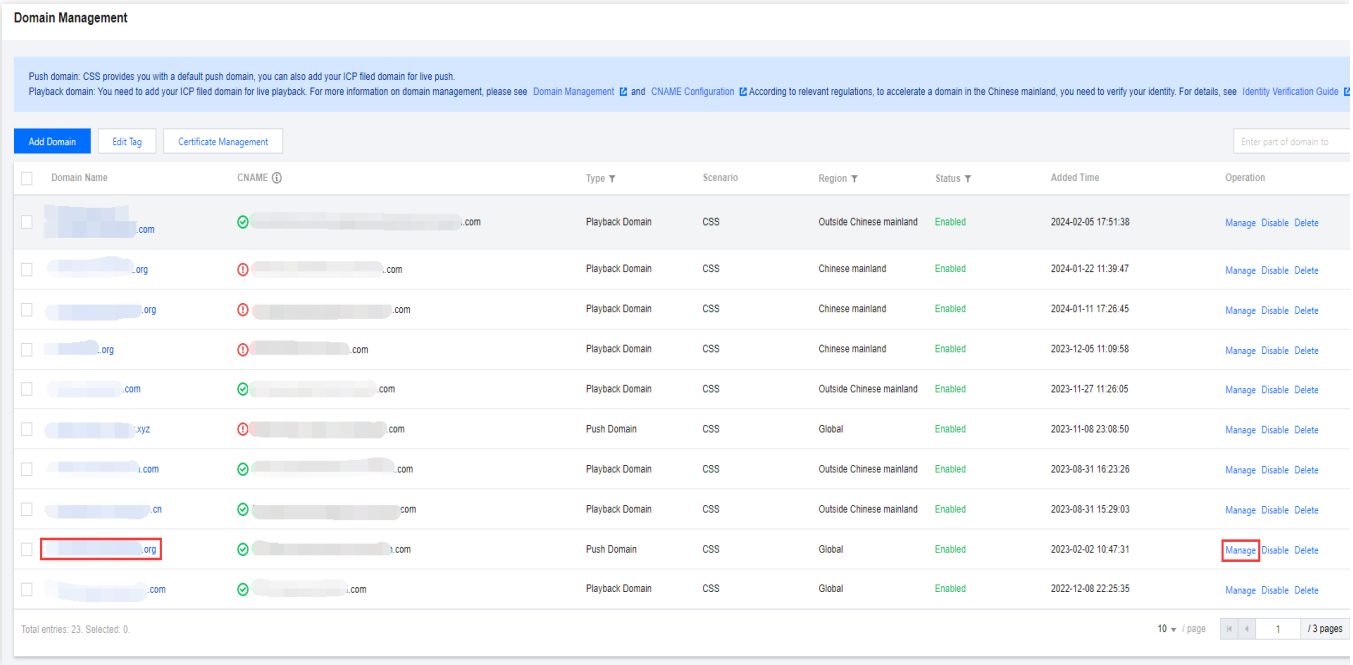
It is possible to control the latency of HLS playback by adjusting the size and number of HLS segments. Note that setting the latency too low may cause playback to stutter.

Prerequisites

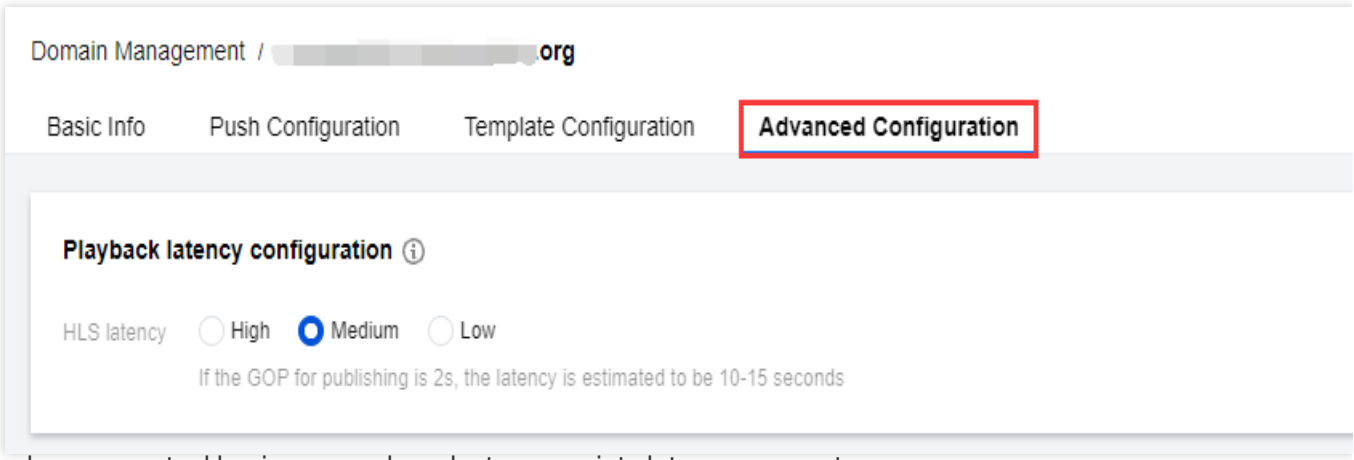
You have activated CSS and logged in to the CSS console.
You have added a push domain name.

Latency control

1. Select Domain Management on the left sidebar and click the target **push domain** or click **Manage** on the right to enter the details page.



2. In **Advanced Configuration** > **Playback latency configuration** , you can configure the latency for HLS.



3. Based on your actual business needs, select appropriate latency parameters.

Select different configurations, corresponding to HLS segments configurations, high for 5 seconds * 4 segments, medium for 4 seconds * 3 segments, and low for 2 seconds * 3 segments. The actual slice duration is related to the GOP length. Each TS should contain at least one GOP. It is recommended to set the push stream GOP to 1s ~ 2s.

4. When GOP is set to two seconds, the latency is as follows:

Setting	High	Medium	Low
Estimated Latency	20-25s	10-15s	6-8s

IP Blocklist/Allowlist Configuration

Last updated：2024-05-16 17:26:18

This document shows you how to configure an IP allowlist/blocklist to filter requests and control access to streaming content.

How It Works

IP **allowlist**: Only the configured IP addresses are allowed to push streams to Cloud Streaming Services.
IP **blocklist**: Only the configured IP addresses are restricted from pushing streams to Cloud Streaming Services.

Reminders

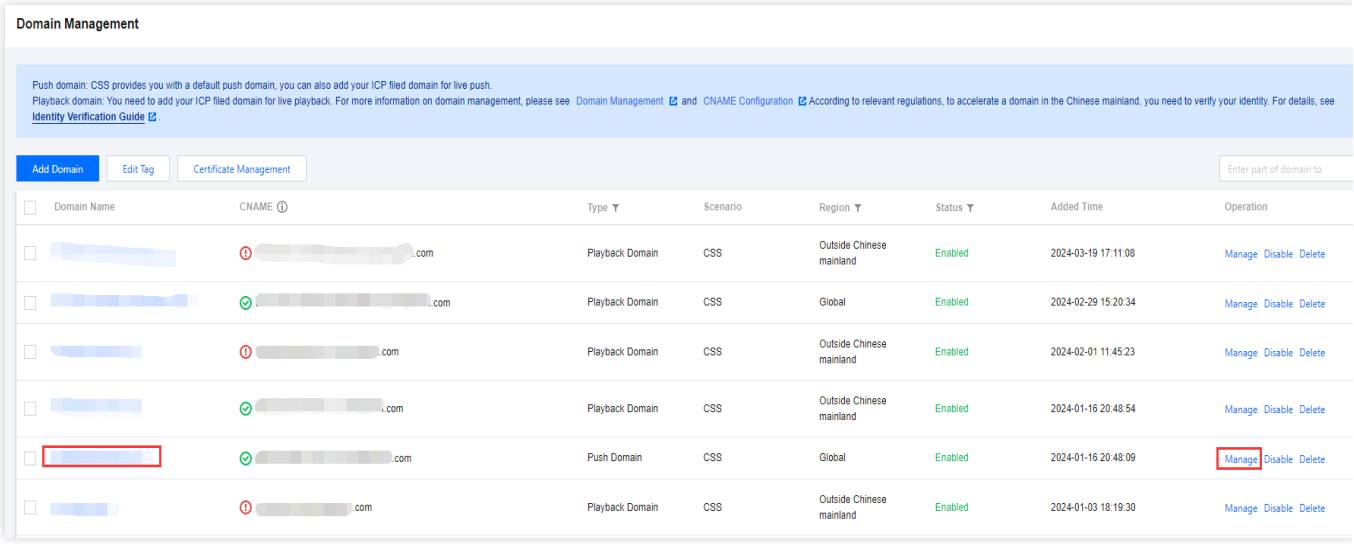
An IP allowlist/blocklist takes effect about ten minutes after configuration.
For an IP allowlist/blocklist configuration to apply to ongoing streams, you need to restart the streams.

Prerequisites

You have activated CSS and logged in to the CSS console.
You have added a push domain.

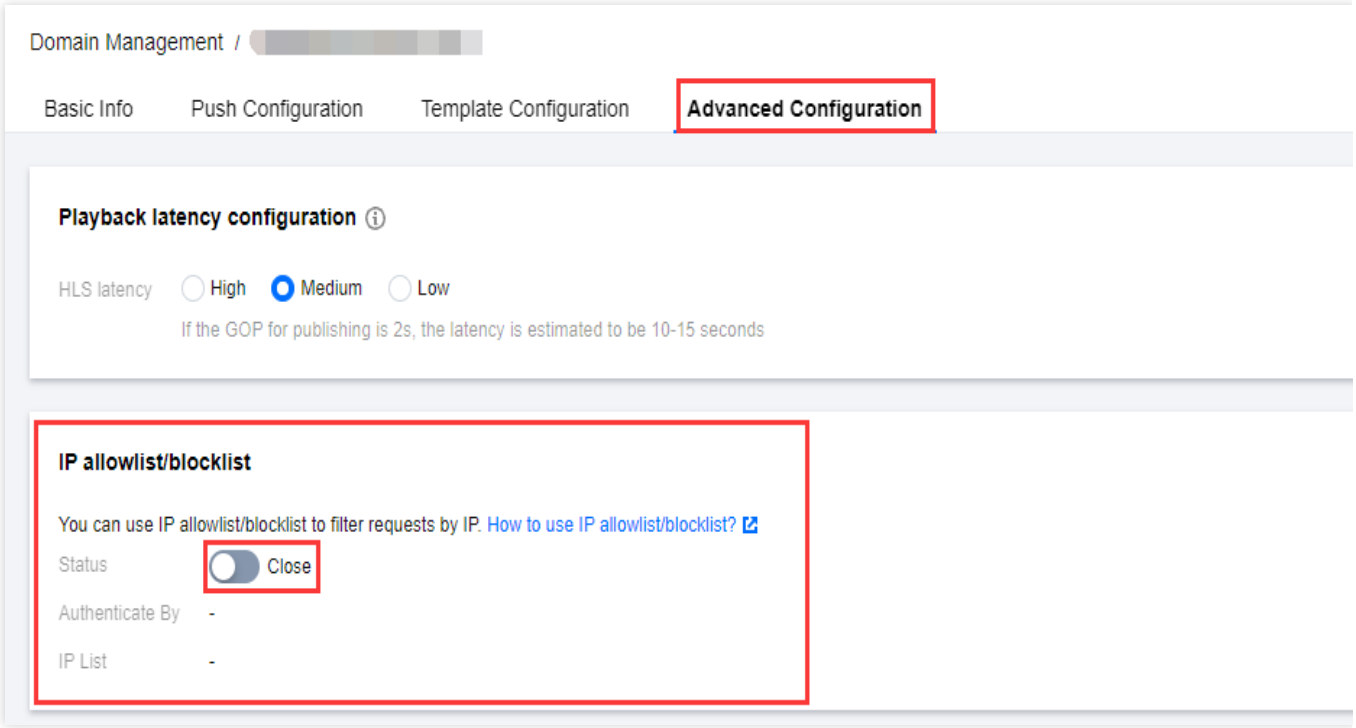
Configuring an IP Allowlist/Blocklist

1. Select Domain Management on the left sidebar. Click the name of the target playback domain or click **Manage** on the right to enter the domain management page.



2. Within the **Advanced Configuration**> **IP allowlist/blocklist**, click on

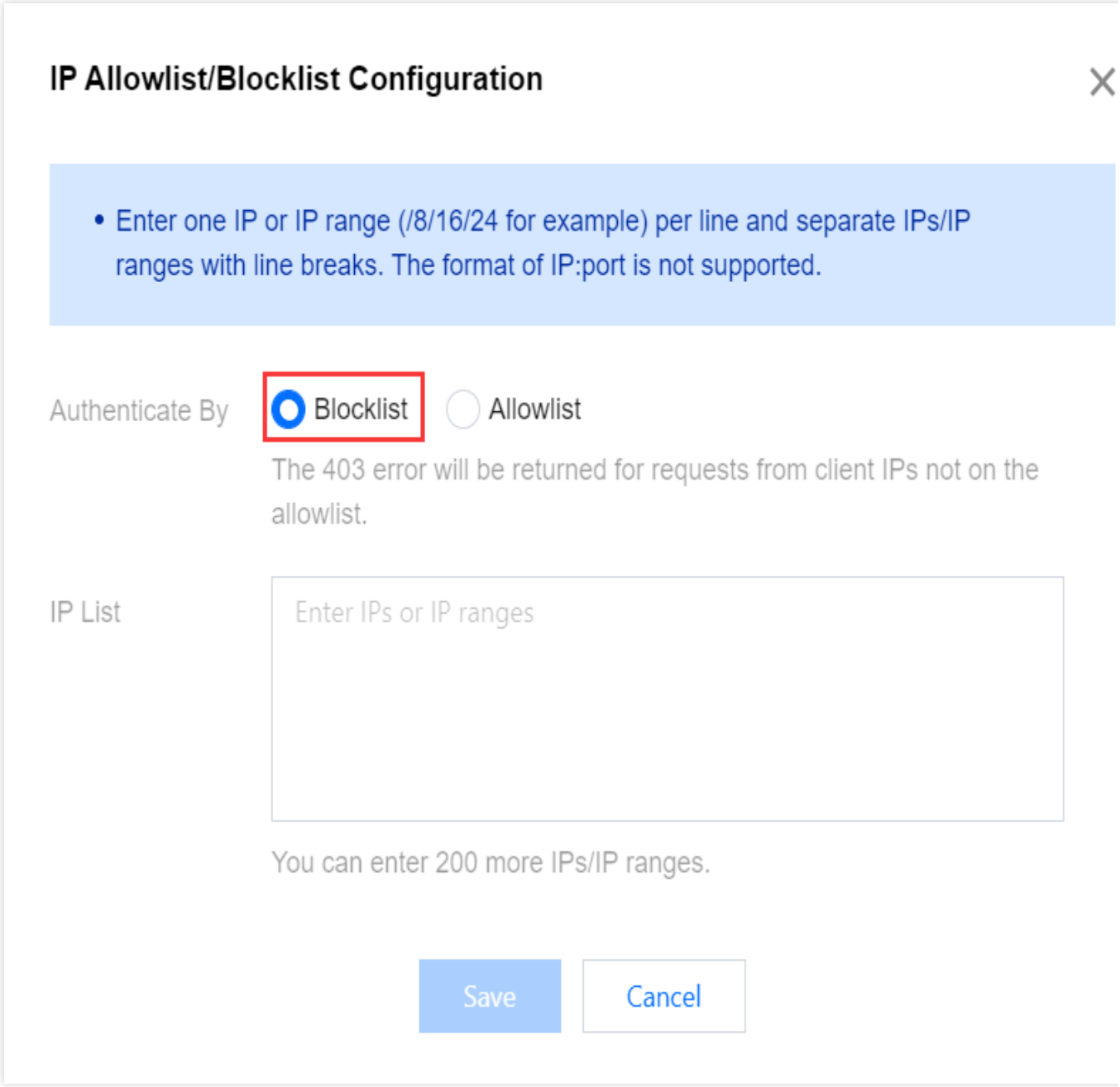
to enable the IP Allowlist/Blocklist.

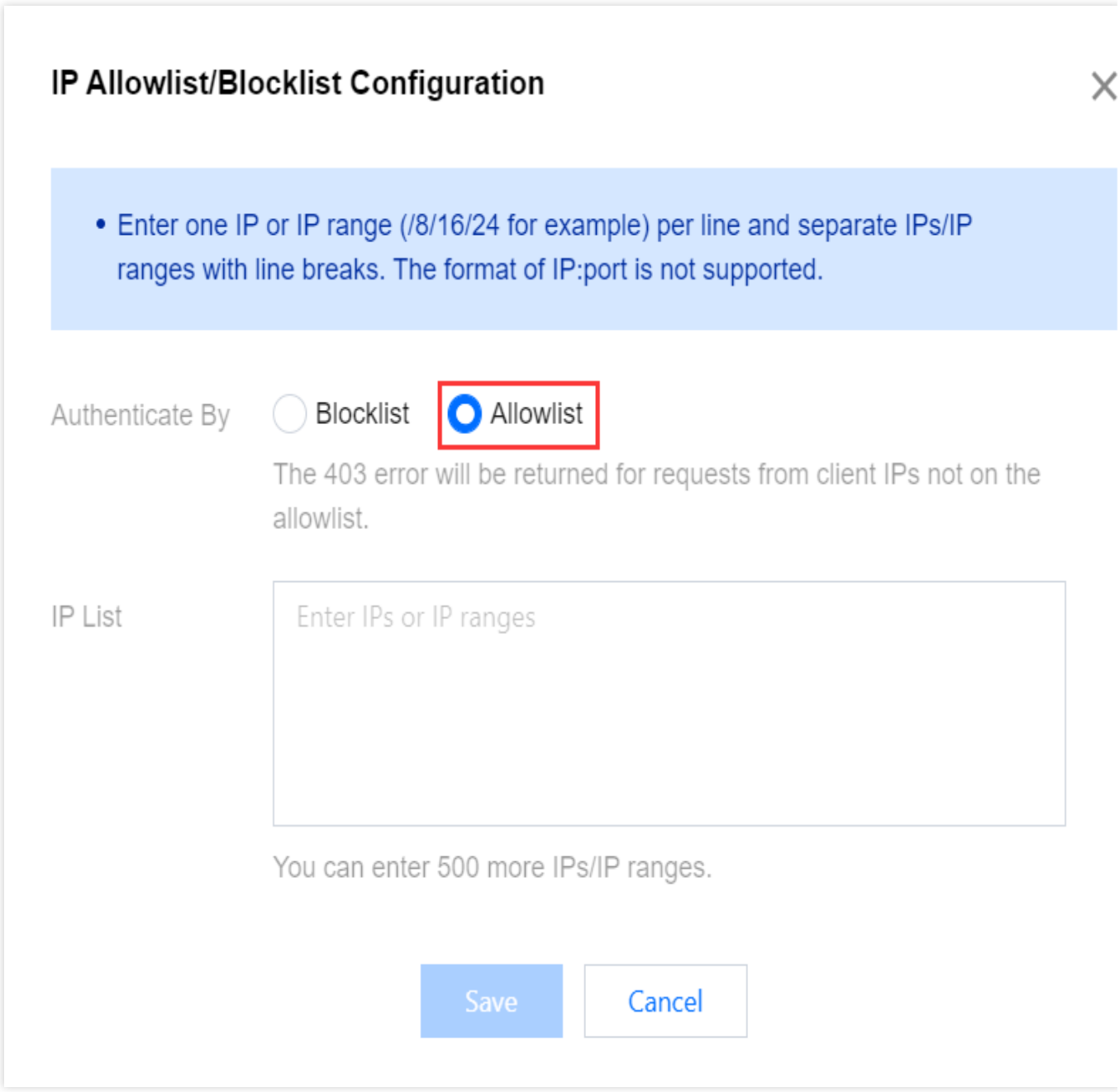


3. After enabling the **IP Allowlist/Blocklist** , enter the **IP Allowlist/Blocklist** configuration page and perform the following configuration:

Blocklist

Allowlist

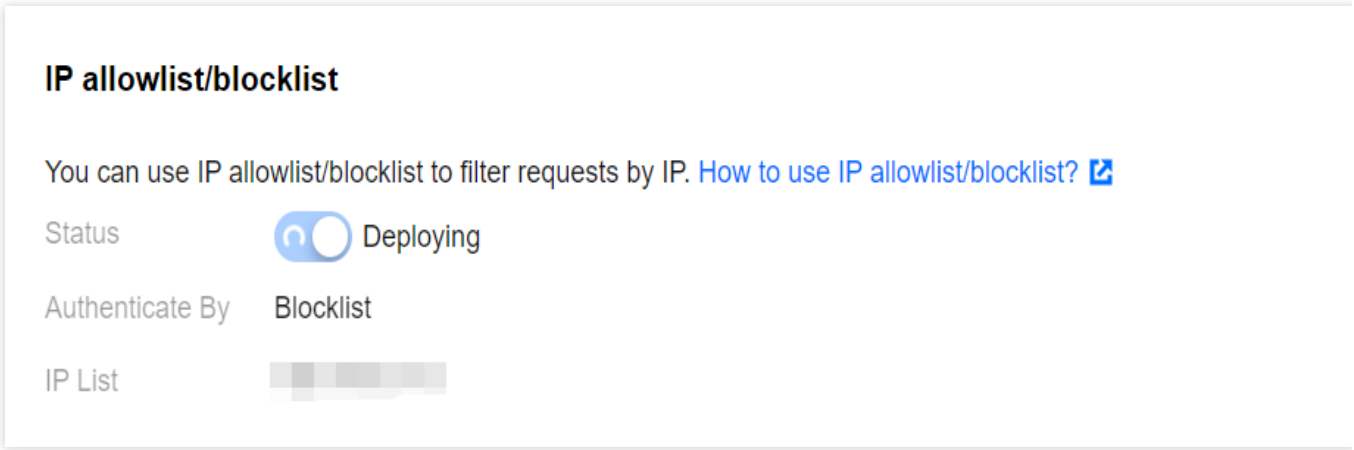

IP Allowlist/Blocklist Configuration
• Enter one IP or IP range (/8/16/24 for example) per line and separate IPs/IP ranges with line breaks. The format of IP:port is not supported.
Authenticate By
Blocklist
Allowlist
The 403 error will be returned for requests from client IPs not on the allowlist.
IP List
Enter IPs or IP ranges
You can enter 200 more IPs/IP ranges.
Save
Cancel



Configuration Item	Description
Authenticate By	Allowlist or blocklist: You cannot select both. If you configure an allowlist, only IP addresses on the list will be able to access your streaming content. If you configure a blocklist, IP addresses on the list cannot access your streaming content.
IP List	The IP blocklist supports a maximum configuration of 200 rules, and the IP allowlist supports up to 500 rules. Please separate entries with a newline character.

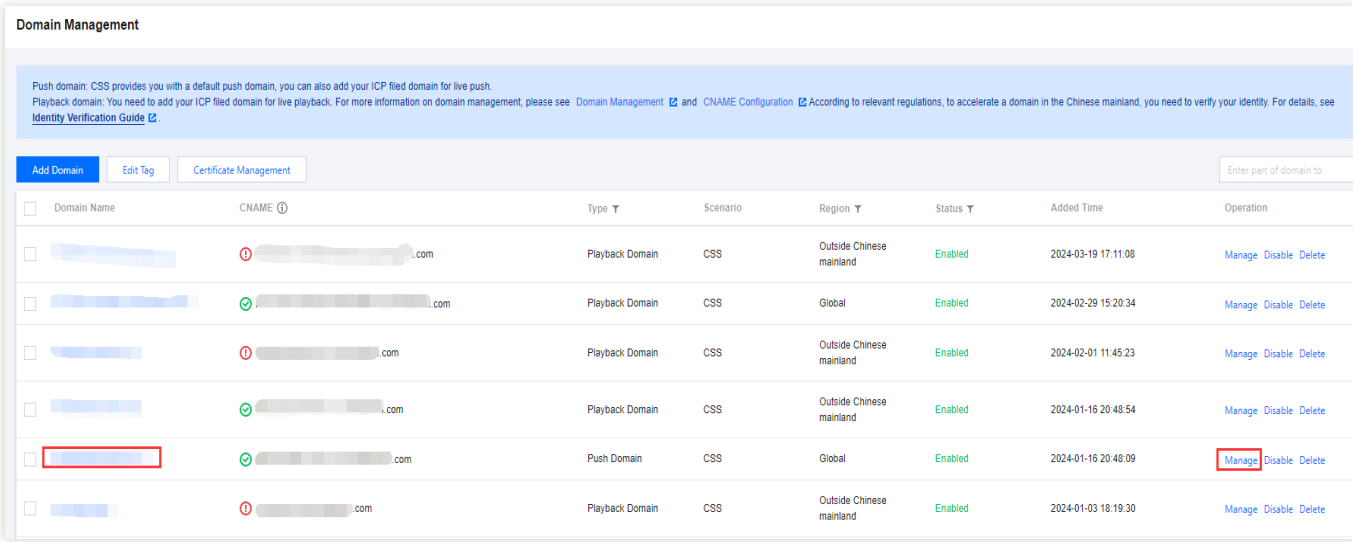
	You can enter IP addresses or IP ranges (/8/16/24). The “IP address: port number” format is not supported. IPv6 is not supported currently.

4. Click **Save** to save the configuration (it takes a while for the configuration to take effect).

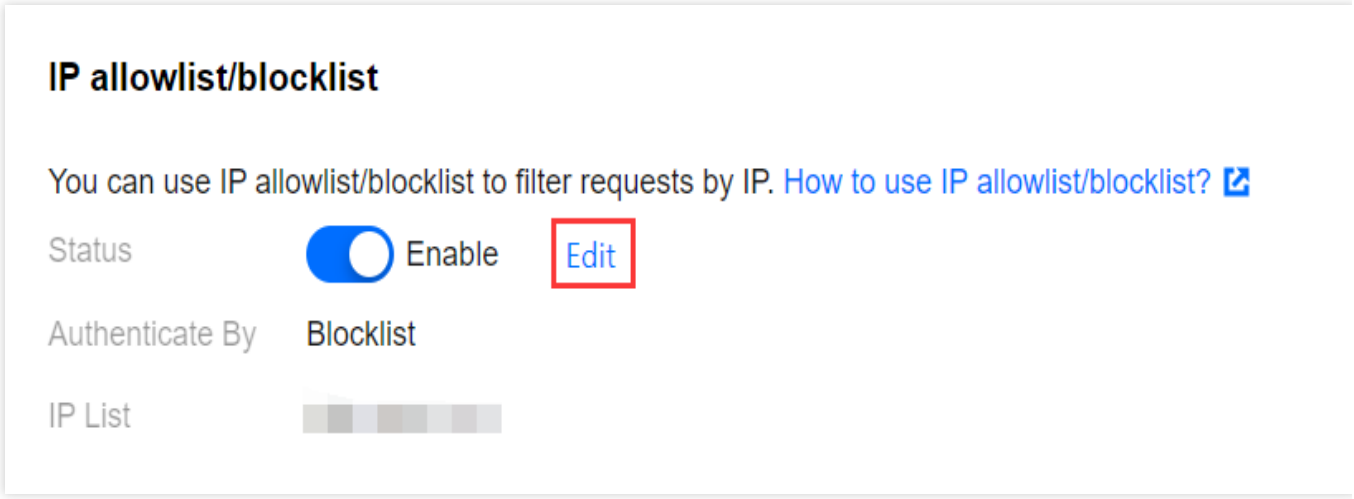


Modifying an IP Allowlist/Blocklist

1. Select Domain Management on the left sidebar. Click the name of the target playback domain or click **Manage** on the right to enter the domain management page.



2. Select the **Access Control** tab. In the **IP allowlist/blocklist** area, click **Edit**.

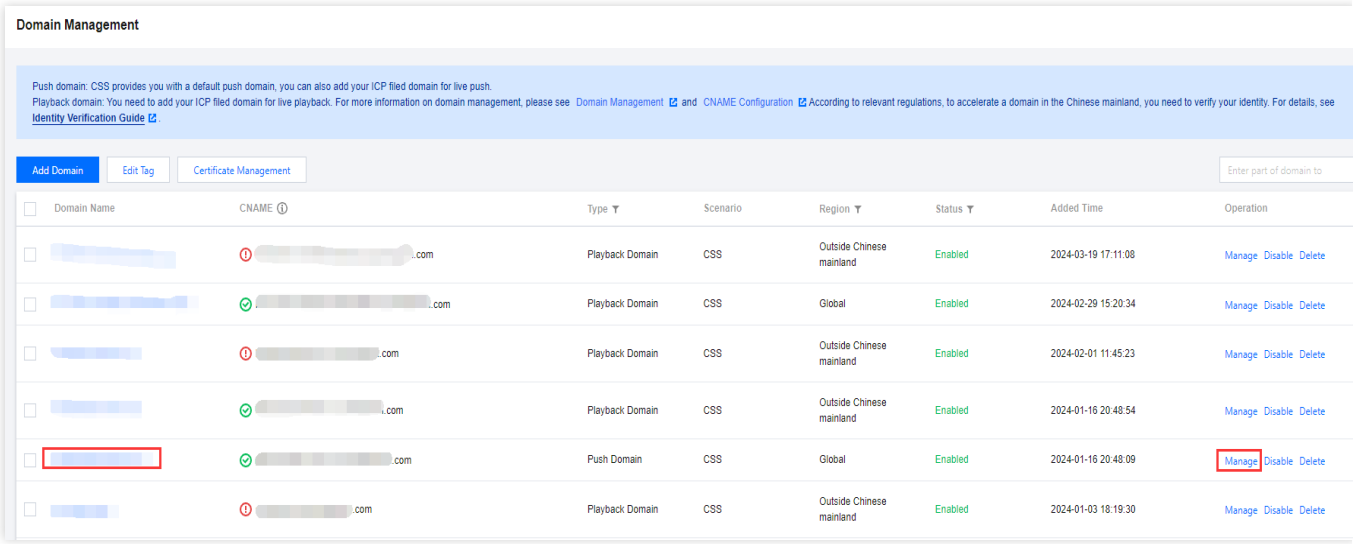


3. Modify the configuration and click **Save**.

Disabling IP Allowlist/Blocklist

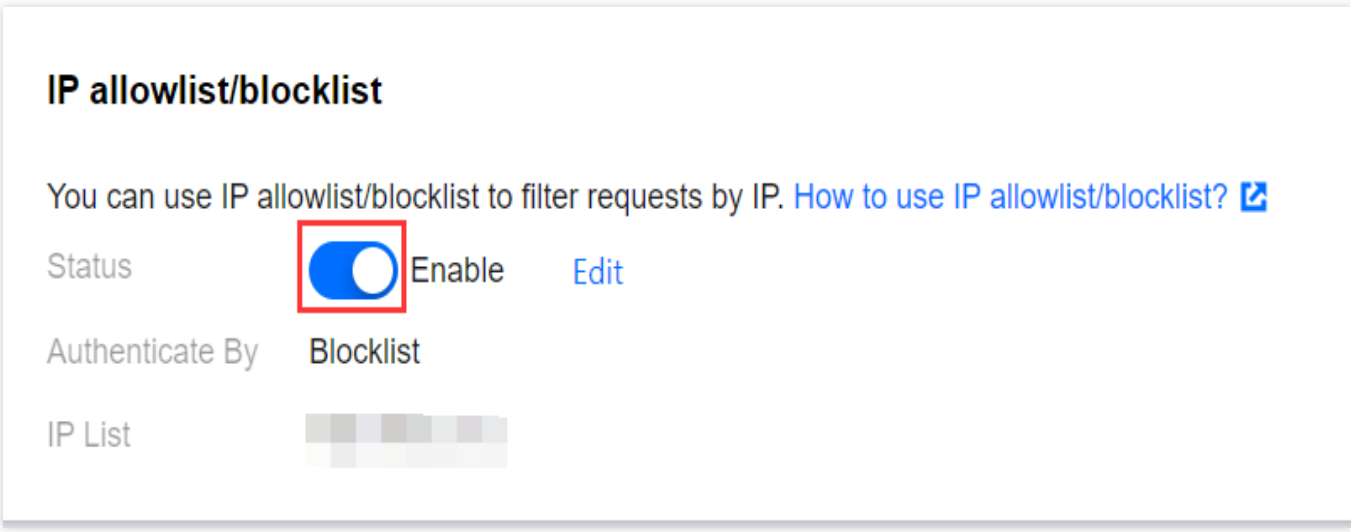
Follow the steps below to disable IP allowlist/blocklist:

1. Select Domain Management on the left sidebar. Click the name of the target playback domain or click **Manage** on the right to enter the domain management page.



2. Select the **Access Control** tab. In the **IP allowlist/blocklist** area, click

to disable IP allowlist/blocklist.


IP allowlist/blocklist
You can use IP allowlist/blocklist to filter requests by IP. How to use IP allowlist/blocklist?
Status
Enable
Edit
Authenticate By
Blocklist
IP List

Delayed Playback

Last updated：2024-08-27 10:34:59

Delayed playback is a feature that processes streams in the cloud, enabling the playback end to operate with a set delay. This delay is distinct from the inherent delay of the protocol itself. Delayed playback is applicable to significant live steaming events. To prevent unforeseen circumstances during the events, if you need to prepare control and response measures in advance, you can configure this feature directly through the console. For instance, during the live streaming of a large-scale evening party, if you set a delay of 5 minutes in advance, the online audience will see the picture 5 minutes later than the actual event. In case of an unexpected incident, the director will have a 5-minute pre-processing time period to switch machine positions or backup streams through the director's console, thereby mitigating live streaming risks.

Notes

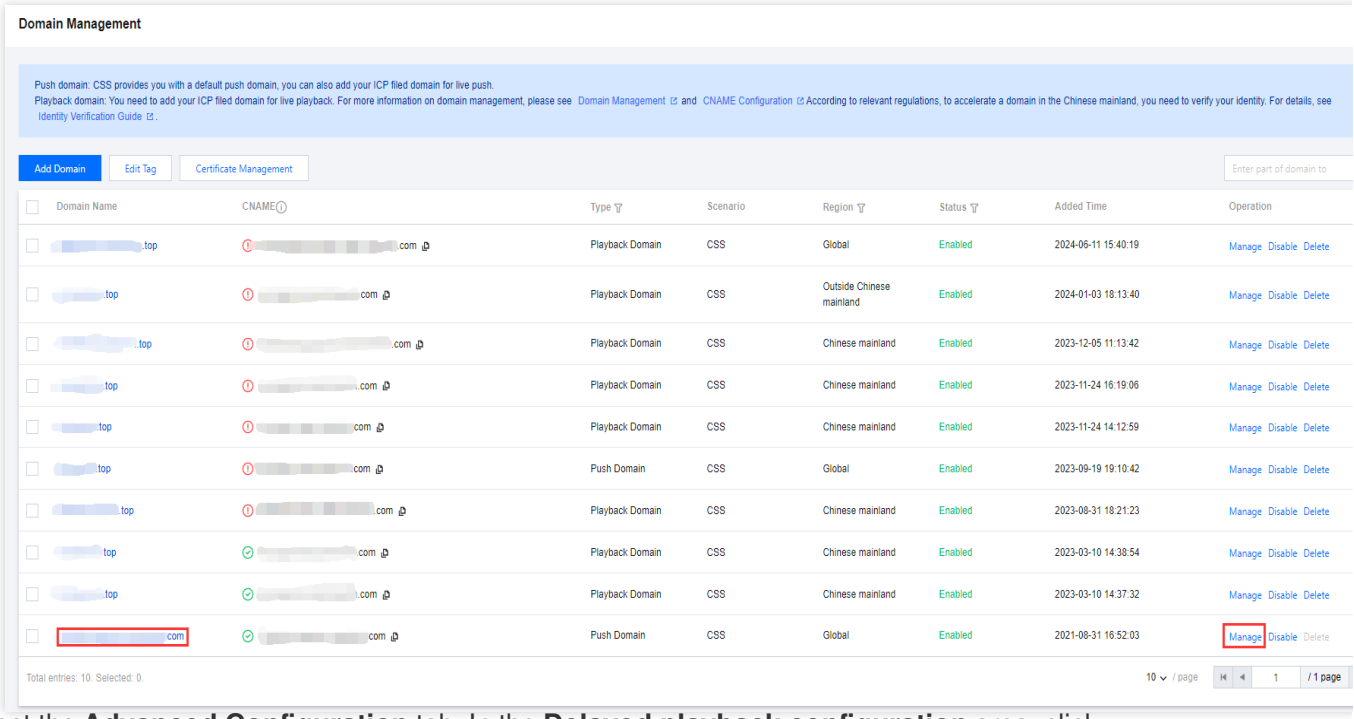
You can enable delayed playback via three methods:
Configure it in the Cloud Streaming Services (CSS) console.
Call the playback delaying API.
Add a `txDelayTime` parameter to the end of a push URL. For details, please see Push Configuration。
Delayed playback is a billing value-added service. To activate the delayed playback feature, use the console settings, call the delayed live streaming interface or carry the delayed playback parameter configuration with the push domain name. After successful push, the Value-added feature billing will be generated.
Note：
Currently, the API method is not recommended because calling an API involves configuration caching, which makes it difficult to estimate when the feature takes effect. You are advised to quickly enable the feature using the first or third method.
After enabling delayed playback, you need to add a delayed playback configuration in the console or using an API before the feature can take effect. After it takes effect, extended feature fees will be incurred for streams published.
Delayed playback will take effect after waiting for 5 minutes once the configuration is completed.

Prerequisites

You have activated the Cloud Streaming Services (CSS) and logged in to the CSS console.
You have added a push domain.

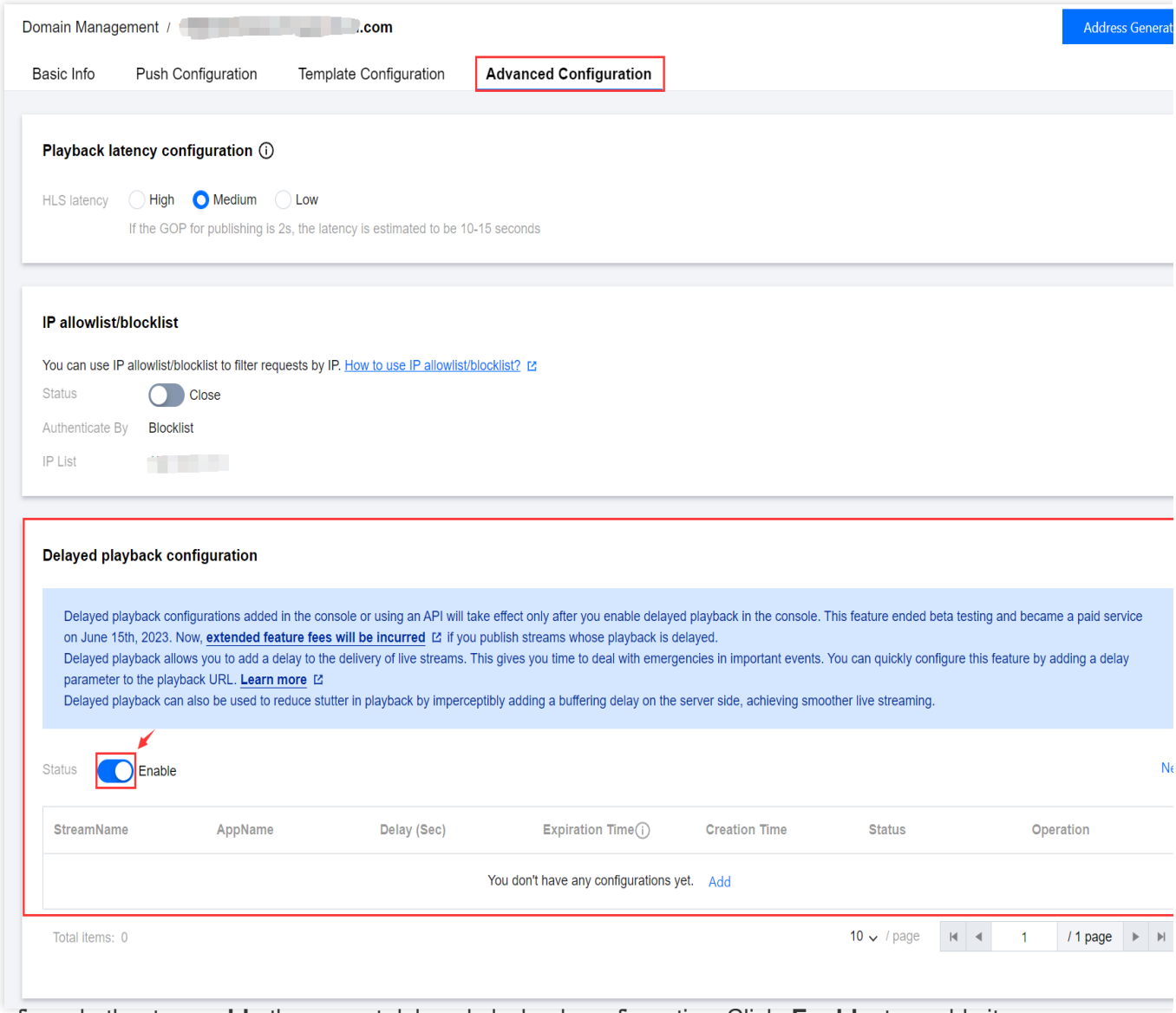
Configuring Delayed Playback

1. Go to Domain Management and click the **push domain** to be configured or click **Manage** on the right to enter the domain details page.

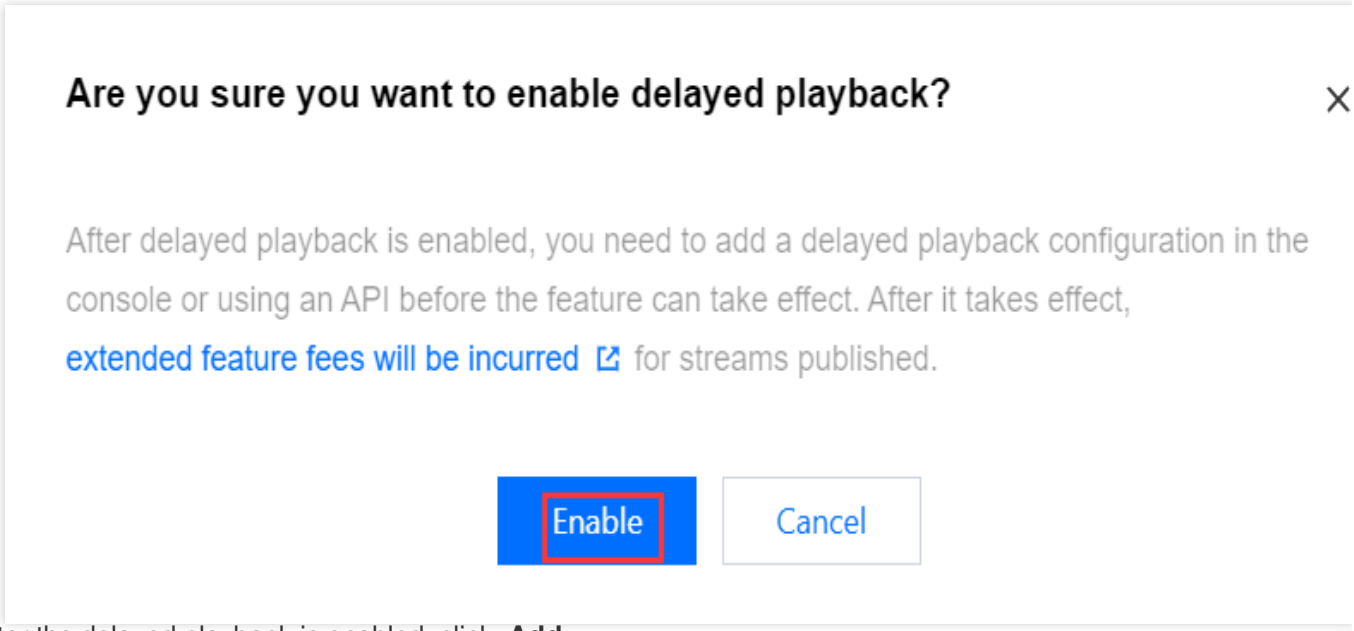


2. Select the **Advanced Configuration** tab. In the **Delayed playback configuration** area, click

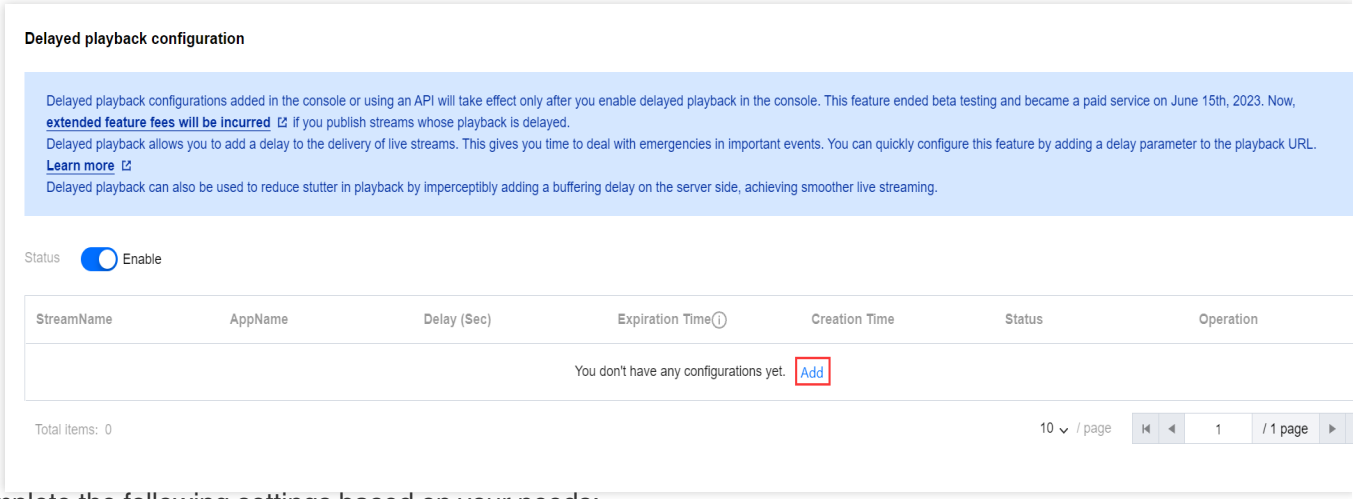
to enable the delayed playback configuration.



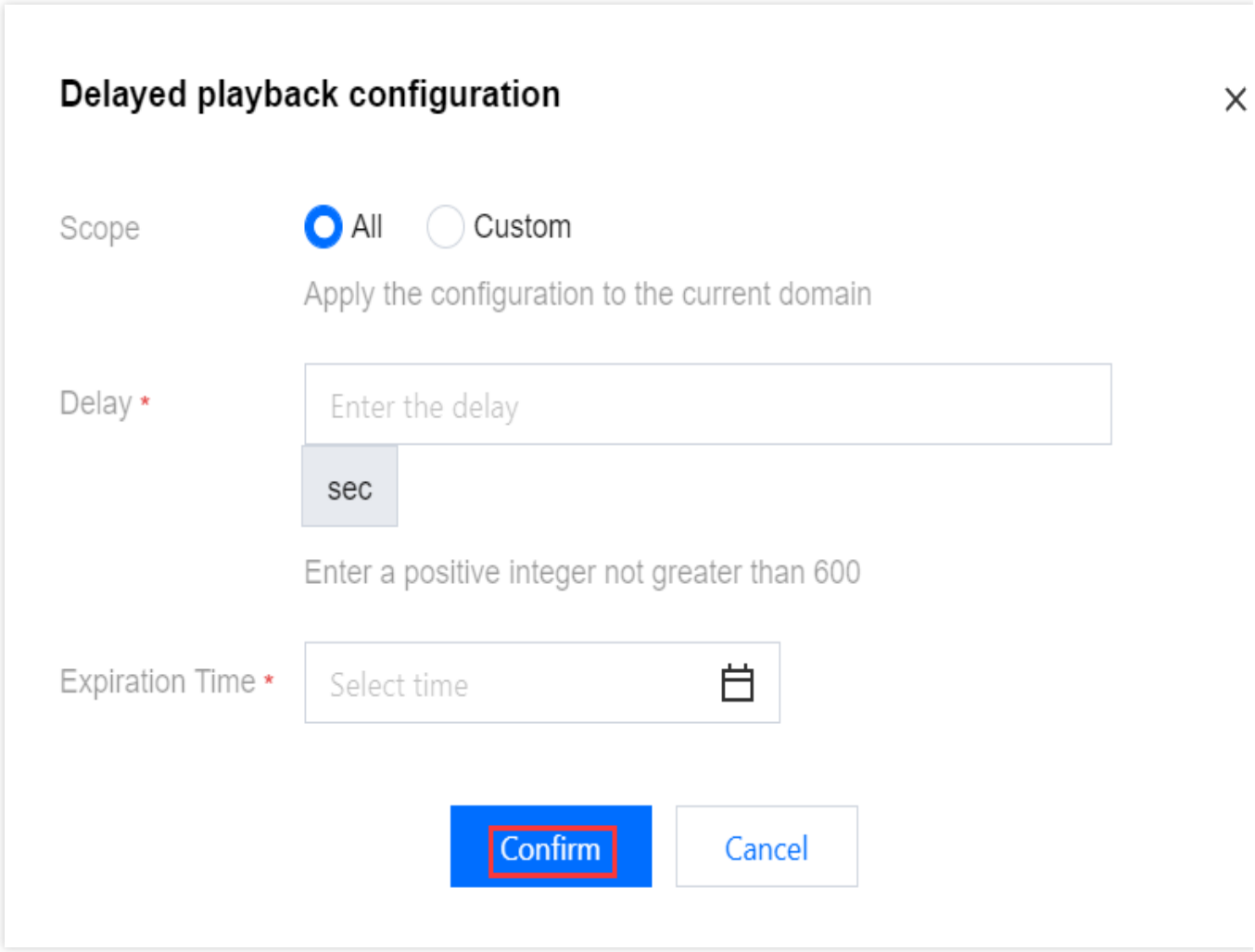
2.1 Confirm whether to **enable** the current delayed playback configuration. Click **Enable** to enable it.

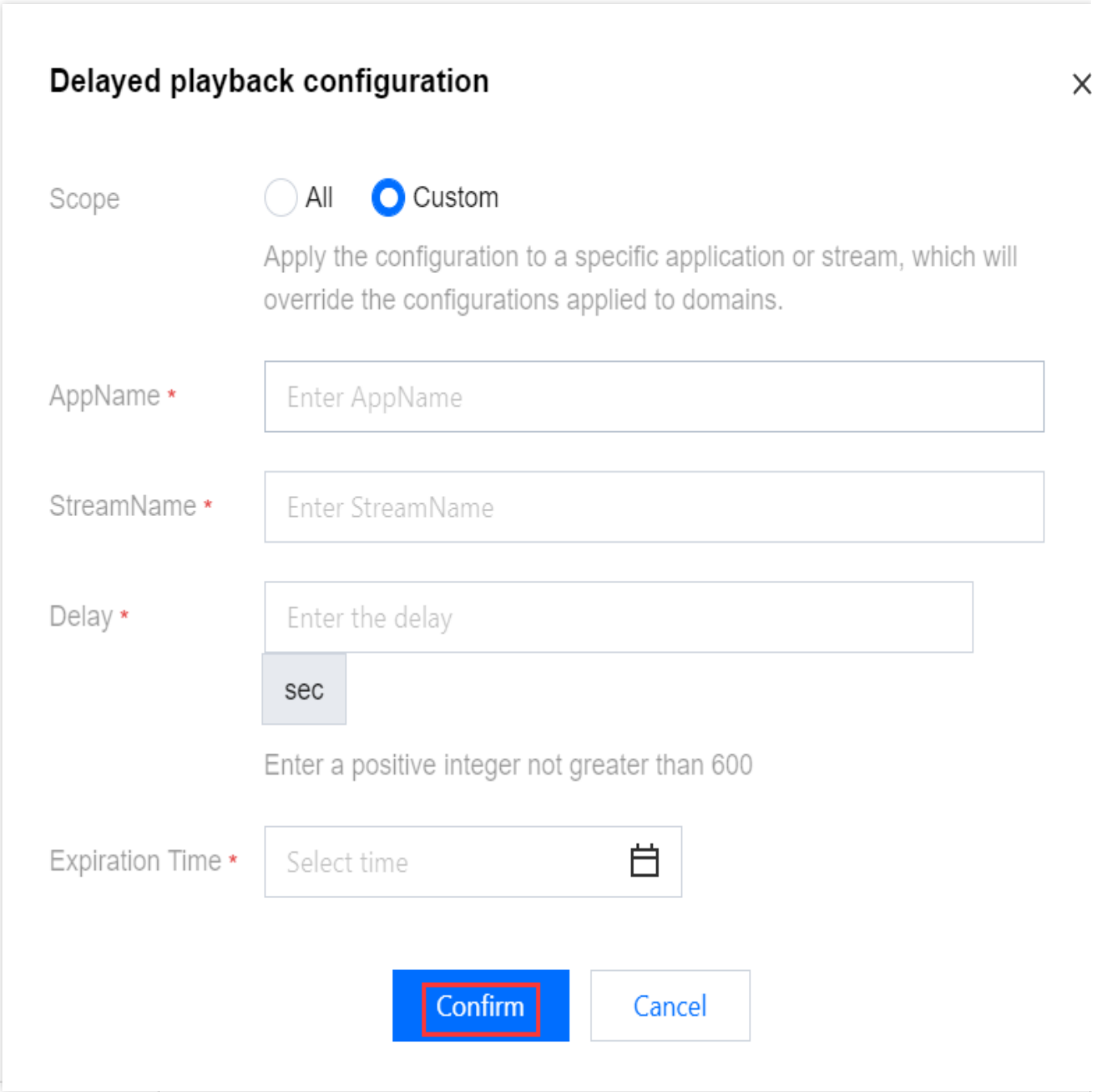


2.2 After the delayed playback is enabled, click **Add** .



3. Complete the following settings based on your needs:


Delayed playback configuration
Scope
All
Custom
Apply the configuration to the current domain
Delay *
Enter the delay
sec
Enter a positive integer not greater than 600
Expiration Time *
Select time
Confirm
Cancel

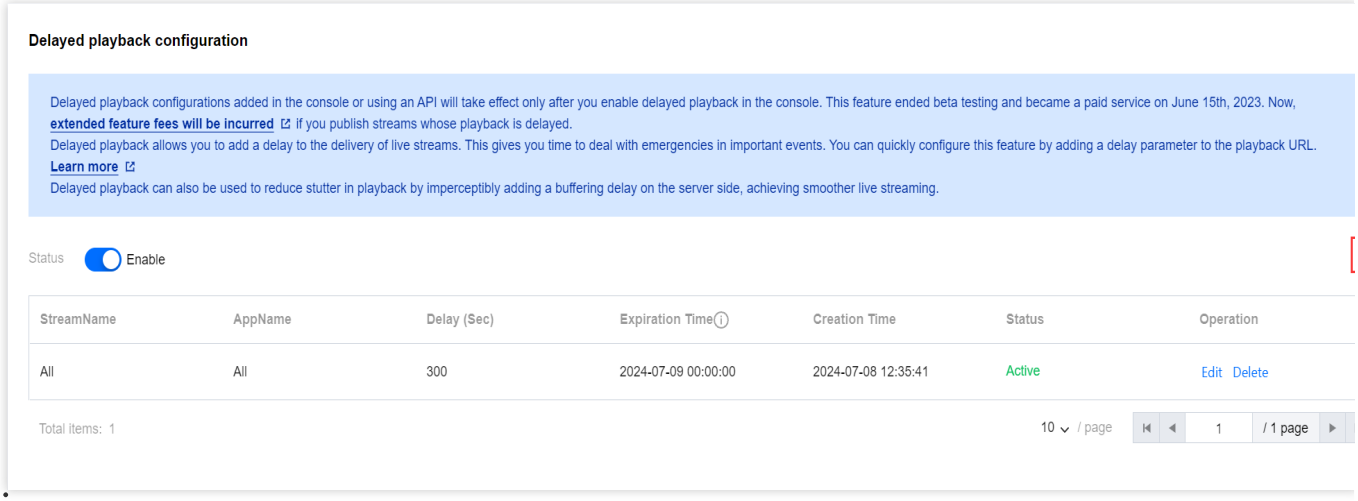


Configuration Item	Description
Scope	Select **All** or **Custom**: **All**: Apply the configuration to the current domain. **Custom**: Apply the configuration to a specific application or stream, which will override the configurations applied to **All**.
AppName	When there are configurations for the same AppName and StreamName, the most recently created configuration takes effect.
StreamName	When there are configurations for the same AppName and StreamName, the most recently created configuration takes effect.

Delay	A positive integer no greater than 600.
Expiration Time	The maximum selectable time is no more than 7 days from the current time.

3.1 Click **Confirm** to save the configuration.

3.2 Based on your actual business needs, click **New** on the right side to continue adding **Delayed playback configuration**.

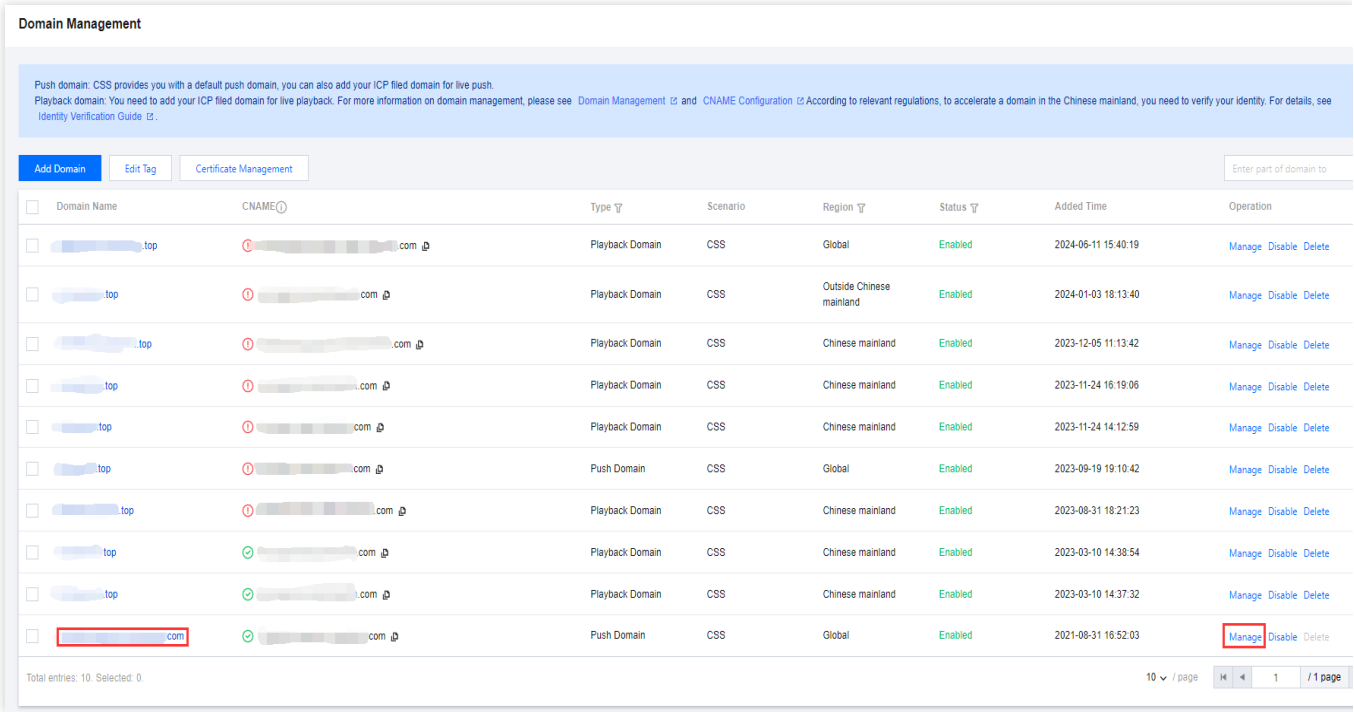


Note：

You can add up to 50 delayed playback configurations.

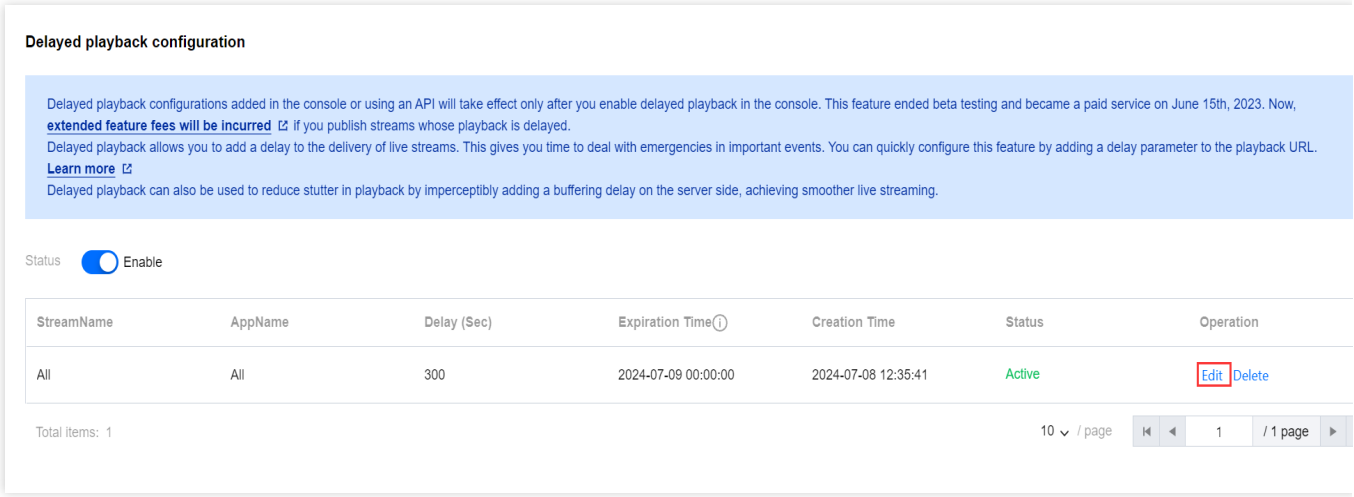
Modifying Delayed Playback Configuration

1. Select Domain Management, and click the **push domain** to be configured or click **Manage** on the right to enter the domain details page.



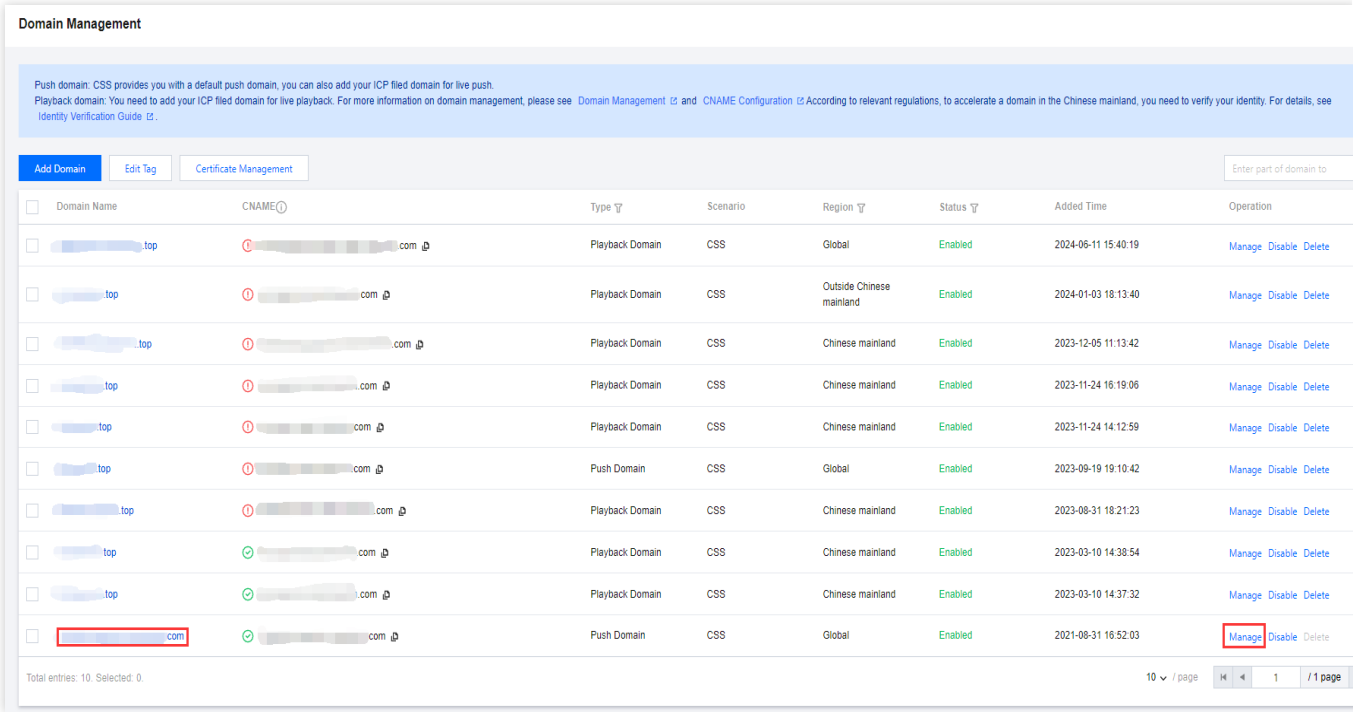
2. Select the **Advanced Configuration** tab. In the **Delayed playback configuration** area. Click **Edit** on the right side to enter the delayed playback configuration page.

3. Update the configurations based on your needs, and click **Confirm** to save the modifications.

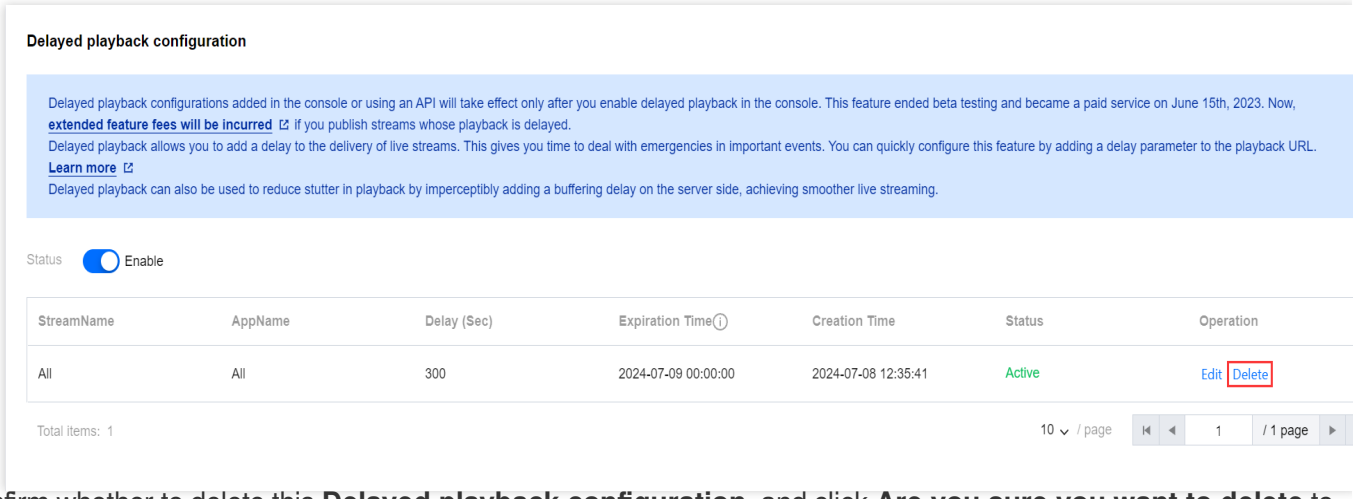


Deleting Delayed Playback Configuration

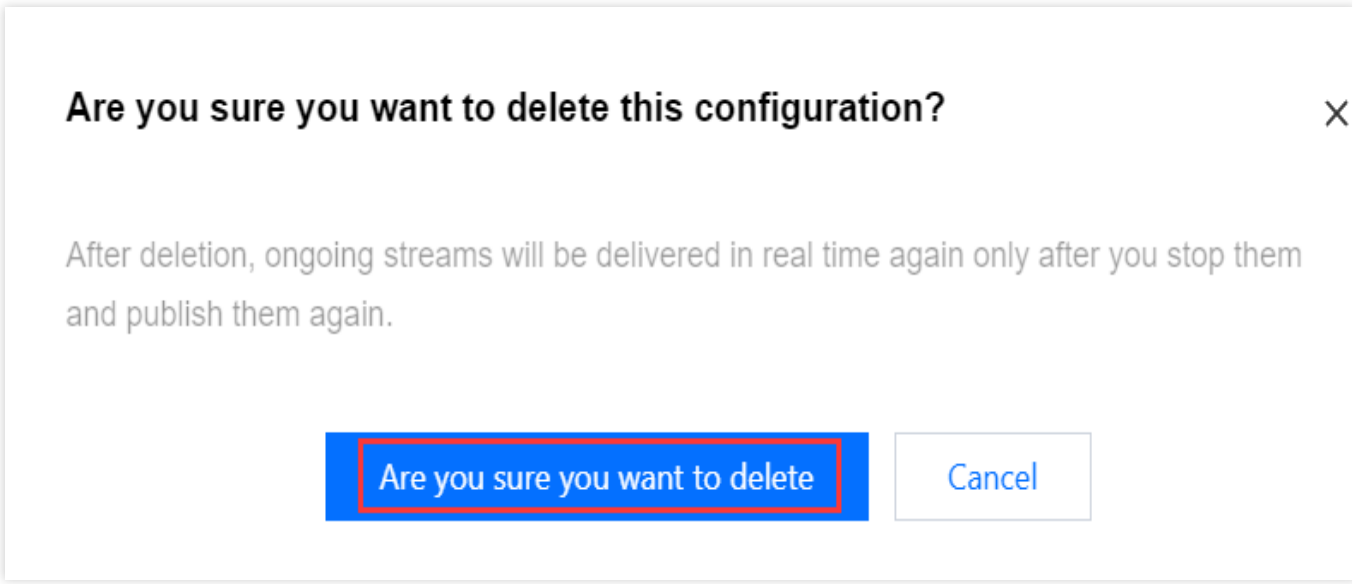
1. Select Domain Management, click the **push domain** to be configured, or click **Manage** on the right to enter the domain details page.



2. Select the **Advanced Configuration** tab. In the **Delayed playback configuration** area, select the configuration to be deleted and click **Delete** on the right side.



3. Confirm whether to delete this **Delayed playback configuration**, and click **Are you sure you want to delete** to successfully delete it.



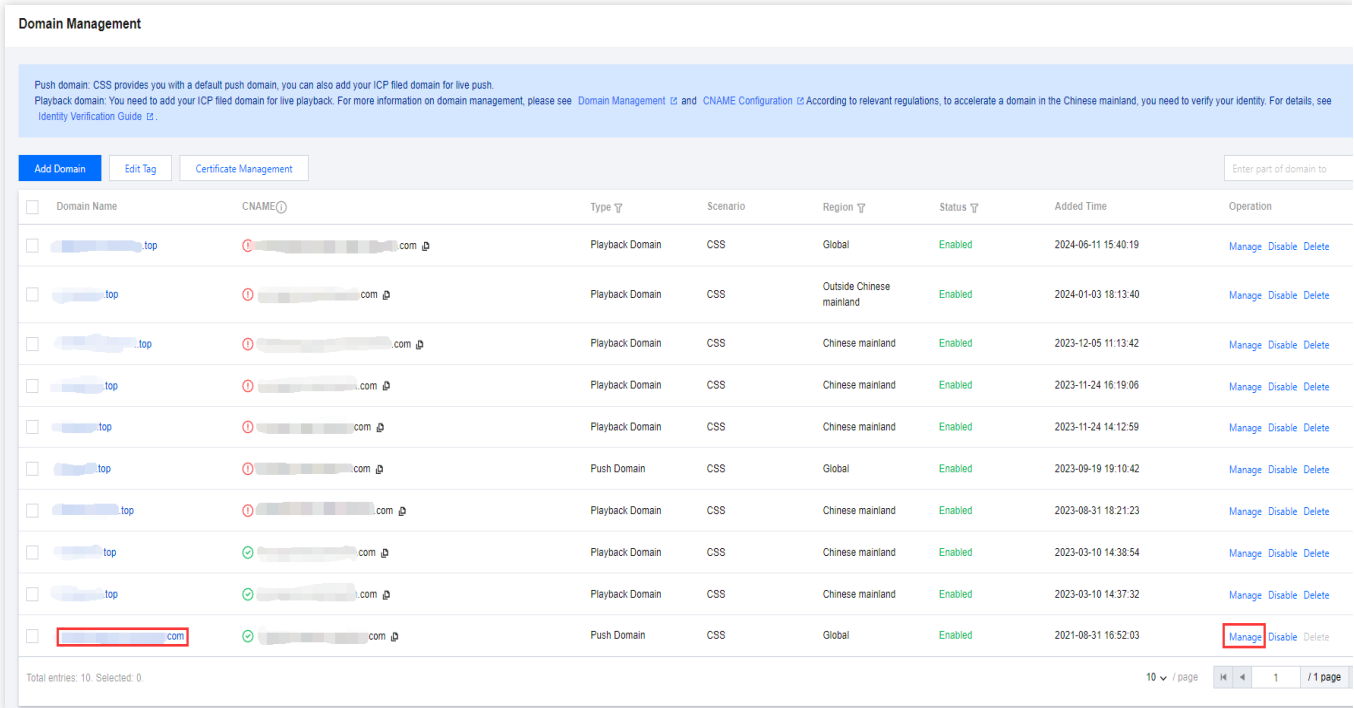
Note:

After deletion, ongoing streams will be delivered in real time again only after you stop them and publish them again.

Disabling Delayed Playback

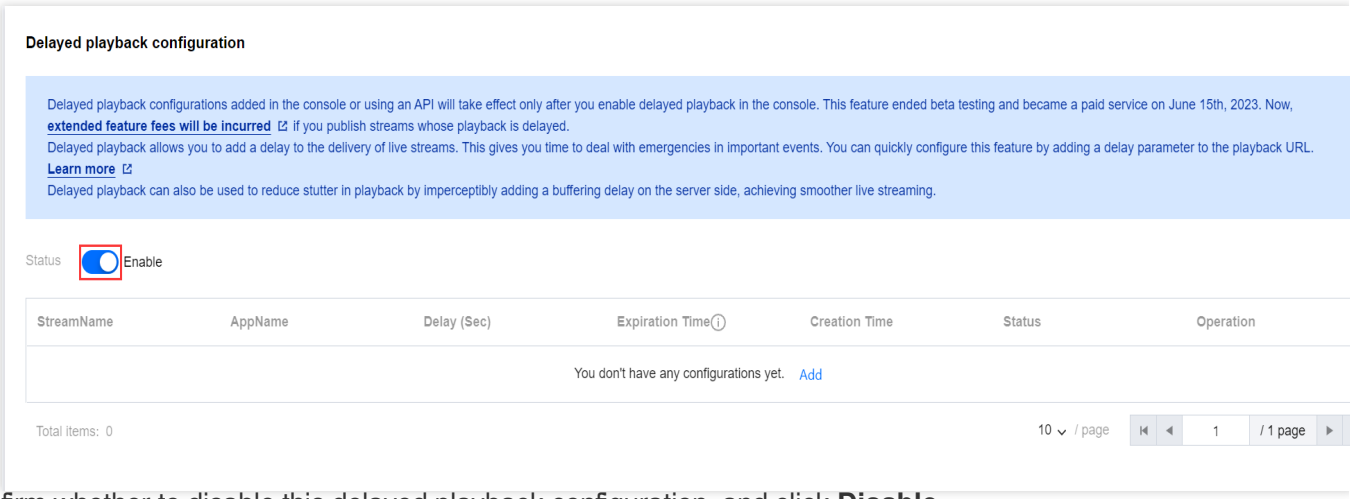
If you want to disable delayed playback configuration after enabling it, follow these steps:

1. Select Domain Management, click the **push domain** to be configured, or click **Manage** on the right side to enter the domain details page.

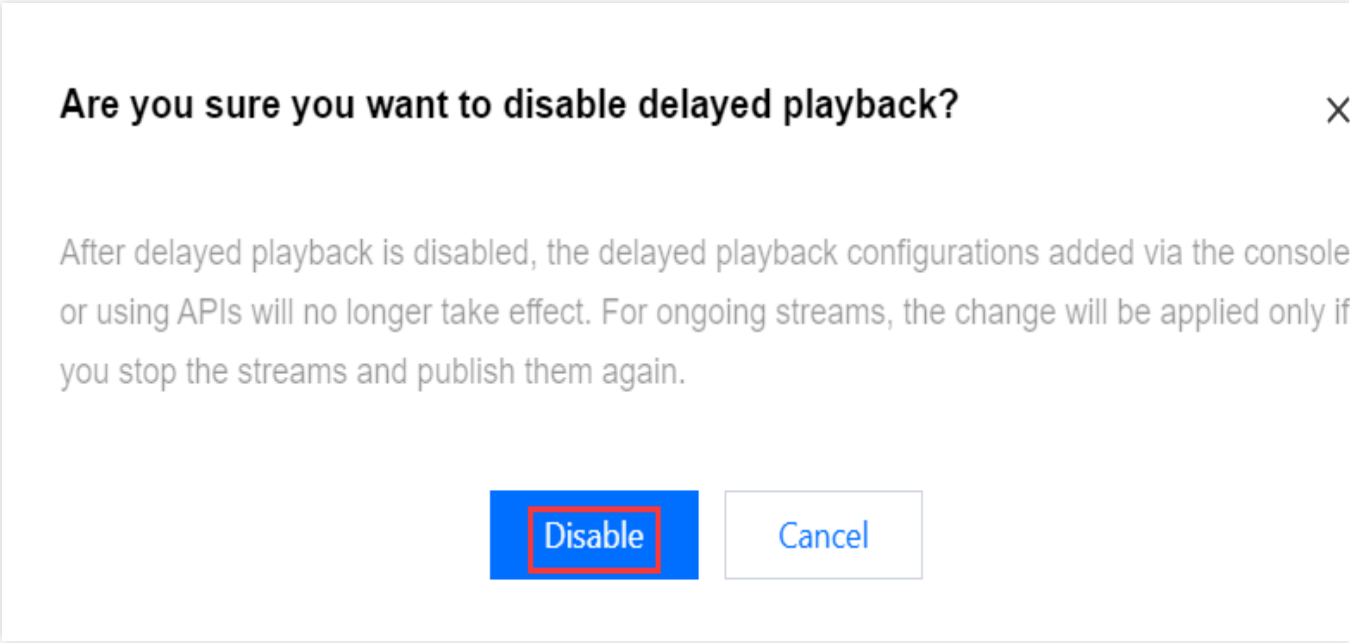


2. Select **Advanced Configuration** tab. In the **Delayed playback configuration** area, click


to toggle off the configuration.



3. Confirm whether to disable this delayed playback configuration, and click **Disable**.



Note:

After delayed playback is disabled, the delayed playback configurations added via the console or using APIs will no longer take effect. For ongoing streams, the change will be applied only if you stop the streams and publish them again.

Moderation Configuration

Last updated：2025-06-04 17:32:33

The moderation feature of live stream pushing is off by default. This document offers instructions on how to associate a moderation template with a specific push domain to activate the moderation feature and how to disassociate the template to deactivate moderation.

Notes

A template comes into effect approximately 5-10 minutes after it is associated.
After a template is successfully associated, the moderation feature will be activated for push URLs under the specified push domain.
Only one moderation template can be associated with a domain. Once associated, all streams under that domain will be moderated in accordance with the associated template.

Prerequisites

You have successfully logged in to the CSS console and have completed Adding Your Own Domain.
A moderation template has been created.

Associating Moderation Template

1. Go to Domain Management. Click **Domain Name** you want to configure or **Manage** to enter the domain details page.

2. Select the **Template Configuration** tab. Click **Edit** in the top-right corner of **Moderation Configuration**.

3. Choose a moderation configuration template according to your business requirements and click **Confirm** to complete the configuration.

Unbinding Moderation Template

1. Go to Domain Management. Click **Domain Name** you want to configure or **Manage** to enter the domain details page.

2. Select the **Template Configuration** tab and click **Edit** in the top-right corner of **Moderation Configuration**.

3. Based on your business requirements, uncheck the relevant template and click **Confirm** to proceed.

Note:
Unbinding a moderation template does not affect ongoing live streams.

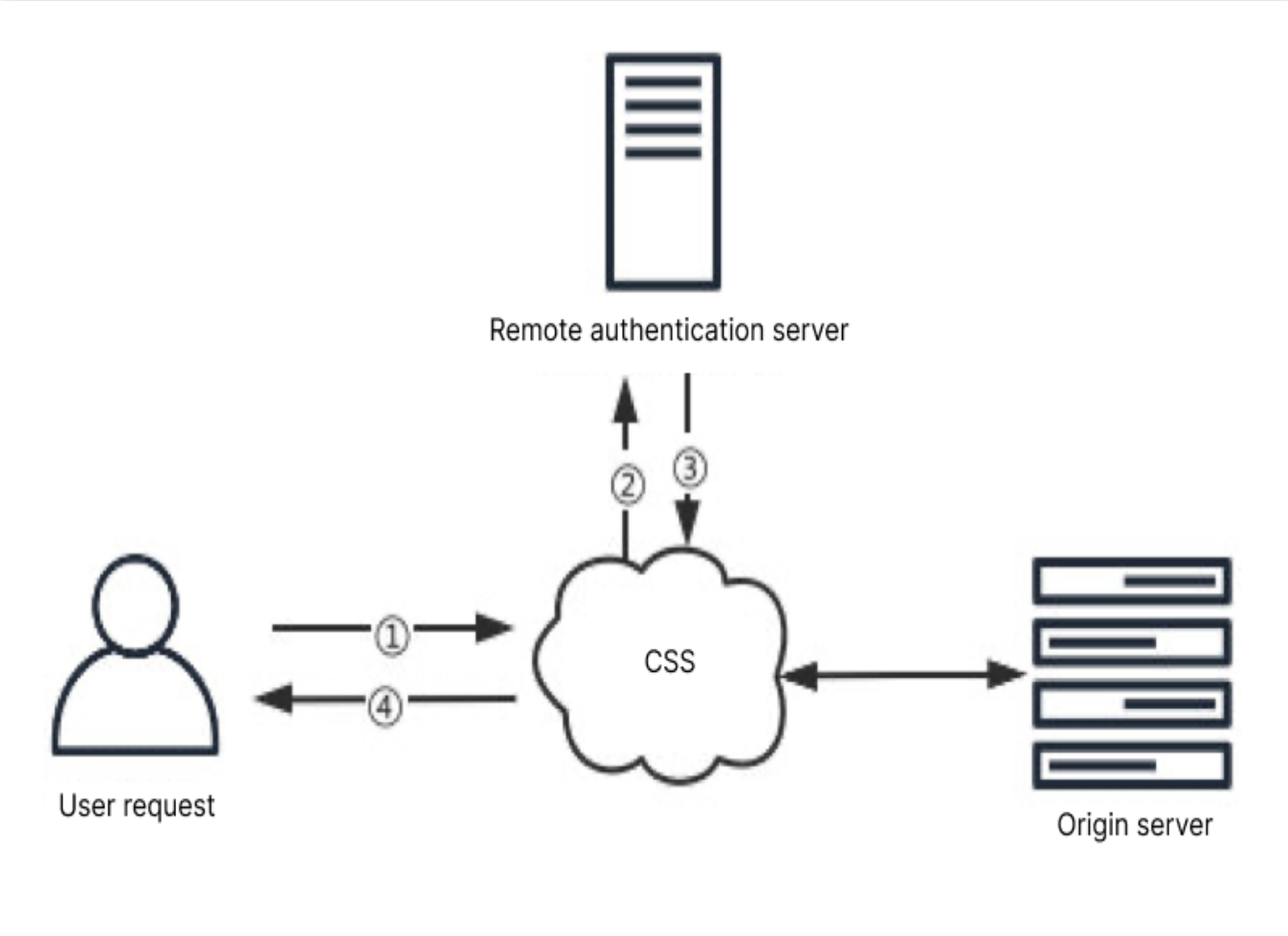
Remote Authentication Configuration

Last updated：2024-06-17 17:32:29

With remote authentication, after authenticating a push/playback request for hotlink protection, CSS will call your server API to send the request to your server so that you can determine whether the request is legitimate. Based on the result your server returns, CSS will approve or reject the push/playback request. This ensures more precise authentication and improves security. However, you need to develop your own authentication server.

Workflow

Remote authentication works as follows:



No	Description
1	A request is sent to CSS.

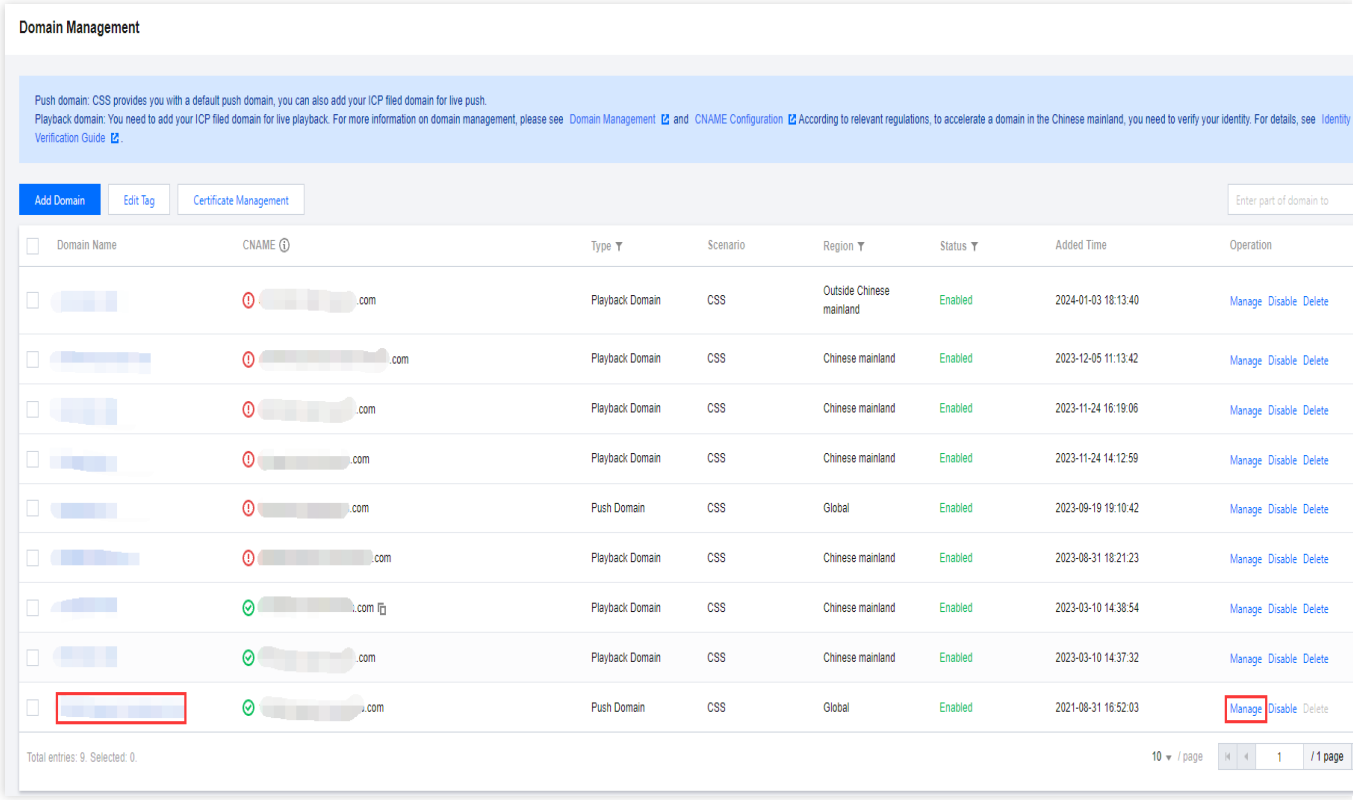
2	If remote authentication is enabled for the domain, CSS will process the request as specified and then send it to your authentication server.
3	Your authentication server returns the result. The HTTP status code 200 indicates that the request should be approved, while the code 403 indicates that the request should be rejected.
4	CSS approves or rejects the request based on the result.

Prerequisites

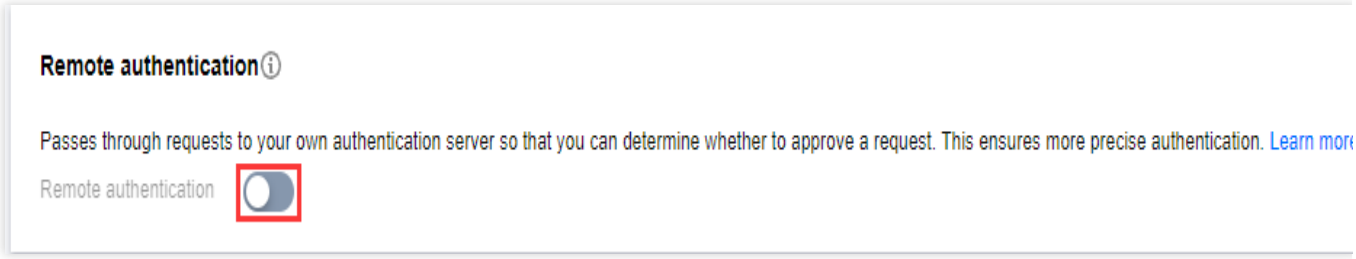
You have activated CSS and logged in to the CSS console.
You have added a push domain.

Configuring Remote Authentication

1. Log in to the CSS Console, and select Domain Management on the left sidebar. Click the the **push domain** you want to configure remote authentication for, or click on **Manage** on the right side to enter the Domain Management page.

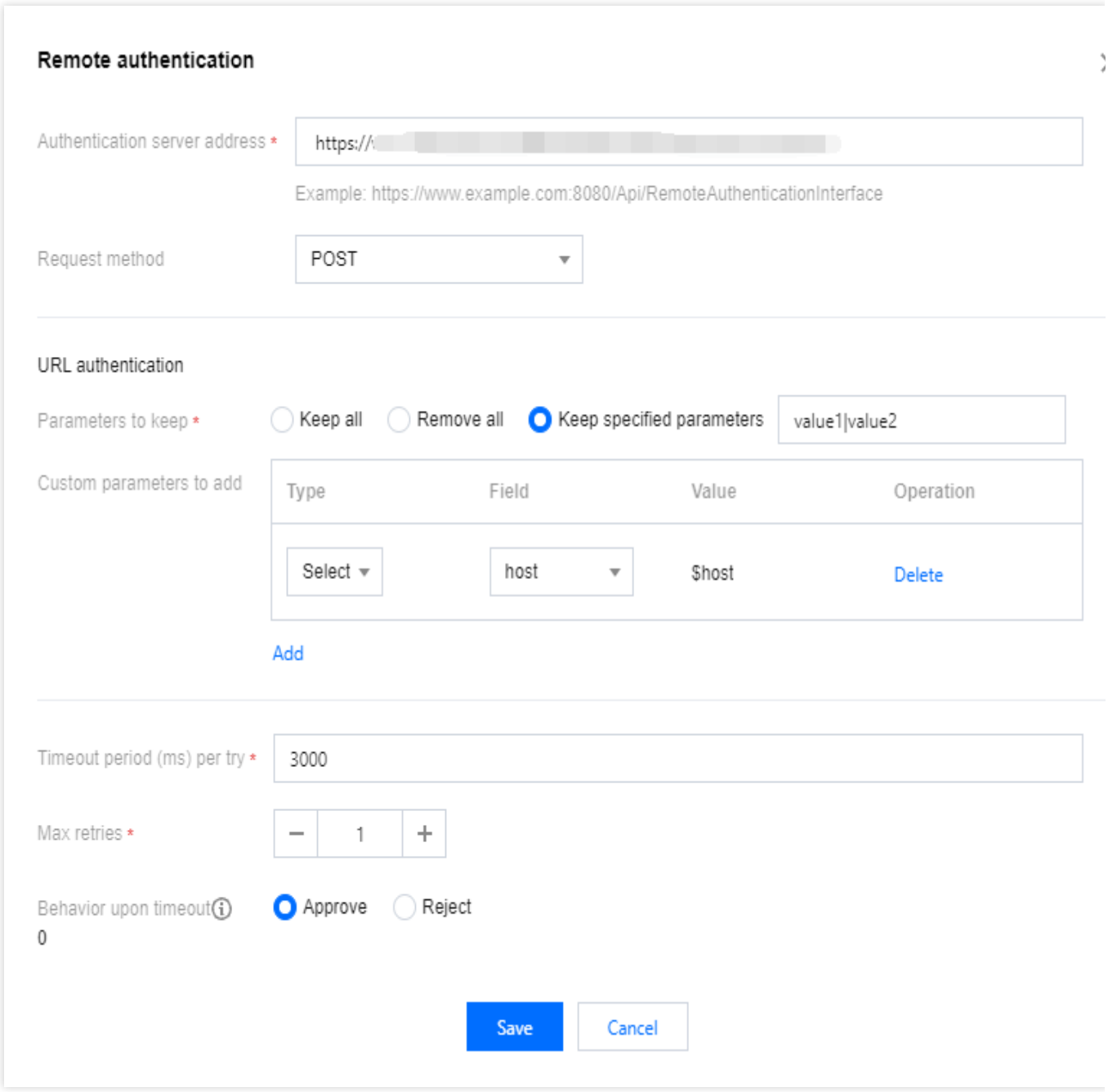


2. Under the **Advanced Configuration** tab, find **Remote authentication**.



3. Click

to enable remote authentication and complete the following settings:



Configuration Item		Description
Authentication server address		The address of your authentication server (required). Format: http(s)://+Domain or IP address+Port+Path.
Request method		POST is selected by default. You can also use HEAD or GET.
URL authentication	Parameters to keep	All URL parameters are kept by default. You can also specify parameters to keep or remove all parameters. If you select **Keep specified parameters**, you need to enter the parameters to be retained in the input box. Chinese characters and

		spaces are not supported. Separate multiple parameters with "|", for example: `value1|value2` . Authentication parameters are case-sensitive; "key" and "KEY" are considered as two different parameters.
	Custom parameters to add	Click **Add**, and the parameter type can be either **Select Parameter** or **Custom**. (Up to 50 parameters can be added) **Select Parameter** supports choosing host, uri, query, client_ip, and cdn_ip parameters. **host**: The push domain. **uri**: The original request URL. **client_ip**: The request client IP. **cdn_ip**: The request CDN-side IP. When you select **Custom**, you need to fill in the parameter and value fields. Chinese characters and spaces are not supported. Authentication parameters are case-sensitive; "key" and "KEY" are considered as two different parameters.
Timeout period (ms) per try		This is required. Enter a value between 500 and 3000. The default is 3000.
Max retries		Enter a value between 0 and 3. The default is 1.
Behavior upon timeout		This specifies whether to approve or reject a request if the system does not receive a response (HTTP status code 200 or 403) after the total timeout period elapses (Total timeout period = Timeout period per try x (Max retries + 1)). The default is **Approve**. You can also set it to **Reject**.

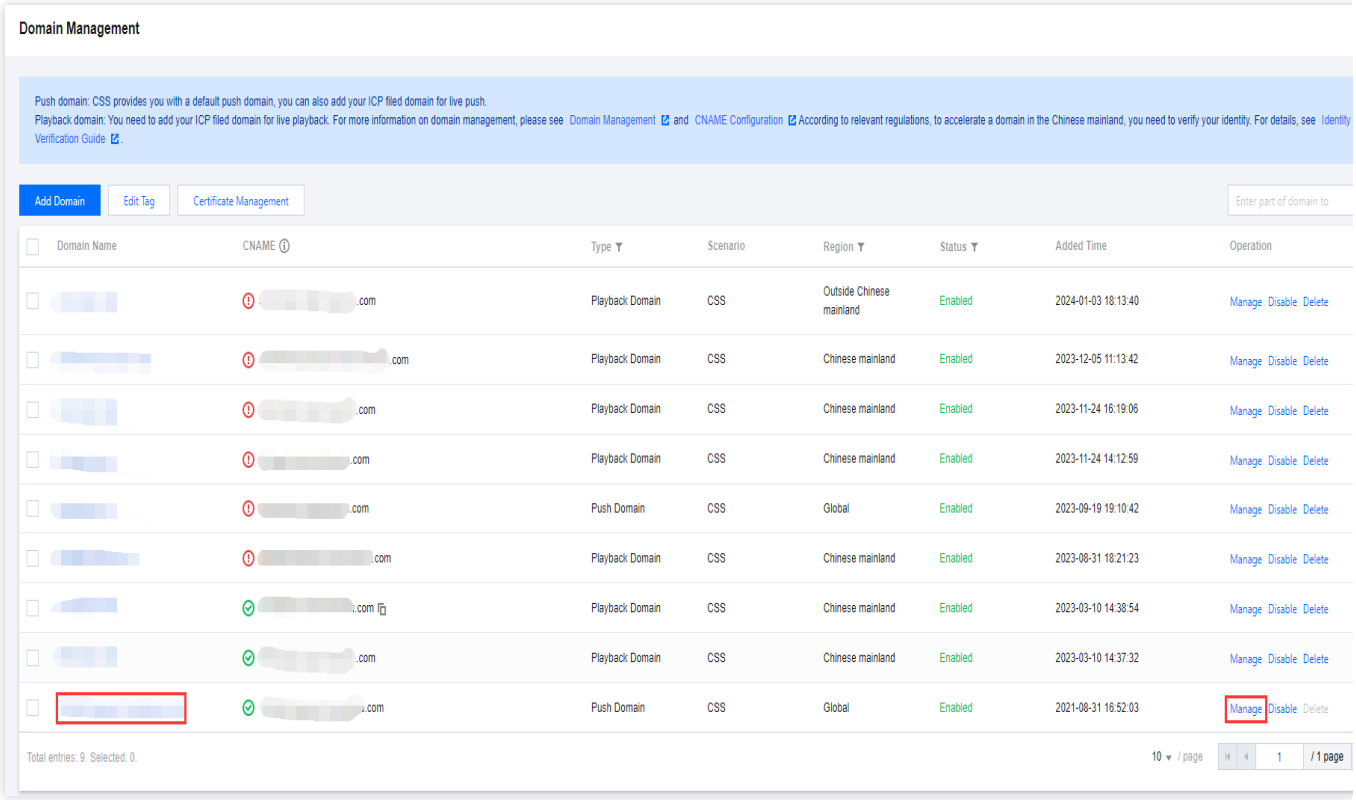
4. Click **Save**.

Note:

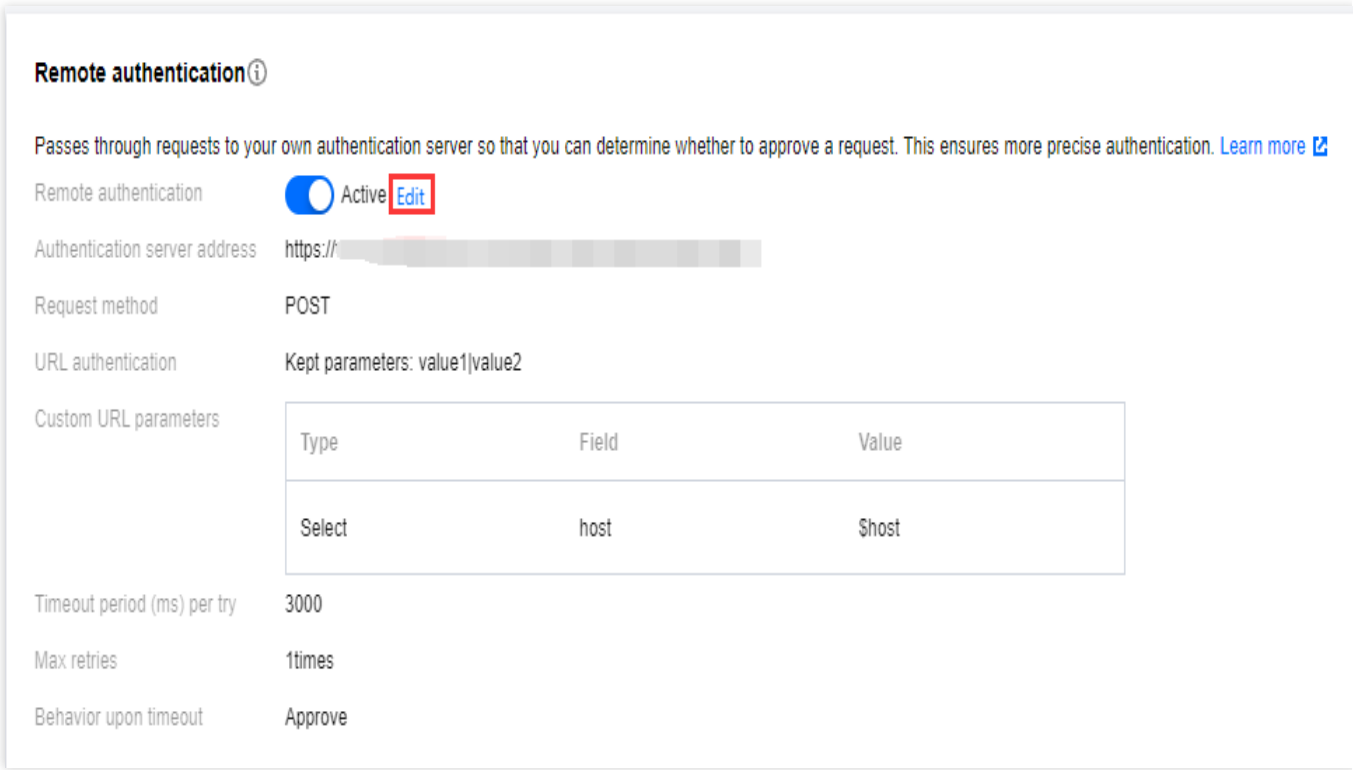
The remote authentication configuration will take effect about 10 minutes after completion.

Modifying Remote Authentication Settings

1. Select Domain Management on the left sidebar. Click the the push domain you want to configure remote authentication for, or click on **Manage** on the right side to enter the Domain Management page.

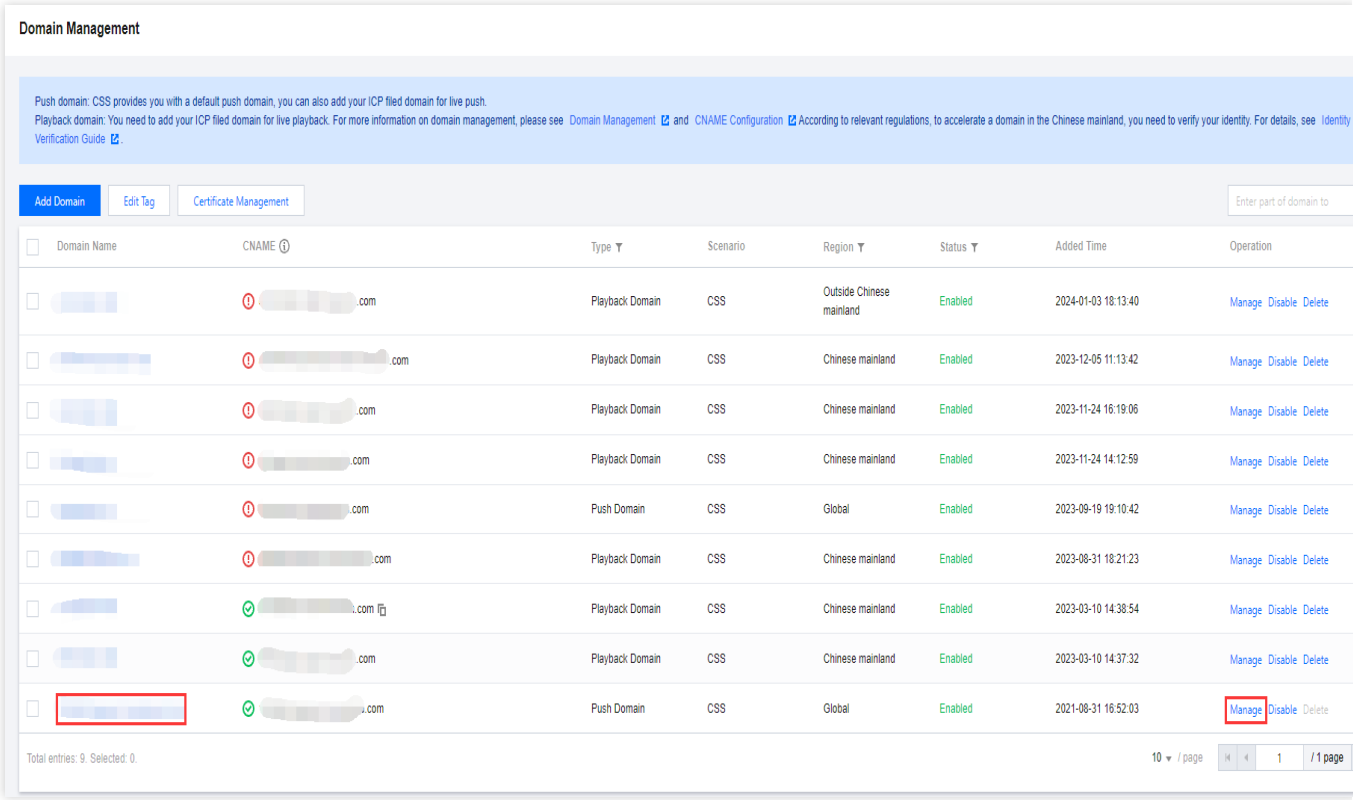


2. Under the **Advanced Configuration** tab, find **Remote authentication** and click Edit.
3. Modify the settings and click **Save**.



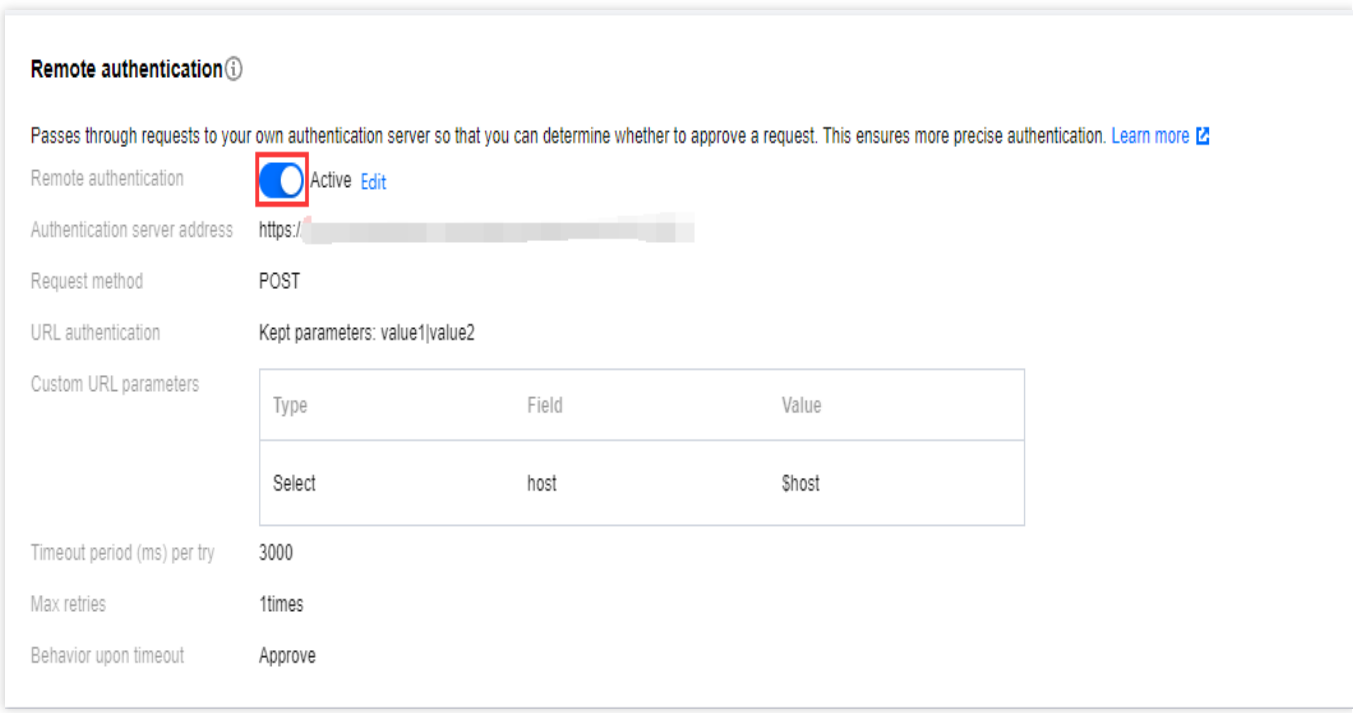
Disabling Remote Authentication

1. Select Domain Management on the left sidebar. Click the **push domain** you want to disable remote authentication for, or click **Manage** on the right to enter the Domain Management page.



2. Under the **Advanced Configuration** tab, find **Remote authentication** and click

to disable remote authentication.


Remote authentication
Passes through requests to your own authentication server so that you can determine whether to approve a request. This ensures more precise authentication. Learn more
Remote authentication
Active
Edit
Authentication server address
https:/
Request method
POST
URL authentication
Kept parameters: value1|value2
Custom URL parameters
Type
Field
Value
Select
host
$host
Timeout period (ms) per try
3000
Max retries
1times
Behavior upon timeout
Approve

Smart Erase Configuration

Last updated：2025-06-04 16:59:07

The Smart Erasing function is off by default.This document offers instructions on how to associate a Smart Erase template with a specific push domain to activate the Smart Erase feature and how to disassociate the template to deactivate Smart Erase.

Notes

A template comes into effect approximately 5-10 minutes after it is associated.
After the template is successfully associated, the smart erase function will be enabled for the push URL under the specified push domain.
Only one Smart Erase template can be associated with a domain. Once associated, all streams under that domain will be Smart Erase in accordance with the associated template.

Prerequisites

You have successfully logged in to the CSS console and have completed Adding Your Own Domain.
A moderation template has been created.

Associating Smart Erase Template

1. Go to Domain Management. Click **Domain Name** you want to configure or **Manage** to enter the domain details page.

2. Select the **Template Configuration** tab. Click **Edit** in the top-right corner of **Smart Erase Configuration**.

3. Choose a smart erase configuration template according to your business requirements and click **Confirm** to complete the configuration.

Unbinding Smart Erase Template

1. Go to Domain Management. Click **Domain Name** you want to configure or **Manage** to enter the domain details page.

2. Select the **Template Configuration** tab and click Edit in the top-right corner of **Smart Erase Configuration**.

3. Based on your business requirements, uncheck the relevant template and click **Confirm** to proceed.

Note:
Unbinding a smart erase template does not affect ongoing live streams.

Playback Domain Name Management
Playback Configuration

Last updated：2024-10-10 17:28:28

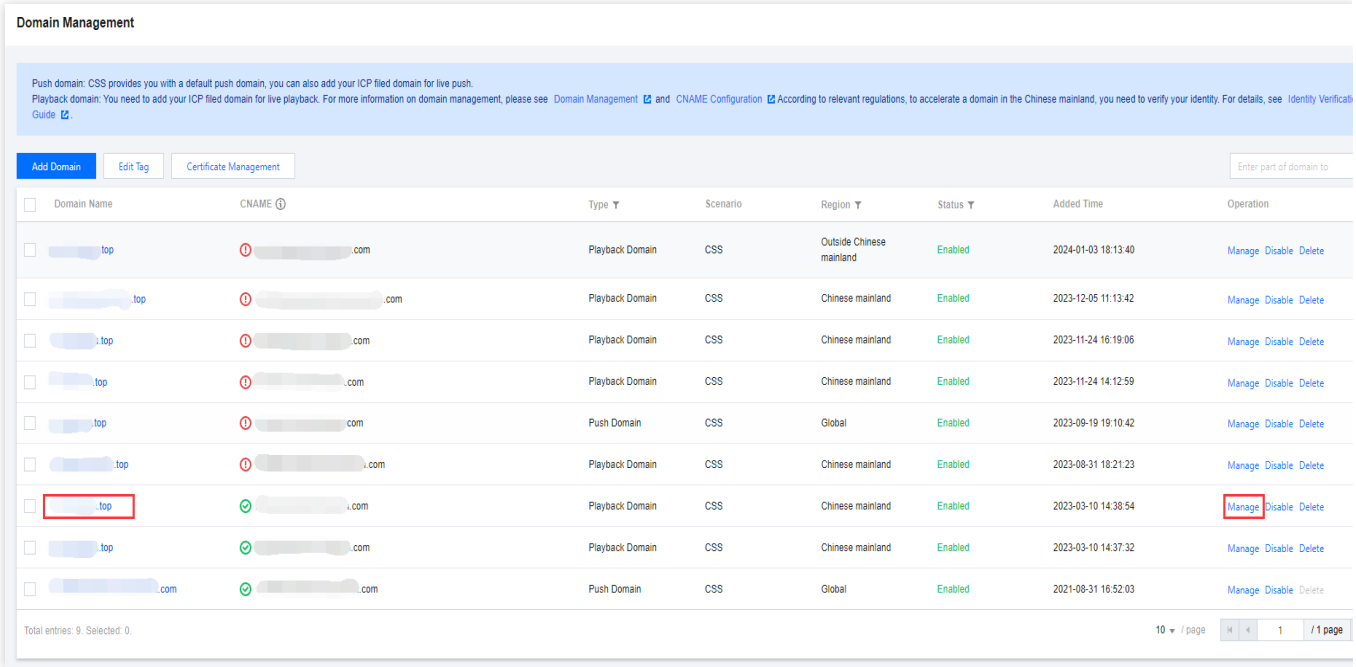
After pushing a stream successfully, you can use the address generator of the CSS console to generate a playback URL (you need to enter the `StreamName`, which should be the same as the stream ID in the push URL).

Prerequisites

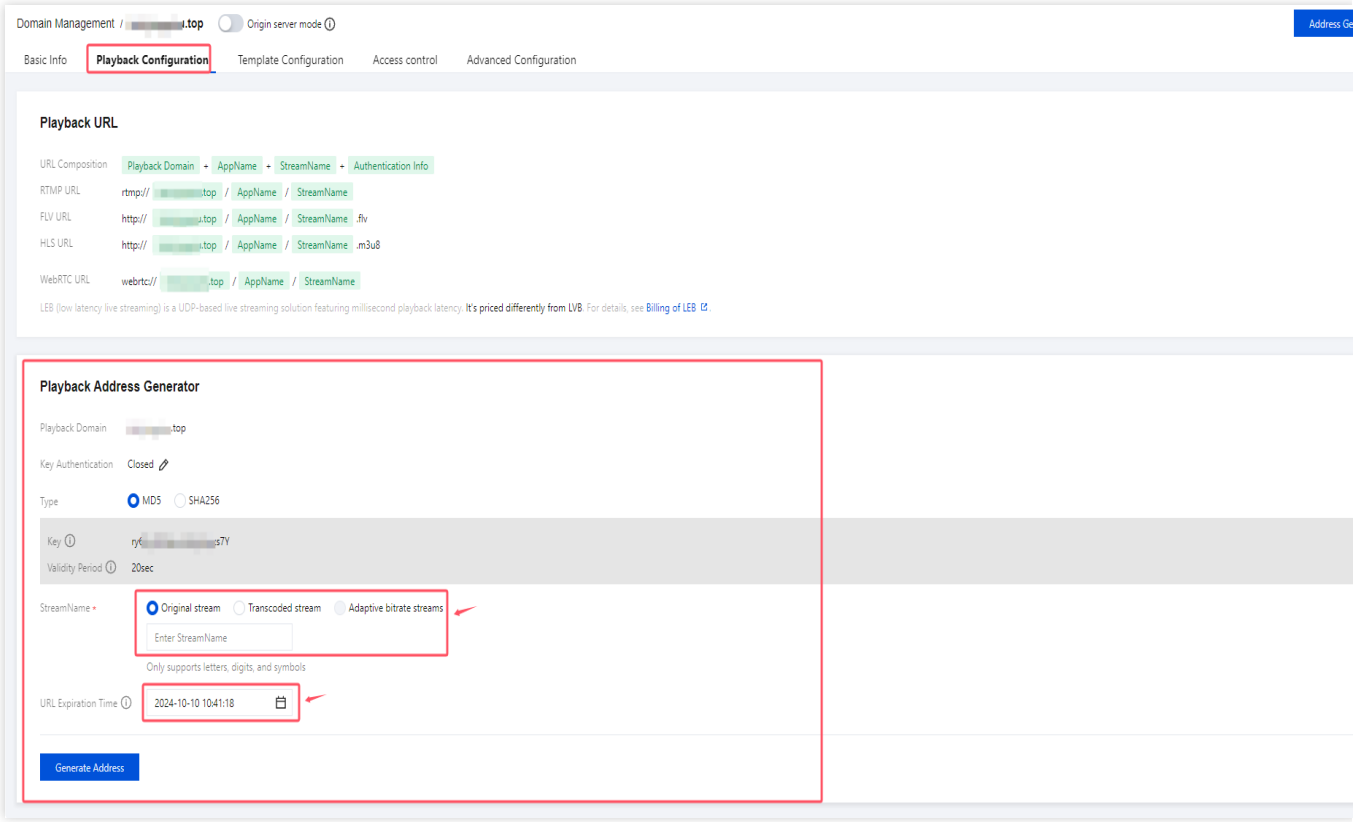
You have logged in to the CSS console.
You have added a **playback domain**. For directions on how to add a domain, see Adding Your Own Domain Name.

Directions

1. Select Domain Management on the left sidebar and click the name of your playback domain or click **Manage** on the right.



2. Select **Playback Configuration** and, in **Playback Address Generator**, complete the following settings:



2.1 You are required to select an **encryption type** . Make your choice based on your security needs and performance considerations. The options for encryption types include MD5 and SHA256, with MD5 being the default.

2.2 Select the type of stream to play, which can be the **original stream**, the **transcoded stream**, or **adaptive bitrate streams**. If you select **Transcoded stream**, you need to specify a transcoding template. If you select **Adaptive bitrate streams**, you need to specify an adaptive bitrate template.

2.3 Enter the **StreamName**.

Only supports English letters, digits, and symbols.

such as **livetеststream**. Make sure it's the same as the **StreamName** in your push URL.

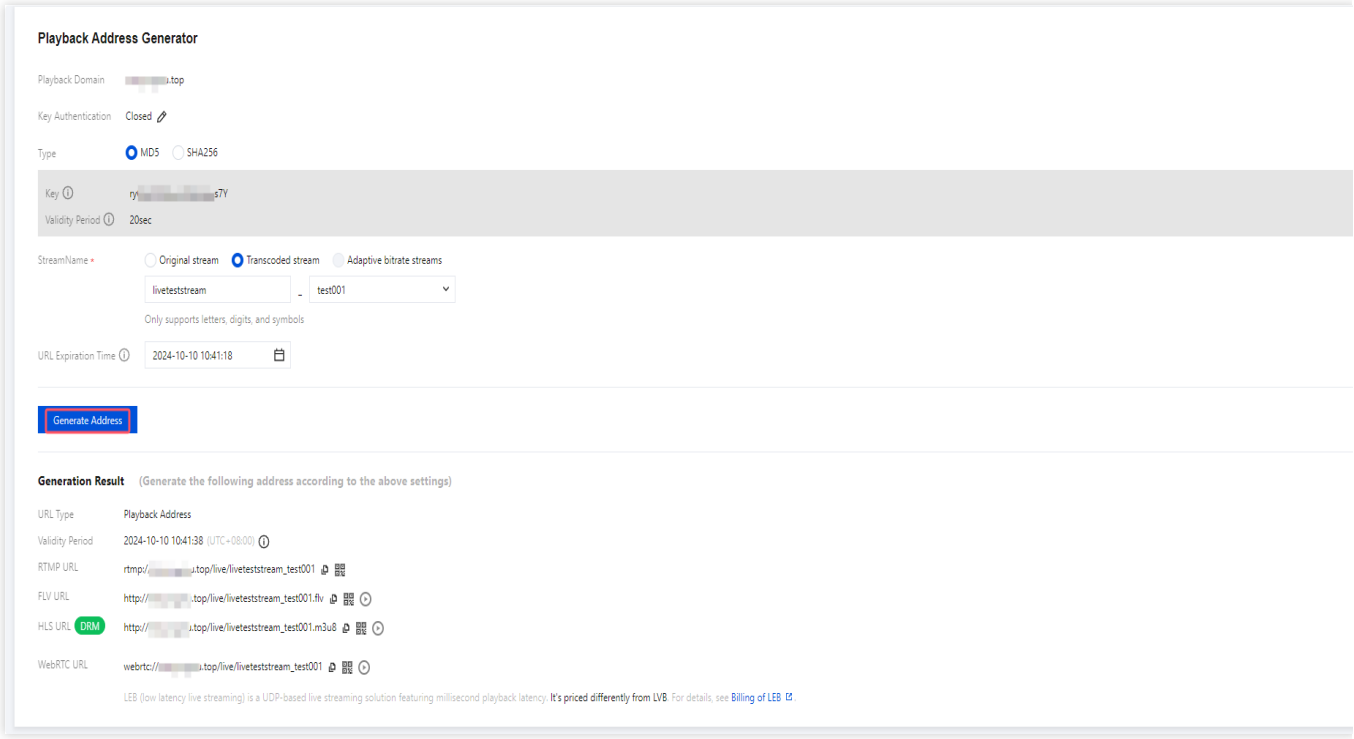
2.4 After you select an adaptive bitrate template, the names of the streams in the template will be listed in descending order by bitrate.

2.5 Select an **URL Expiration Time**, such as `2024-10-10 10:41:18` .

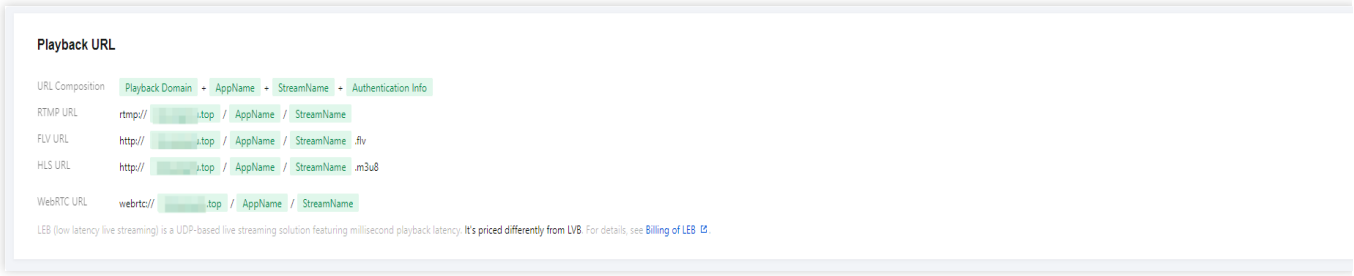
Note:

The URL expiration time refers to the hex(time) in the authentication information, and modifying it will change the playback URL. The actual validity period is the sum of the URL expiration time and the authentication validity period. Beyond this actual validity period, new requests will be denied, preventing further streaming through that address.

3. Click **Generate Address**.



4. If you haven't enabled authentication for your playback domain, in the **Playback URL** area on the same page, you can find playback URLs for RTMP, FLV, HLS, and UDP. Replace `StreamName` in the URLs with the stream ID in your push URL, and you can use the URLs to play the stream.



Note:

For more information, see Live Playback.

Playback URL Format

Playback URL for the original stream

```
RTMP format: `rtmp://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time
FLV format: `http://domain/AppName/StreamName.flv?txSecret=Md5(key+StreamName+hex(t
M3U8 format: `http://domain/AppName/StreamName.m3u8?txSecret=Md5(key+StreamName+hex
```

```
UDP format: webrtc://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time
```

`domain` : Your playback domain name.

`AppName` : The live streaming application name, which is `live` by default and is customizable.

`StreamName` : The stream ID, which uniquely identifies a stream and is customizable.

`txSecret` : The authentication string generated after playback authentication is enabled.

`txTime` : The expiration timestamp of the playback URL configured in the console.

Note:

If you have enabled authentication, the actual expiration time of a URL will be `txTime` plus the validity period of the authentication key.

For the sake of convenience, the console allows you to specify the URL expiration time in human-readable format. If you enable authentication, when generating playback URLs, the system will convert it to a hex timestamp (the value of `txTime`).

As long as you start push or playback before the expiration time and the stream is not interrupted, the push or playback can continue even after the URL expires.

Playback URL for the transcoded stream

If a transcoding template is bound to your playback domain, and you want to play the transcoded stream, you need to append the template name (`_transcoding template name`) to the original playback URL.

For example, if the original playback URL is `http://domain/AppName/StreamName.flv?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)` and the name of the transcoding template bound is `hd` , the playback URL of the transcoded stream would be `http://domain/AppName/StreamName_hd.flv?txSecret=Md5(key+StreamName_hd+hex(time))&txTime=hex(time)` .

Adaptive bitrate playback URL

Only HLS and WebRTC are supported for adaptive bitrate playback. The URL formats for the two protocols are different.

To get an **HLS adaptive bitrate URL**, add the template name (`_adaptive bitrate template name`) after `StreamName` of the original playback URL.

For example, suppose the original playback URL is `http://domain/AppName/StreamName.m3u8?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)` and the name of the adaptive bitrate template bound is `autobitrate` .

The HLS adaptive bitrate URL would be `http://domain/AppName/StreamName_autobitrate.m3u8?txSecret=Md5(key+StreamName_autobitrate+hex(time))&txTime=hex(time)` .

The format of a **WebRTC adaptive bitrate URL** is:

```
Playback domain (domain) + Application name (AppName, which is live by default),
Stream ID (StreamName) + Authentication information + Adaptive bitrate stream names
+ Name of the initially played stream + Bitrate control mode.
```

Note:

The adaptive stream names are listed in descending order by bitrate.

Suppose the adaptive bitrate template bound has three streams. Their names are "test 1", "test 2", and "test 3", and their bitrates are 200 Kbps, 300 Kbps, and 400 Kbps respectively.The WebRTC adaptive bitrate URL would be:

```
webrtc://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time))&txTime=he
```

H.265 playback URL

CSS supports pushing and playing H.265 streams. If the original stream is an H.264 stream, you can configure a transcoding template to transcode it into an H.265 stream. For details about how to do this in the console or by calling an API, see Live Remuxing and Transcoding.

Playback Authentication Configuration

Last updated：2024-06-19 16:08:10

Overview

By default, the content of Cloud Streaming Services (CSS) is publicly accessible, allowing you to view the live streaming content as soon as you obtain the playback address. If you require access control over the live streaming content during the use of Live Video Broadcasting (LVB) or Live Event Broadcasting (LEB), this can be achieved through authentication settings to protect the content of the live streaming resources. Key authentication is used to generate the authentication txSecret field in the live streaming address, which can prevent unauthorized use of the live streaming due to domain name leaks. We recommend that you enable the key authentication feature to enhance the security of your live streaming content.

How to Configure

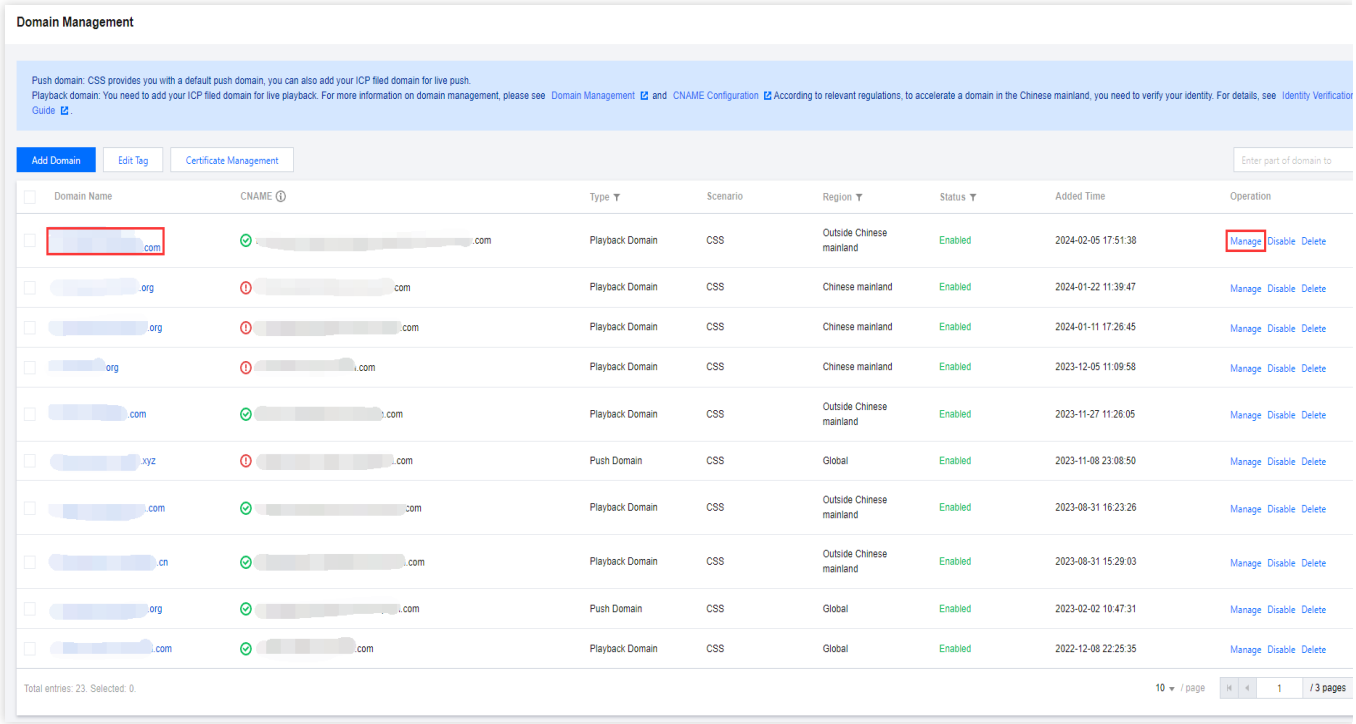
To enable URL authentication, a CSS user needs to generate an encrypted URL and provide it to other users. When a user requests content using the encrypted URL from a CSS acceleration node, the node will check the authentication information of the request to determine whether the request is valid. If it is, the node will return the content normally; otherwise, the node will reject the request, protecting your live streaming content.

Prerequisites

CSS has been activated, and you have logged in to the CSS console.
You have added a playback domain name.

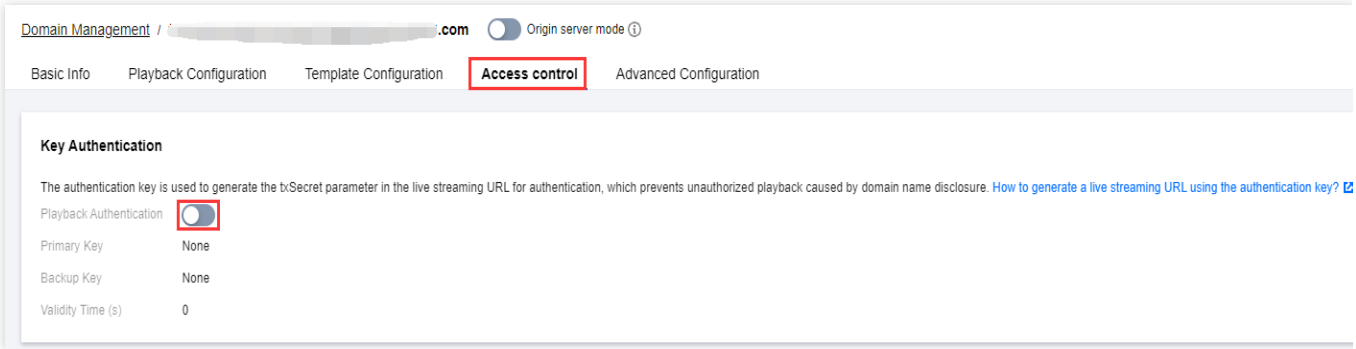
Enabling **Key Authentication**

1. Select **Domain Management** and click the **playback domain name** for which you want to enable authentication or click **Manage** to enter the domain name management page.

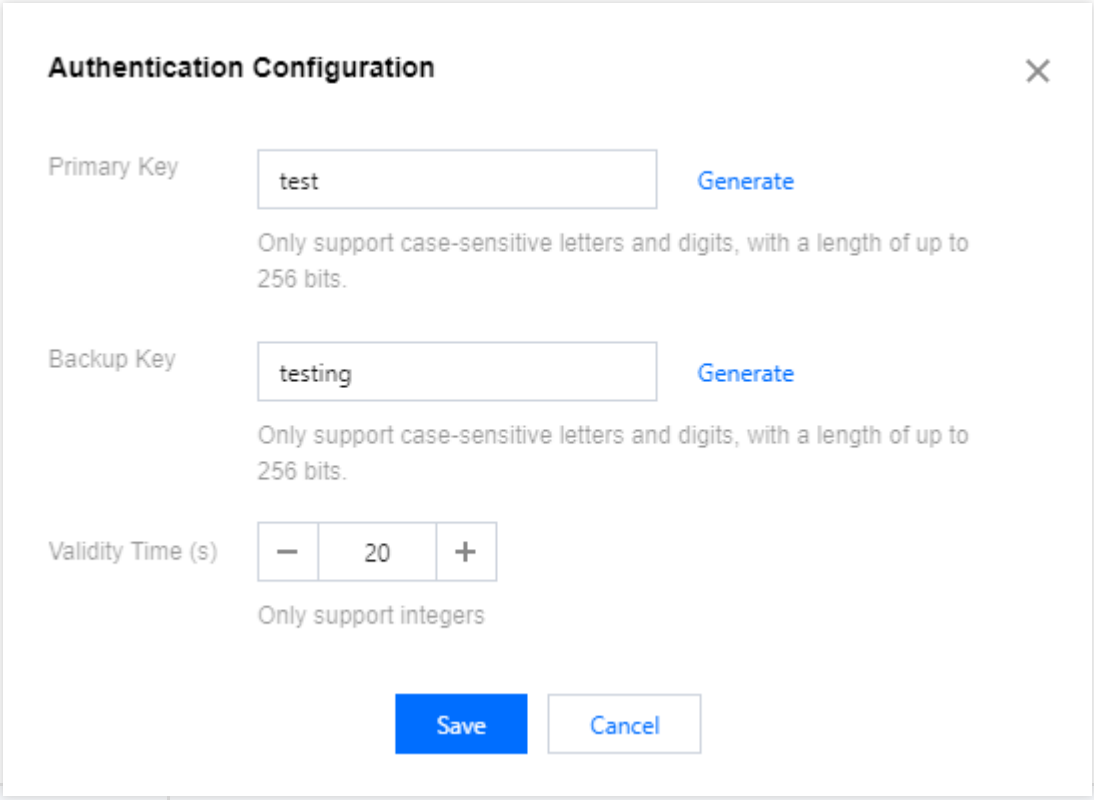


2. In the **Access control** > **Key Authentication** section, click

to enable key authentication.



3. Complete the following settings on the authentication configuration page:



Configuration Item	Description
Primary Key	When configuring a primary key for authentication, based on your actual needs and security policy, you can select a primary key **randomly generated** by the system, or enter a **custom** primary key, for example, test. It supports only uppercase letters, lowercase letters, and digits, with a maximum length of 256 characters.
Backup Key	When configuring a backup key for authentication, based on your actual needs and security policy, you can select a backup key randomly generated by the system, or enter a custom backup key, for example, testing. It supports only uppercase letters, lowercase letters, and digits, with a maximum length of 256 characters.
Validity Time (s)	It supports only integers. Enter the signature validity period, such as 20.

Note:

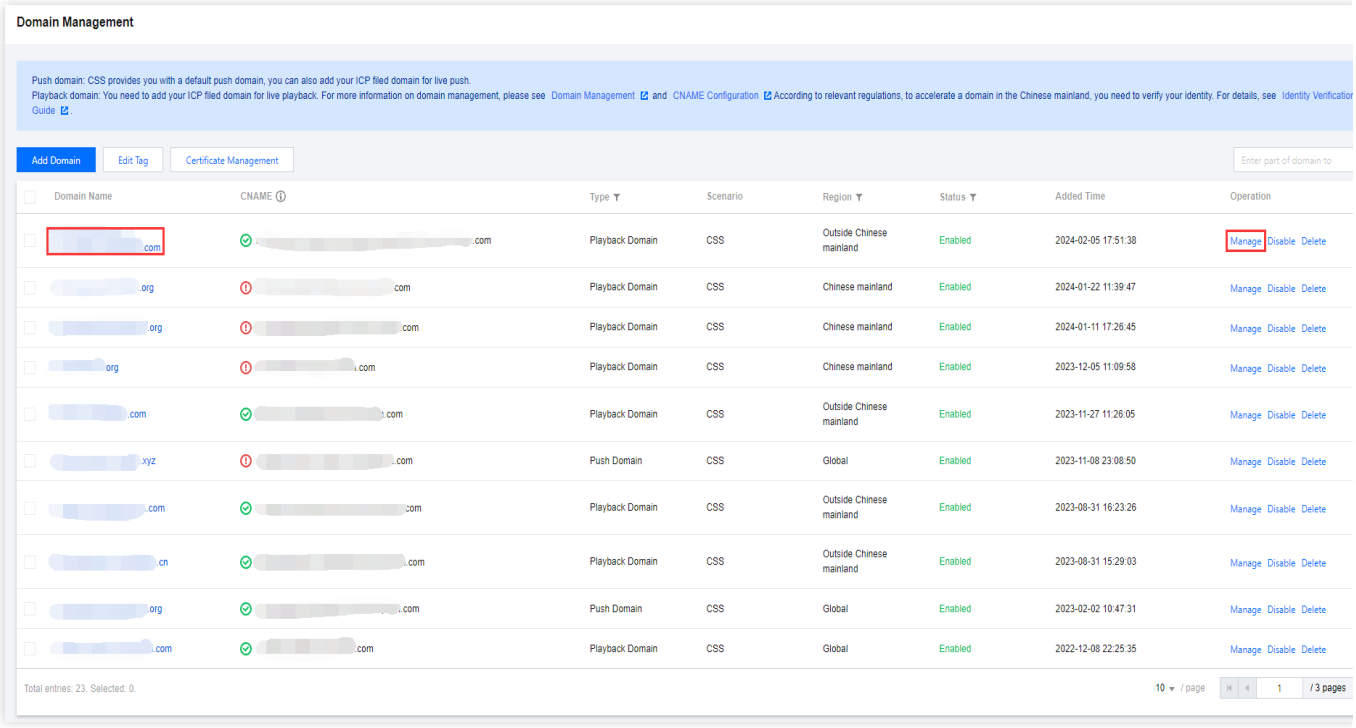
Playback authentication of a playback domain name is **disabled** by default.

Authentication Key : It includes a primary key (required) and a backup key (optional). You can switch smoothly to the backup key if your primary key is disclosed.

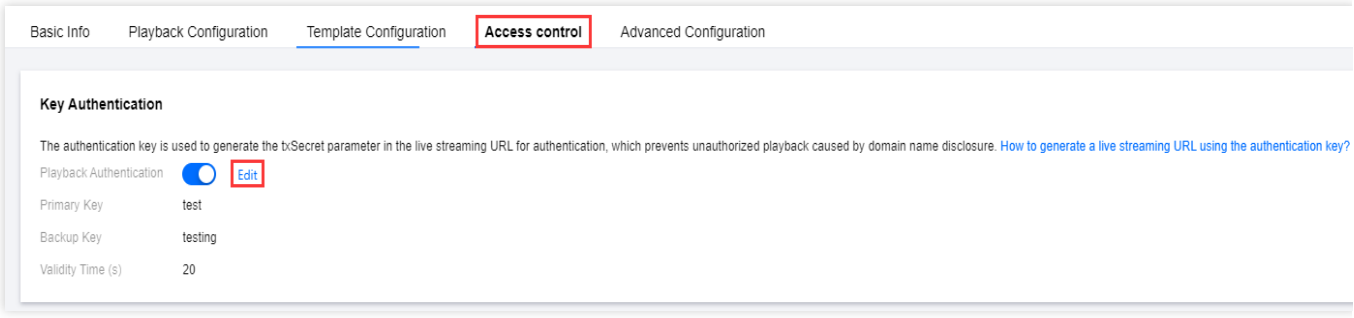
4. Click **Save** to save the configuration.

Modifying **Key Authentication**

1. Select **Domain Management**, and click the **playback domain name** that requires authentication configuration or click **Manage** to enter the domain name management page.



2. In the **Access control** > **Key Authentication** section, click **Edit** to enter the key authentication configuration page.



3. Modify the configuration item information according to your actual needs, and click **Save** to complete the modification.

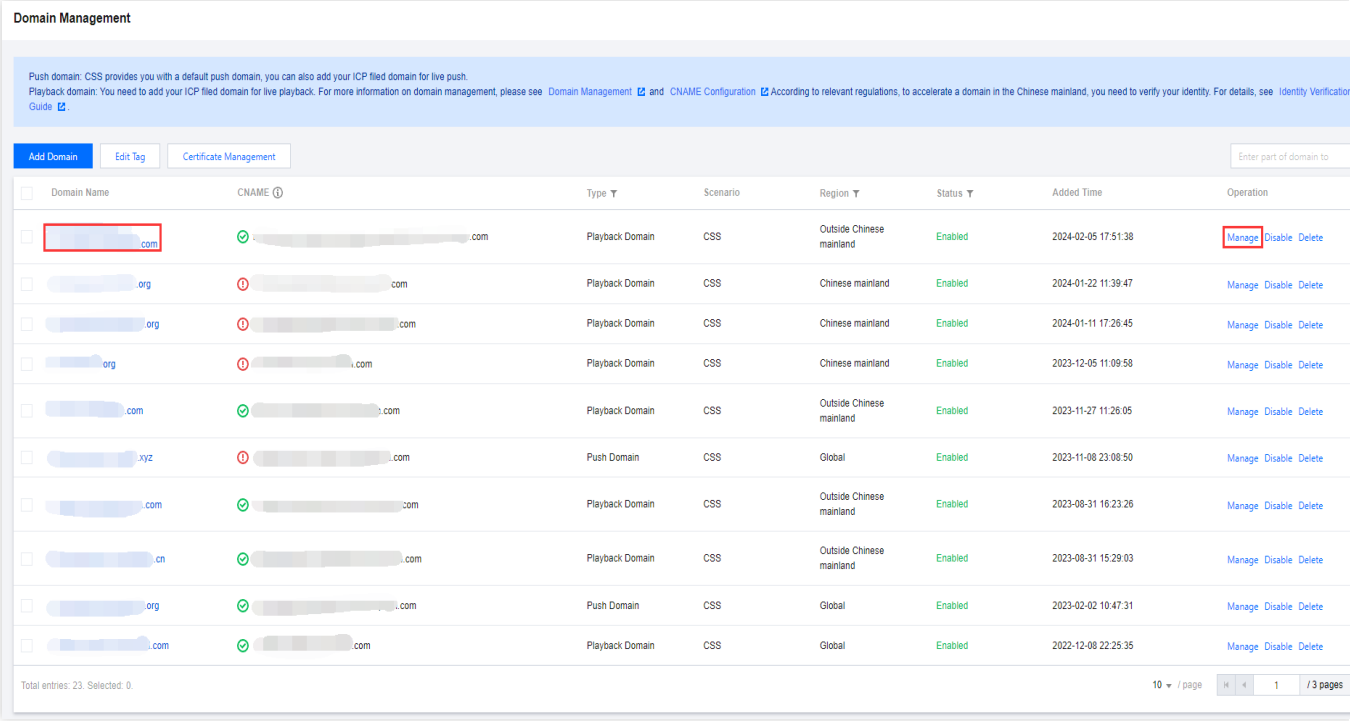
Disabling **Key Authentication**

Note:

When you choose to disable key authentication, make sure you understand the risks involved. Disabling key authentication may expose your live streaming service to piracy, resulting in additional service fees. Therefore, we recommend that you keep key authentication enabled to protect your live streaming content.

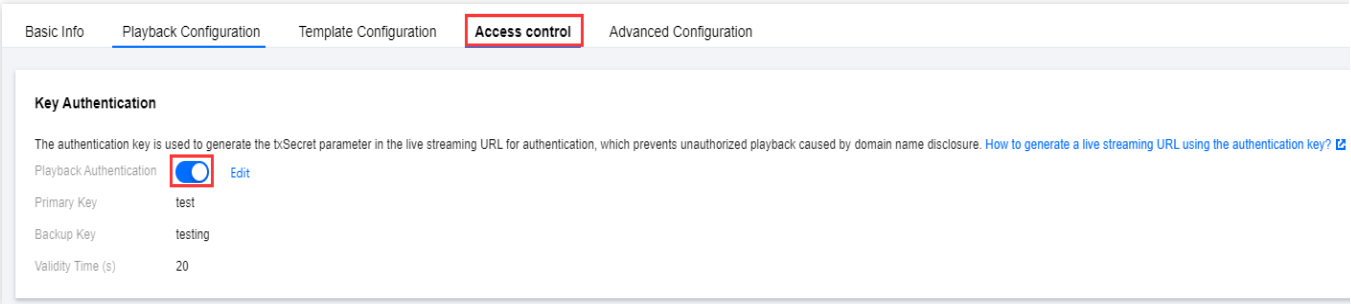
After Enabling Key Authentication, if you need to disable this feature, follow these steps:

1. Select **Domain Management**, and click the **playback domain name** that requires authentication configuration or click **Manage** to enter the domain name management page.

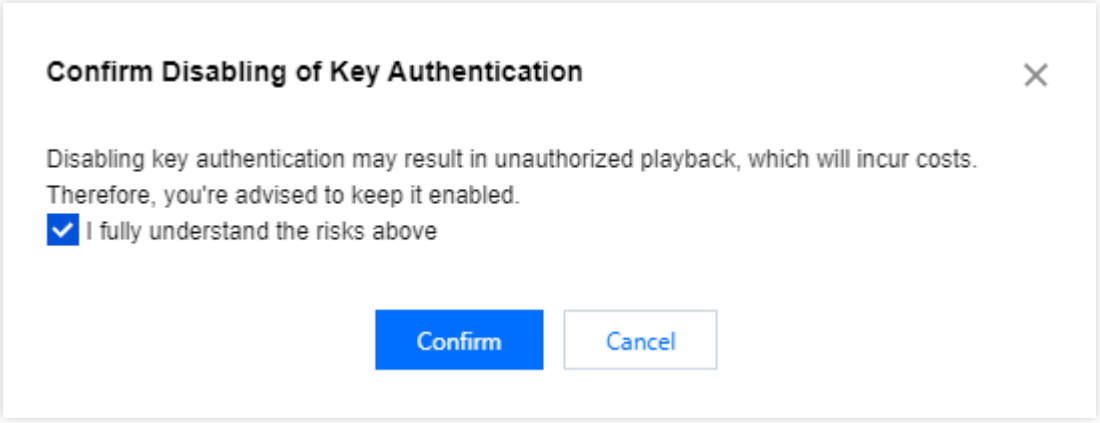


2. In the **Access control** > **Key Authentication** section, click

to disable key authentication.



3. Before disabling key authentication, confirm once more if you really wish to proceed. If you understand and accept the risks, click **Confirm** to proceed.



Note:

After authentication is enabled for the playback domain name, the original playback URL will be inaccessible and an error 403 will be returned. Before enabling this feature, please make sure that your live streaming platform is compatible with the following authentication algorithm so that your streaming services will not be affected.

Example

Original playback URL:

```
http://www.test.com/live/test01.flv
```

The authentication parameters configured are as follows:

```
Primary key: ngoeiq03
Backup key: -
Validity period: 12495 seconds
```

Note:

If you have enabled authentication, the actual expiration time of a URL will be `txTime` plus the validity period of the key.

For the sake of convenience, the time you set in the console is the actual expiration time. **If you have enabled authentication, the system will calculate the `txTime` when generating playback URLs.**

If you use FLV or RTMP methods to start pulling the stream before the expiration time, the stream will be maintained normally as long as the connection is not interrupted or stopped, even if the expiration time has passed.

If you use the HLS method to start pulling the stream before the expiration time, the stream will be stopped when the expiration time is reached.

Timestamp calculation:

```
Setting time: 2018.12.01 08:30:00
Decimal Unix timestamp: 1543624200
```

```
Hexadecimal Unix timestamp: 5C01D608 (case-insensitive). CSS uses hexadecimal
timestamps for authentication.
```

Authentication signature calculation:

```
txSecret = MD5(key+StreamName+txTime)
StreamName is the stream name, which is the same as the StreamID
txTime is the timestamp
key is the authentication key
txSecret = MD5(ngoeiq03+test01+5C01D608)
txSecret = MD5(ngoeiq03test015C01D608)
txSecret = ce797dc6238156d548ef945e6ad1ea20
```

New playback URL:

```
http://www.test.com/live/test01.flv?
txSecret=ce797dc6238156d548ef945e6ad1ea20&txTime=5C01D608
```

The expiration time of this URL is 2018.12.01 08:30:00 + 12495 seconds, i.e., 2018.12.01 11:58:15 Beijing time.

If authentication fails or the URL expires, CSS will return 403.

Referer Configuration

Last updated：2025-03-31 17:56:38

You can set referer blocklist/allowlist and rules to block/allow playback requests so as to protect live streaming content. You can also choose whether to allow empty referer.

How to Configure

Referer URL is based on the HTTP protocol. CSS uses the referer field in an HTTP request to identify the source and verify the request, and then determine whether to accept or reject the request.

Notes

Referer information is included in HTTP requests. After you enable referer configuration, live streams using RTMP or WebRTC for playback will not authenticate the referer and can be played back normally. To make the referer configuration effective, the FLV or HLS protocol is recommended for playback.
Enabling, disabling, or modifying the referer takes effects in 15-20 minutes after the configuration. You don't need to push streams again.
The referer hotlink protection feature verifies the referer information in the header of an HTTP request so as to check whether the request is valid and allow or reject live streaming accordingly. However, there may be cases where a forged referer bypasses the verification to hotlink the service. Therefore, we recommend you not strongly rely on referer for content protection.

Prerequisites

You have activated the CSS service and logged in to the CSS console.
You have added a playback domain name.

Enabling Referer

1. Select **Domain Management**, and click the target **playback domain** or click **Manage** on the right to enter the domain management page.

2. In **Access Control** > **Referer Configuration**, click

to enable Referer Hotlink Protection.

3. And configure as follows:

Configuration Item	Description
Referer Type	Select **Blocklist** or **Allowlist** as the referer type. You cannot select both of them, When the referer allowlist is configured, request sources on the list will be allowed to access the live streaming content while those not on the list will be blocked. When the referer blocklist is configured, request sources on the list will be blocked to access the live streaming content while those not on the list will be allowed.
Allow Empty Referer	When this feature is enabled, access will be allowed for HTTP requests with empty or no referer field. Users can access the live stream URL directly via browsers. When this feature is disabled, requests with empty referer will be rejected.
Referer Patterns	The total number of characters for rules cannot exceed 4,000. (Itis recommended that the number of rules be no greater than 200.) Separate rules by line breaks. Blank lines and semicolons (;) are not allowed. For ordinary rules, strings in these rules can be matched, and the wildcard character * is supported for fuzzy matching. For example, `https://*.domain.com` . For regular expression rules, they should be included in parentheses () . For example, you can use `(^https?://www.domain.com($/)` to match `www.domain.com` and use `(https?://[^/?]*domain.com($|/) to match*.domain.com.`

4. Click **Save** to save the configuration.

Modifying Referer

1. Select **Domain Management**, and click the target **playback domain** or click **Manage** on the right to enter the domain management page.

2. In **Access Control** > **Referer Configuration**, click **Edit** to enter the referer configuration page.
3. Modify the configuration items and click **Save**.

Disabling Referer

After enabling the referer, you can disable it by performing the following steps:

1. Select **Domain Management**, and click the target **playback domain** or click **Manage** on the right to enter the domain management page.

2. In **Access Control** > **Referer Configuration**, click

to disable the referer.

Template Configuration

Last updated：2024-05-28 10:26:22

With CSS, the original bitrate is used for playback by default. To use a different playback bitrate, you can bind your domain with a transcoding or adaptive bitrate template. This document shows you how to bind a template to and unbind a template from a playback domain.

Notes

A template takes effect about 5-10 minutes after it is bound to a domain.
After you specify a transcoding template, the backend will generate playback URLs of different formats for the transcoded stream. To avoid image distortion, push the stream at a resolution as close as possible to the original resolution.
H.265 is supported by fewer players than H.264. Playback may fail if a player does not support H.265. To solve this issue, you can configure a transcoding template to transcode your video to H.264.
Loading may take some time for the first user accessing the URL that uses a different playback bitrate.
One domain can be bound with multiple transcoding templates. After you bind a template, videos will be transcoded as specified in the template.
You can create up to **50** transcoding templates.

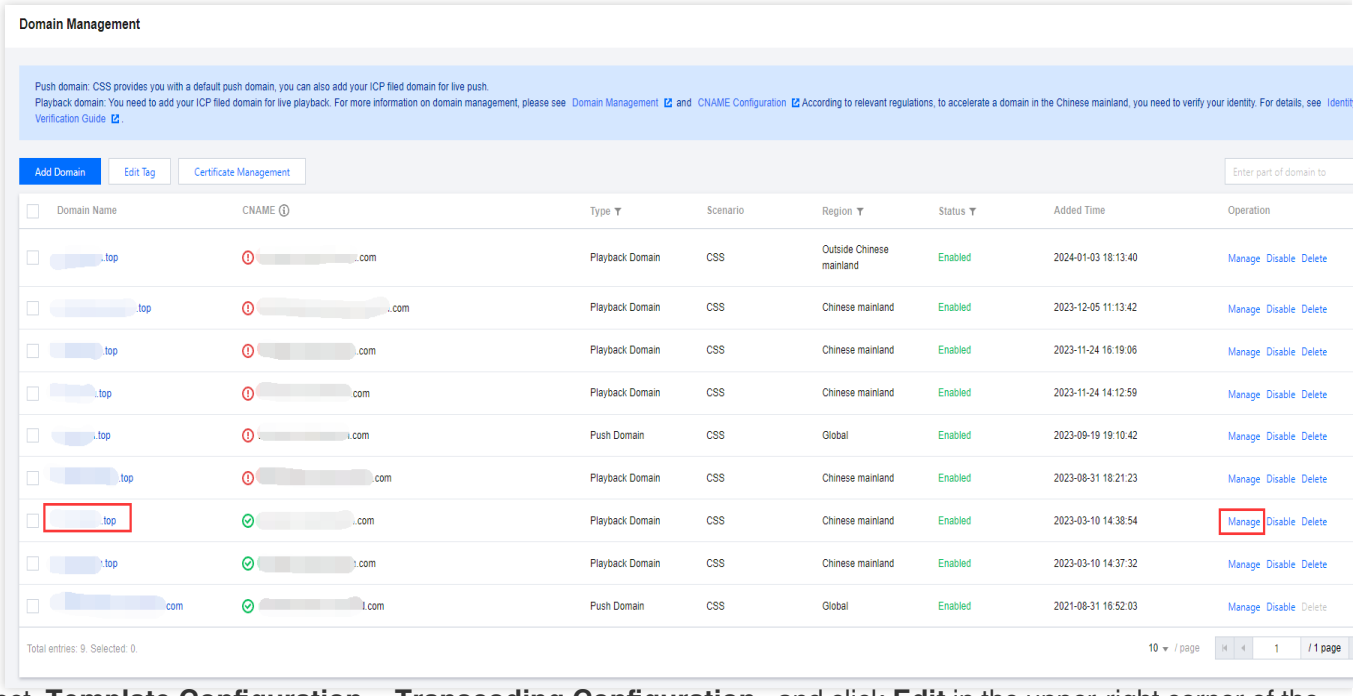
Prerequisites

You have logged in to the CSS console and added a playback domain name.
You have created a transcoding template or an adaptive bitrate template.

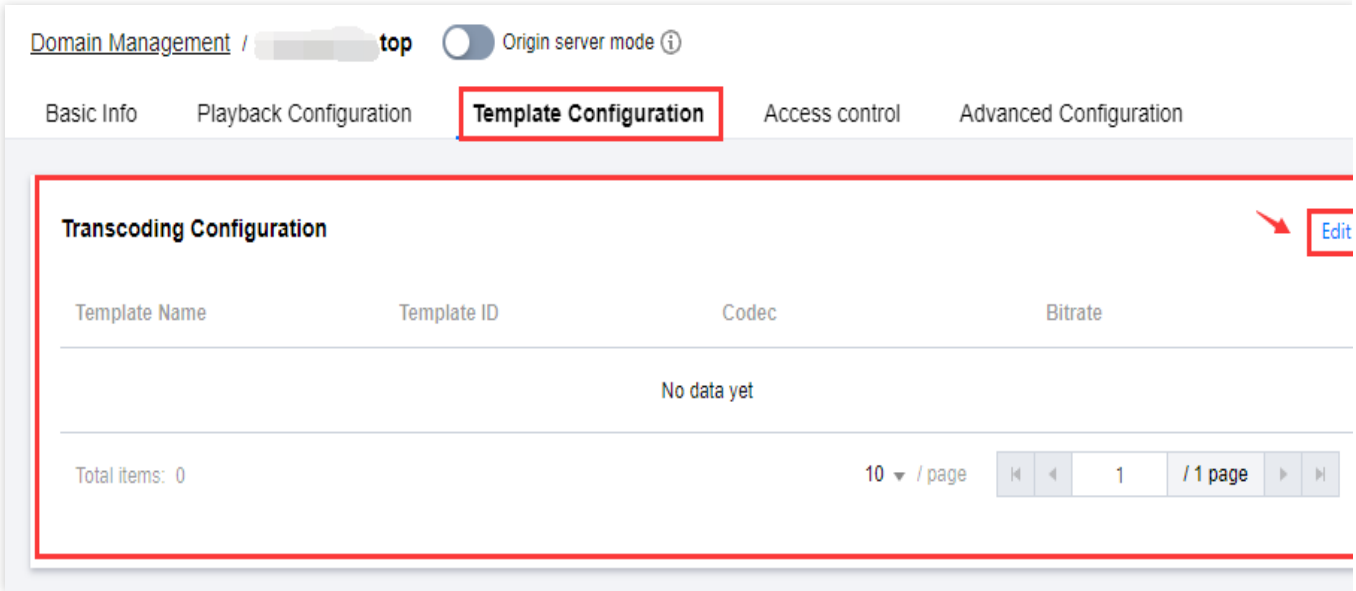
Transcoding Template

Binding a transcoding template

1. Go to Domain Management. Click the name of your playback domain or **Manage** on the right.



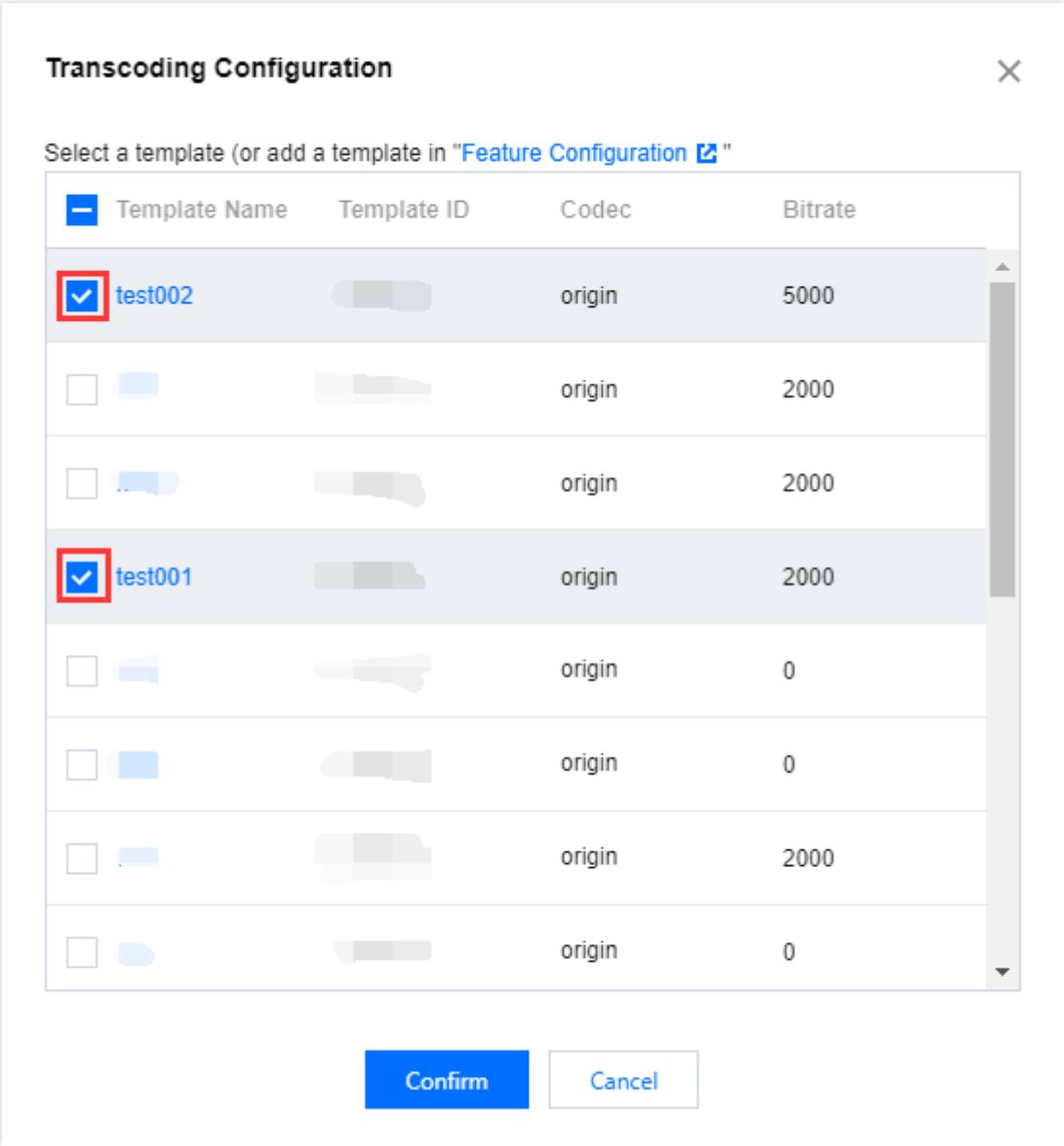
2. Select **Template Configuration > Transcoding Configuration** , and click **Edit** in the upper-right corner of the **Transcoding Configuration** tab.



3. Based on your actual business needs, choose different transcoding configuration templates.

Note:

Choosing different transcoding configuration templates will specify the encoding method and bitrate settings set by the transcoding template for the playback URL under that domain.



4. Click **Confirm**.

URL format for transcoded streams

After binding a transcoding template, append its name to your playback URL (**playback URL_transcoding template name**). If you do not append the template name, the original stream will be played. For more information on playback URLs, see Playback Configuration.

Suppose the name of the transcoding template bound is **hd**, and the original playback URL is as follows:

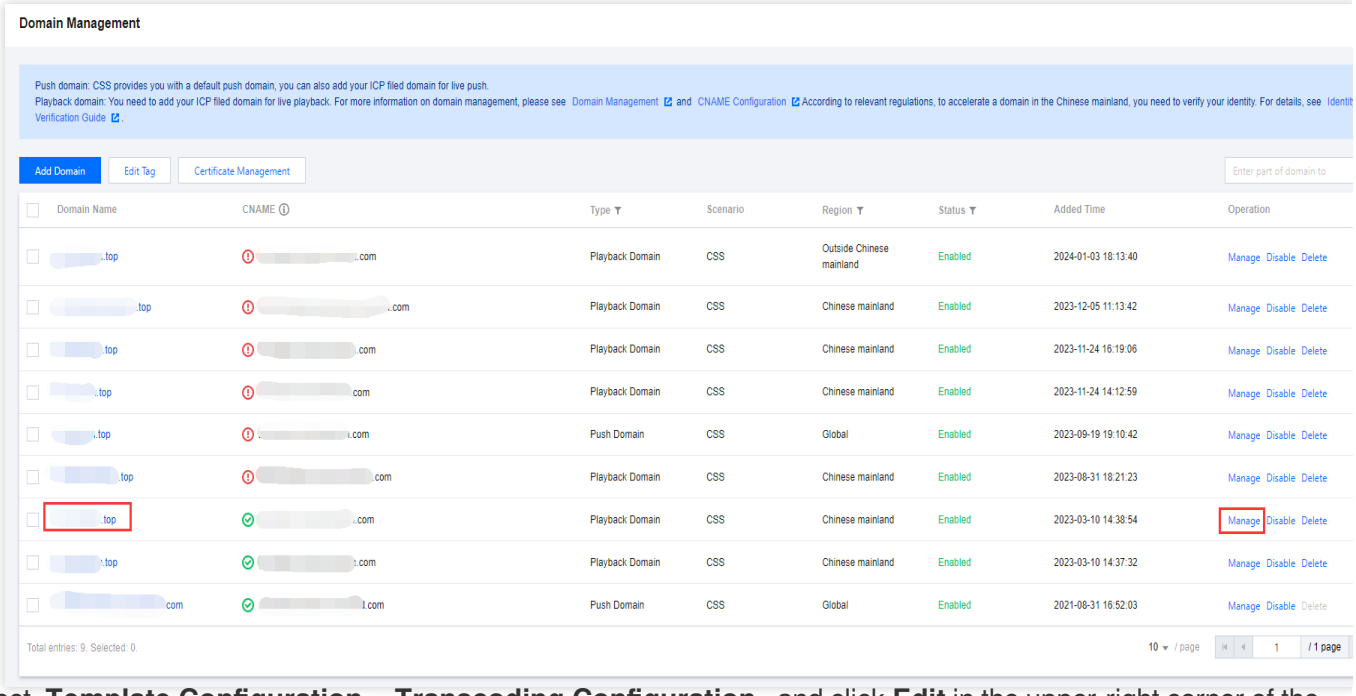
```
http://domain/AppName/StreamName.flv?txSecret=Md5(key+StreamName+hex(time))&txTime=
```

To play the transcoded stream, you need to use the following URL:

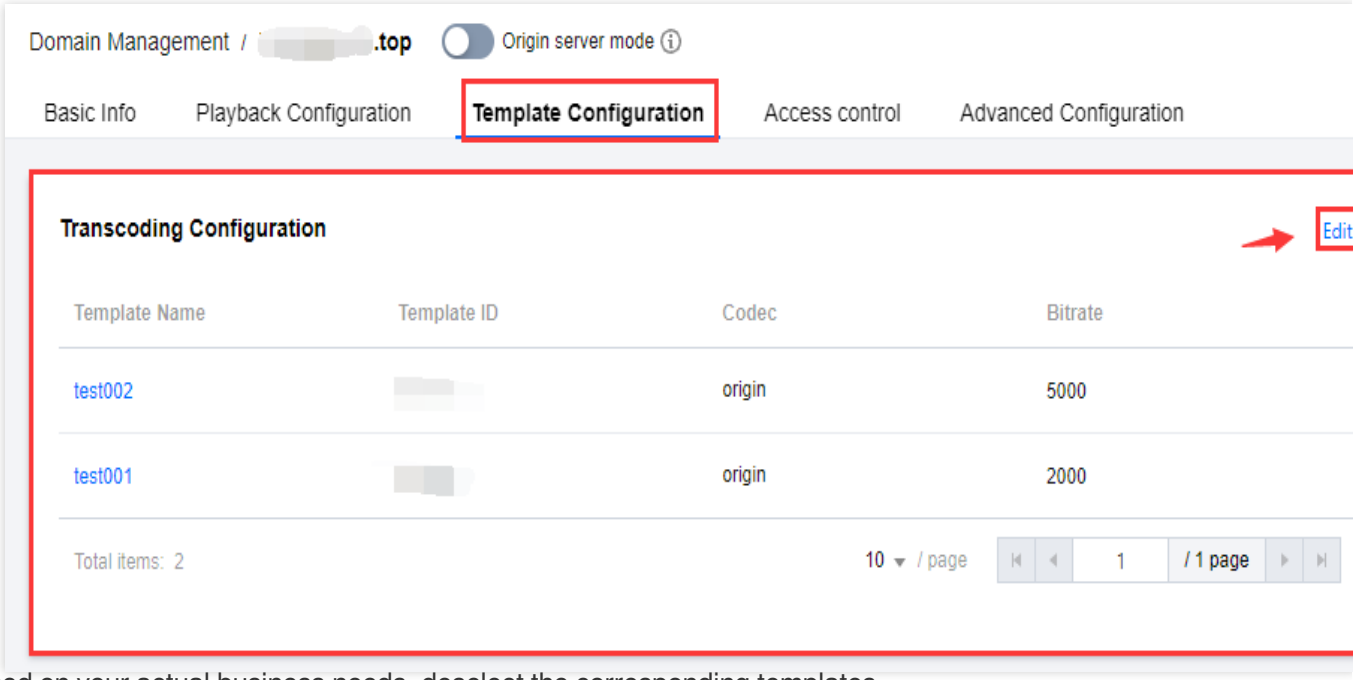
```
http://domain/AppName/StreamName_hd.flv?txSecret=Md5(key+StreamName_hd+hex(time))&t
```

Unbinding a transcoding template

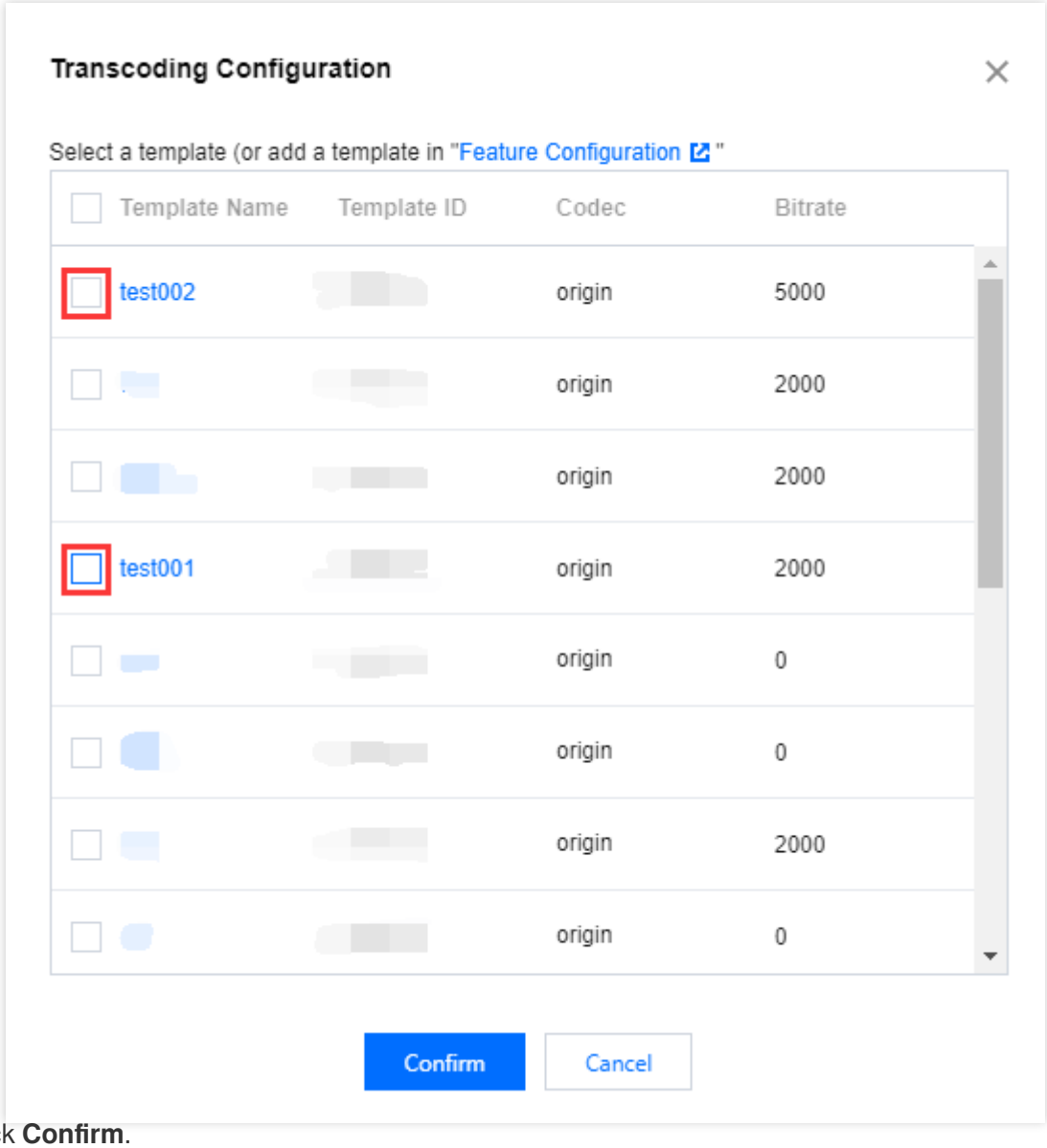
1. Go to Domain Management. Click the name of your playback domain or click **Manage** on the right.



2. Select **Template Configuration > Transcoding Configuration** , and click **Edit** in the upper-right corner of the **Transcoding Configuration** tab.



3. Based on your actual business needs, deselect the corresponding templates.



4. Click **Confirm**.

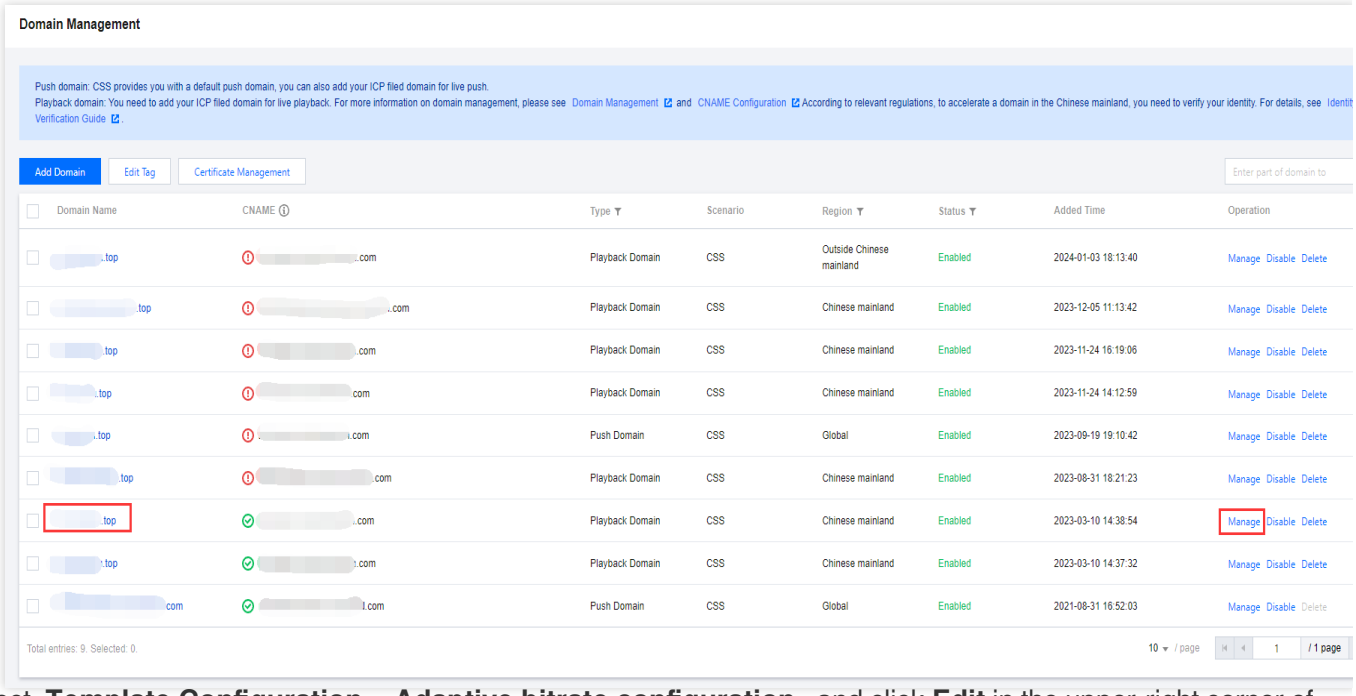
Note

To delete a template, you need to unbind it first and then go to **Feature Configuration** > Live Transcoding to delete it. For details, see Deleting a Template.

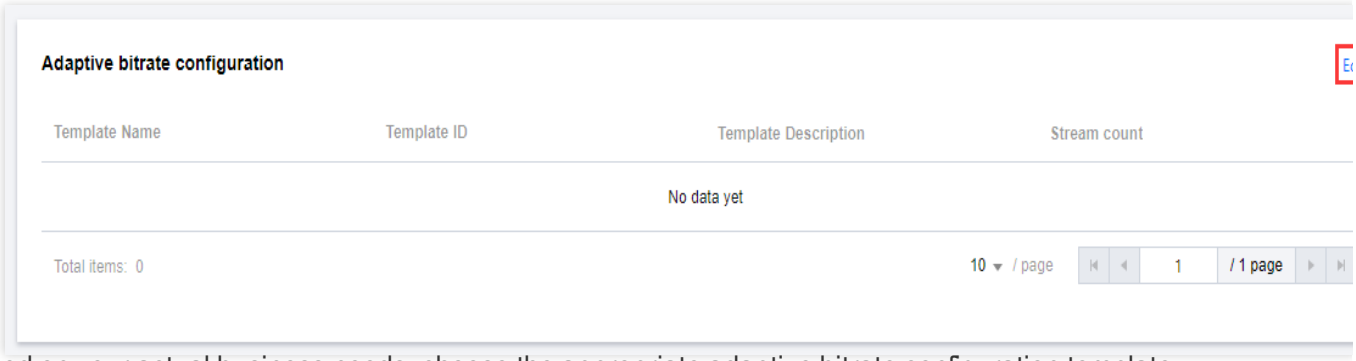
Adaptive Bitrate Template

Binding an adaptive bitrate template

1. Go to Domain Management. Click the name of your playback domain or **Manage** on the right.



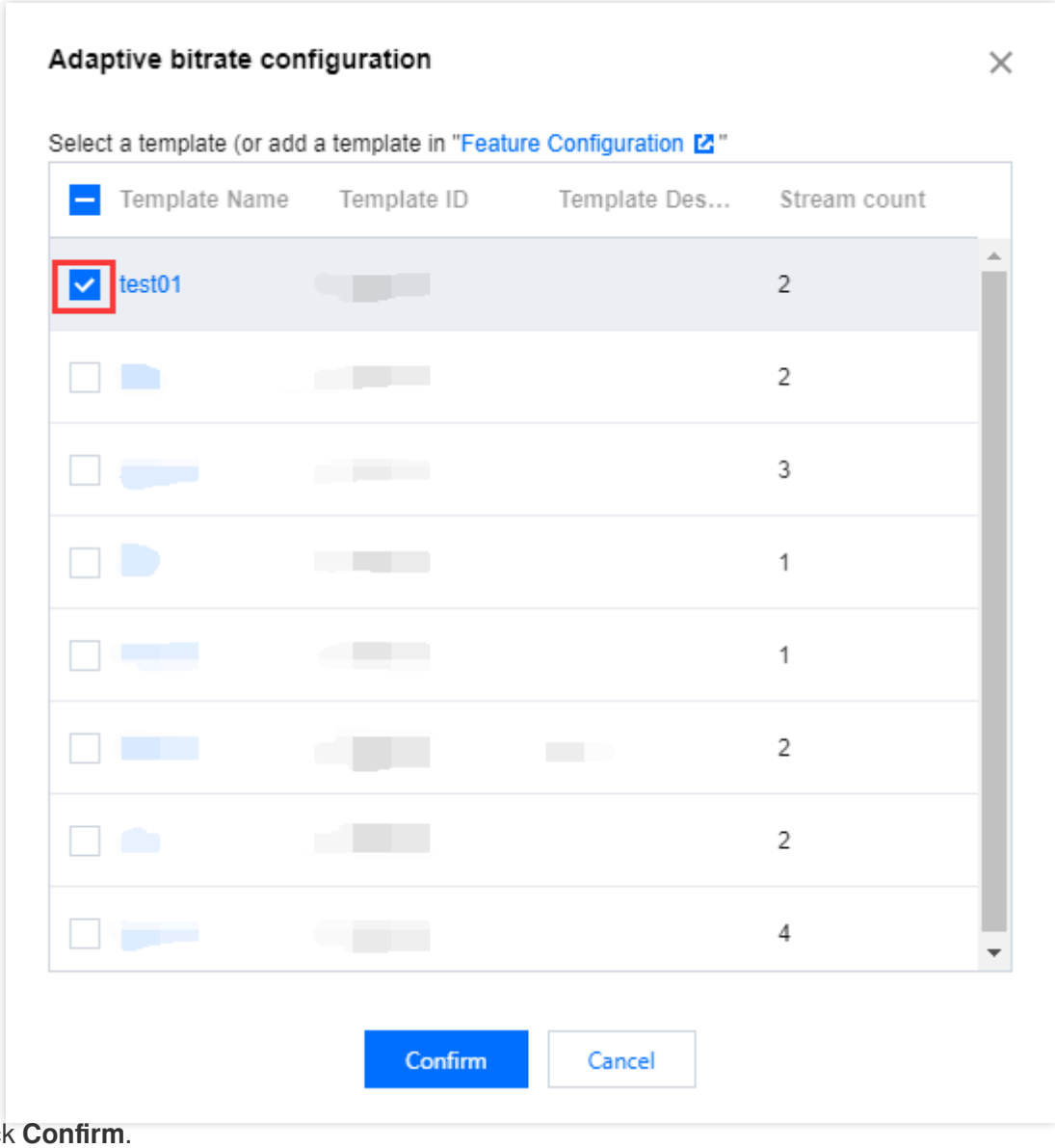
2. Select **Template Configuration > Adaptive bitrate configuration** , and click **Edit** in the upper-right corner of the **Adaptive bitrate configuration** tab .



3. Based on your actual business needs, choose the appropriate adaptive bitrate configuration template.

Note:

Choosing different adaptive bitrate configuration templates will specify the sub-stream information set by the adaptive bitrate template for the playback URL under that domain.



4. Click **Confirm**.

Adaptive bitrate URL format

Only HLS and WebRTC are supported for adaptive bitrate playback. The URL formats for the two protocols are different. For details, see Playback Configuration.

HLS URL:

Suppose the name of the adaptive bitrate template bound is **autobitrate**, and the original playback URL is as follows:

```
http://domain/AppName/StreamName.m3u8?txSecret=Md5(key+StreamName+hex(time))&txTime
```

To play the transcoded stream, you need to use the following URL:

```
http://domain/AppName/StreamName_autobitrate.m3u8?txSecret=Md5(key+StreamName_autob
```

WebRTC URL:

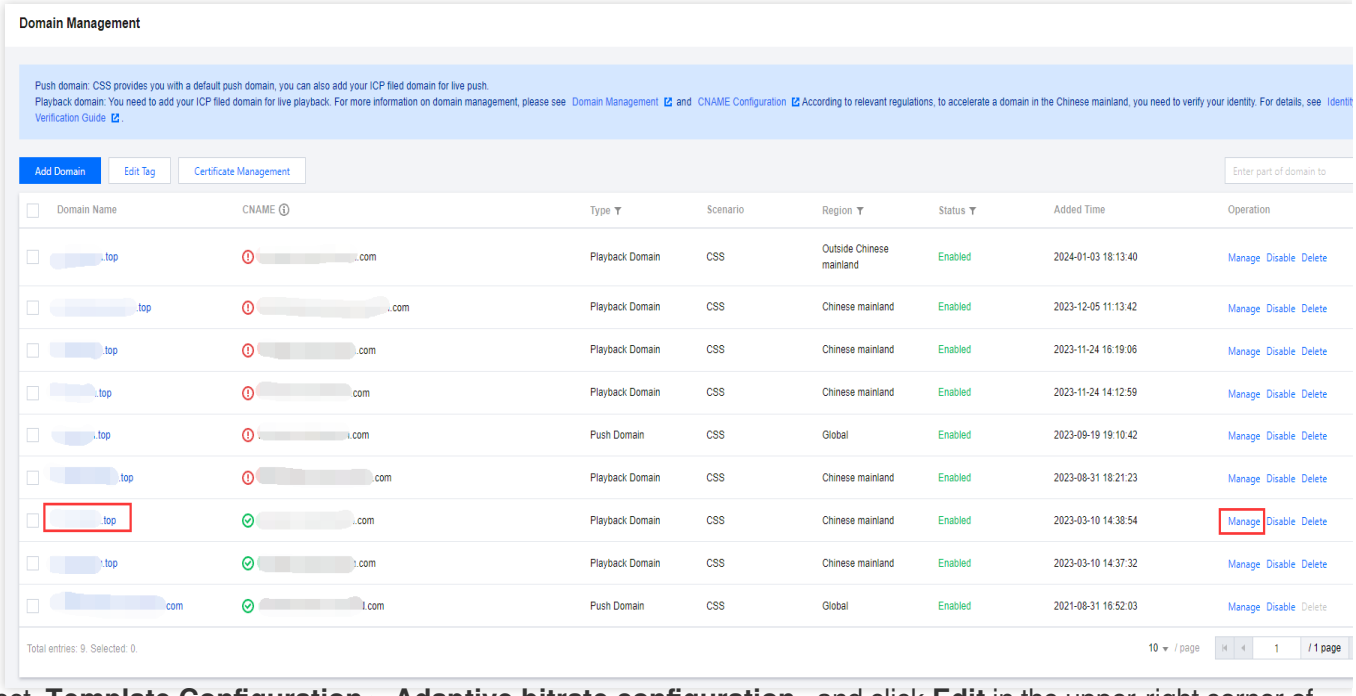
Suppose the adaptive bitrate template bound has three streams. Their names are "test 1", "test 2", and "test 3", and their bitrates are 200 Kbps, 300 Kbps, and 400 Kbps respectively.

The adaptive bitrate playback URL would be as follows:

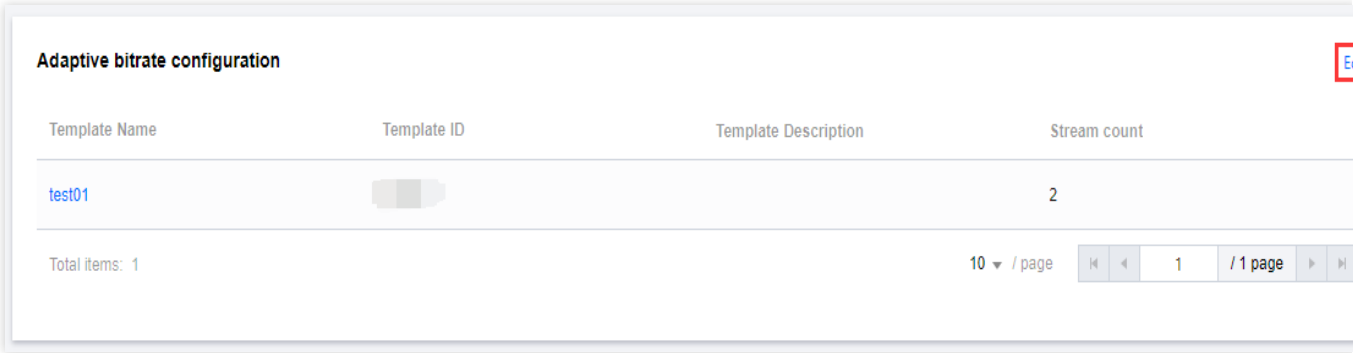
```
webrtc://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time))&txTime=he
```

Unbinding an adaptive bitrate template

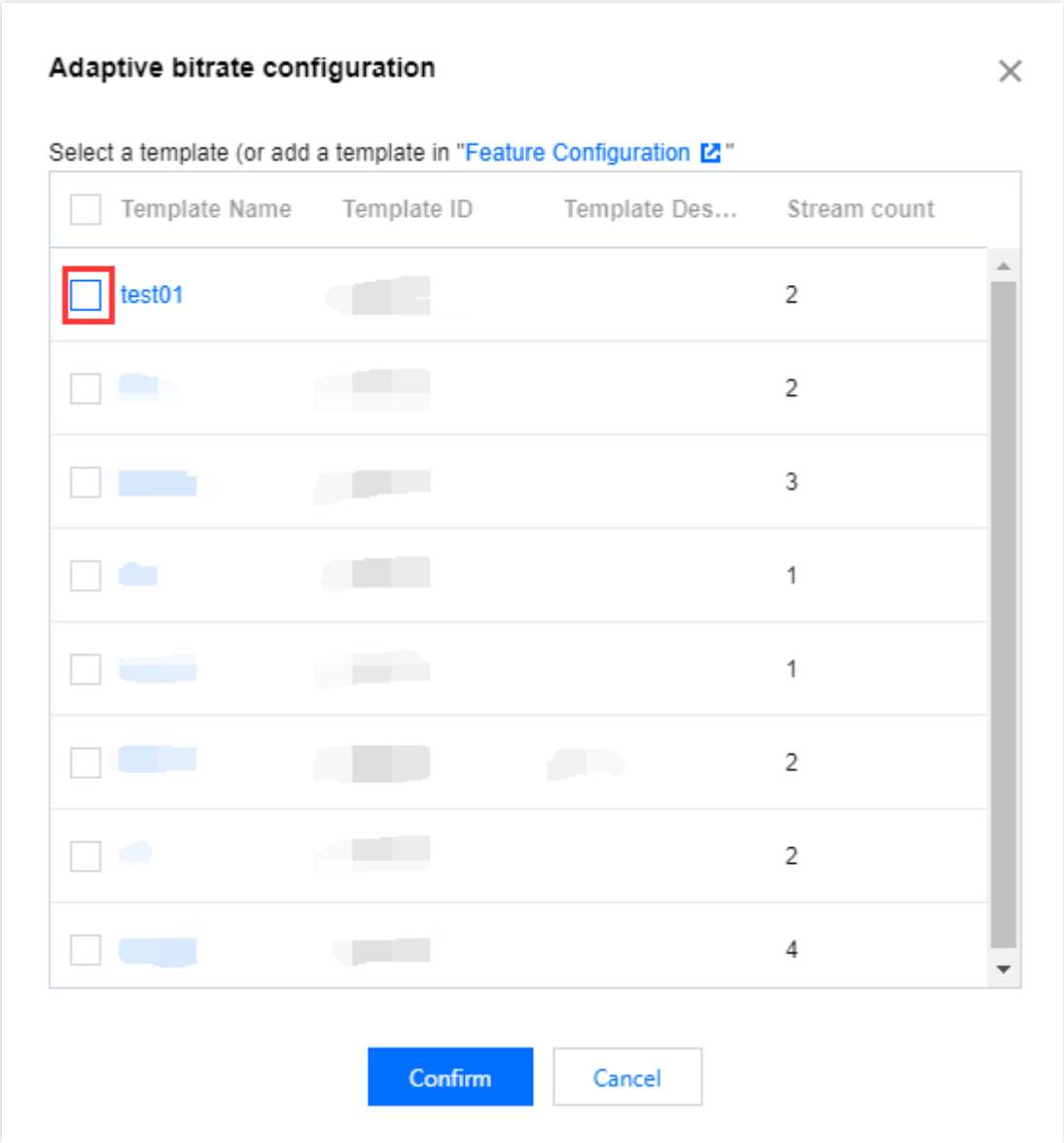
1. Go to Domain Management. Click the name of your playback domain or click **Manage** on the right.



2. Select **Template Configuration > Adaptive bitrate configuration** , and click **Edit** in the upper-right corner of the **Adaptive bitrate configuration** tab .



3. Based on your actual business needs, deselect the corresponding templates.



4. Click **Confirm**.

Note

To delete a template, you need to unbind it first and then go to **Feature Configuration** > Live Transcoding to delete it. For details, see Deleting a Template.

HTTPS Configuration

HTTPS Configuration

Last updated：2025-02-08 11:42:31

Overview

The HTTPS protocol is a network protocol built based on the SSL and HTTP protocols for encrypted transfer and authentication, which is more secure than the HTTP protocol. If you want to enable HTTPS acceleration, you can do so by enabling the HTTPS feature for the playback domain name and configuring a correct and valid certificate. You can purchase a certificate from Tencent Cloud SSL Certificate Service. If you already have one, you can upload it to the CSS console for configuration. Currently, CSS only supports the PEM format. If your certificate is in another format, you need to convert it to PEM format first. The format requirements and configuration method for the certificate are as follows:

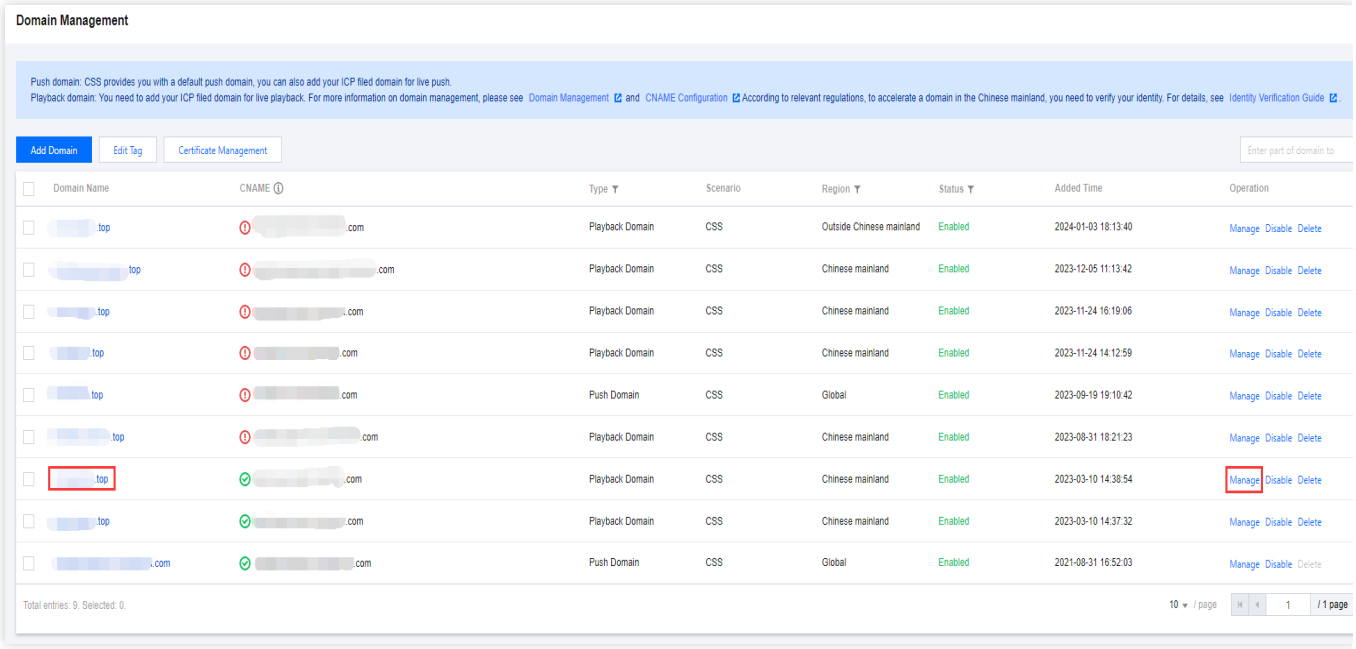
Prerequisites

You have logged in to the CSS console.
You have added a playback domain name.

Directions

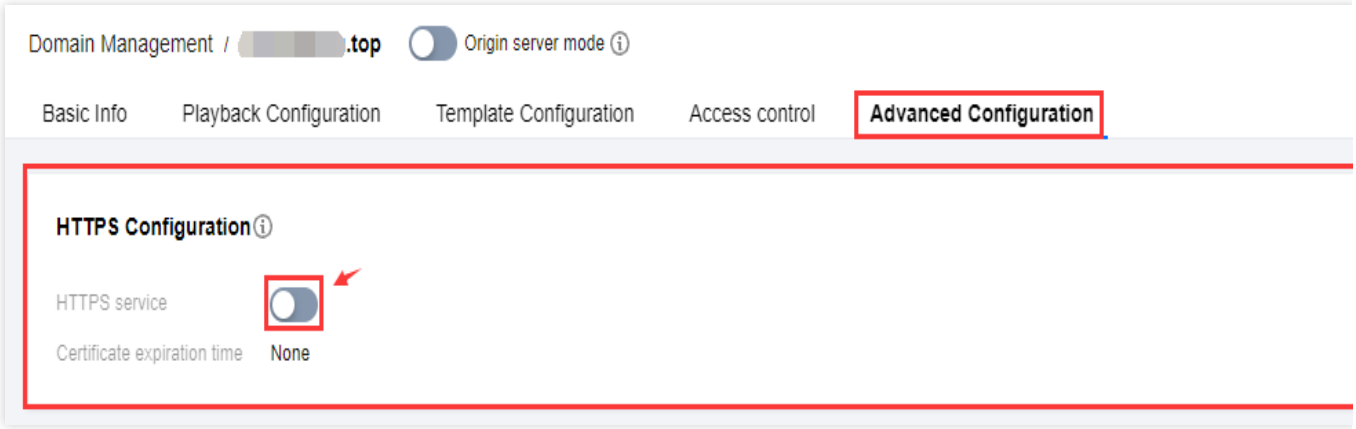
Step 1. Edit the HTTPS configuration

1. Enter **Domain Management** and click the **playback domain name** to be configured or **Manage** on the right to enter the domain name details page.

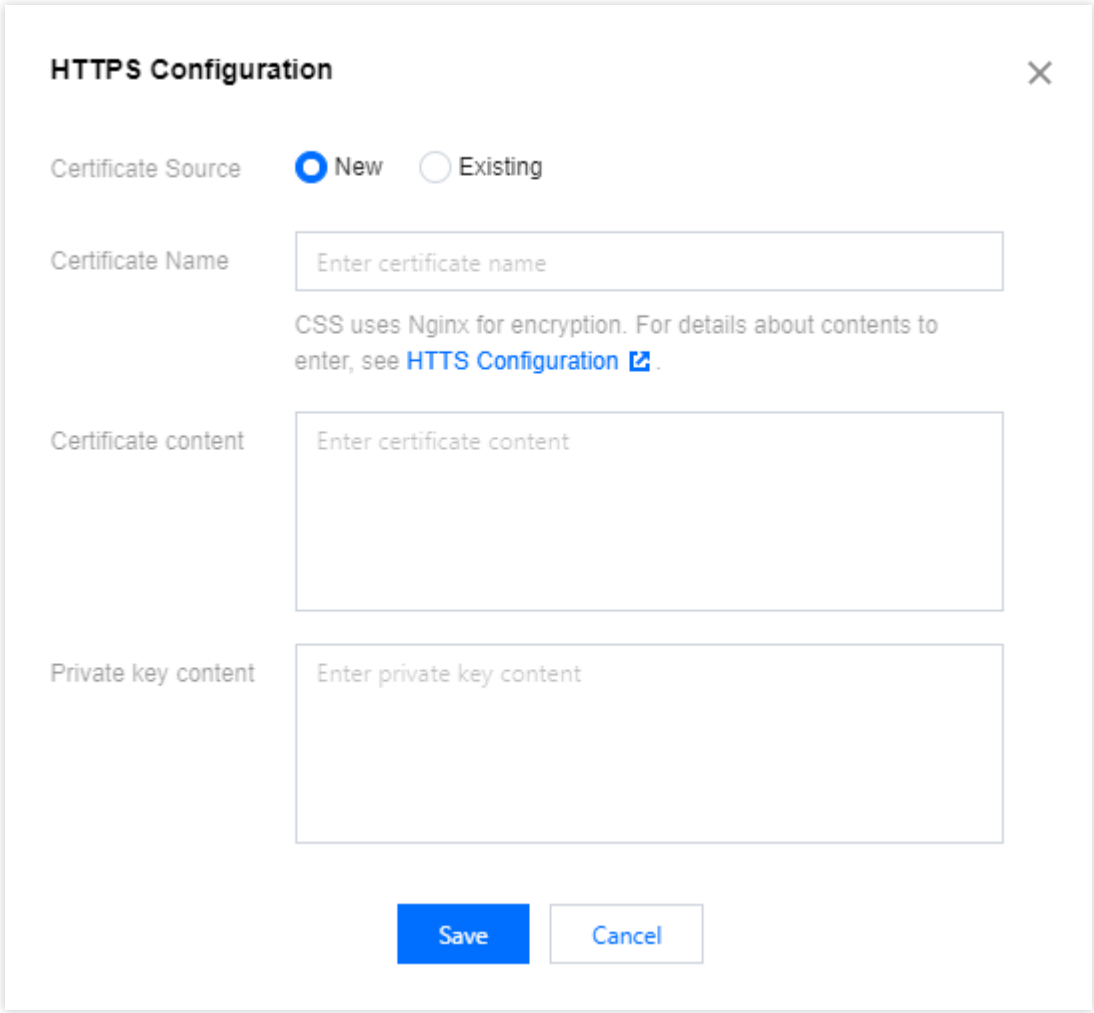


2. Select **Advanced Configuration** > **HTTPS Configuration**, then click

to enable the HTTPS service.



3. After enabling the HTTPS service, enter the HTTPS Configuration page.



4. Select the source of the certificate to be configured, enter relevant information, and click **Save**.

Certificate Source	Required Configuration Items
Self-owned certificate	Certificate Name: enter a custom name used to identify the certificate. Certificate Content: enter the content of the .crt file for Nginx. For more information, please see Certificate content. Private Key Content: enter the content of the .key file for Nginx. For more information, please see Certificate key.
Tencent Cloud-hosted certificate	Certificate List: select an uploaded certificate in SSL Certificate Service.

Note:

The HTTPS feature will take effect approximately 2 hours after configuration is completed, please be patient.

Certificate Description

A certificate provided by the CA includes Apache, IIS, Nginx, and Tomcat files. **The encryption service of CSS uses Nginx, so you should select the content of the Nginx files for the configuration.**

Go to **SSL Certificate Service console** > **Certificate Management**, select the target certificate, click **Download** in the "Operation" column, and decompress the downloaded package to get the following files:

Certificate content:

Select the `.crt` file in Nginx and fill in the input box with everything including `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.

Sample content:

```
-----BEGIN CERTIFICATE-----
MIIFvDCCBKSgAwIBAgIQBTo6zUPDP8ibV9JskbZwazANBgkqhkiG9w0BAQsFADBy
MQswCQYDVQQGEwJDTjElMCMGA1UEChMcVHJ1c3RBc2lhIFRlY2hub2xvZ2llcywg
SW5                                                          FRy
dXN                                                          DAw
MFo                                                          kiG
9w0                                                          vfq
9NL                                                          9N9
COm                                                          BhS
js1                                                          MNC
dr9                                                          X7t
75W                                                          jCC
Apo                                                          OsF
CIl                                                          G93
LmN                                                          QQW
MBQ                                                          jAq
MCg                                                          meB
DAE                                                          GF0
dXN                                                          HA6
Ly9                                                          ExT
UlN                                                          gD2
XJQ                                                          EUC
IGQ                                                          Nvh
0GY                                                          KOU
sl7                                                          uEG
MB8                                                          QYJ
KoZ                                                          kT9
oru                                                          OKJ
ivf                                                          dgJ
BH6                                                          EHi
UkP/Y5/sTG9A28P6MDpOj31h/RhQFdWsMDA8yxPAvDiyQ8PJ3UoqRdx/1PxFA+My
+OvIvbbMI4aPJvoA80654H1RmTsWOeL9ghPXIOyneKc=
-----END CERTIFICATE-----
```

Note:

If your certificate is issued by an intermediate CA and contains multiple certificates, the certificate content should be spliced as follows:

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

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

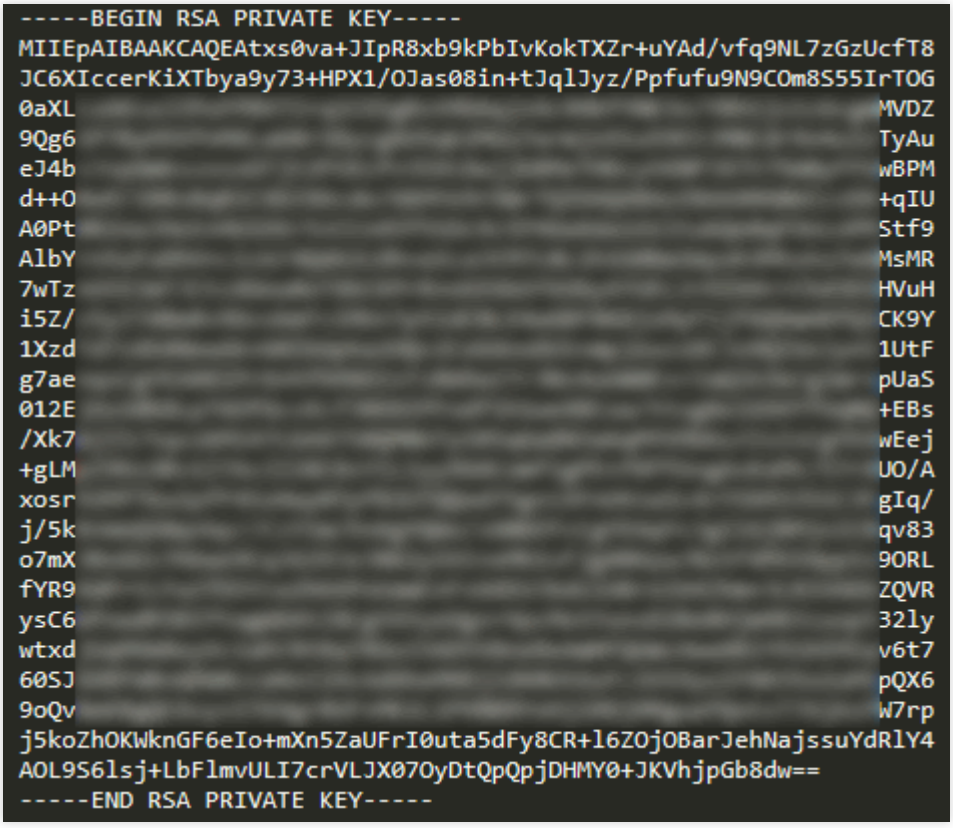
-----BEGIN CERTIFICATE-----

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

Certificate private key:

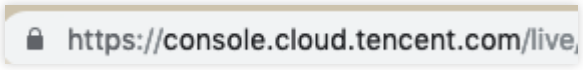
enter the entire content between `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` in the `.key` file for Nginx.

Sample content:



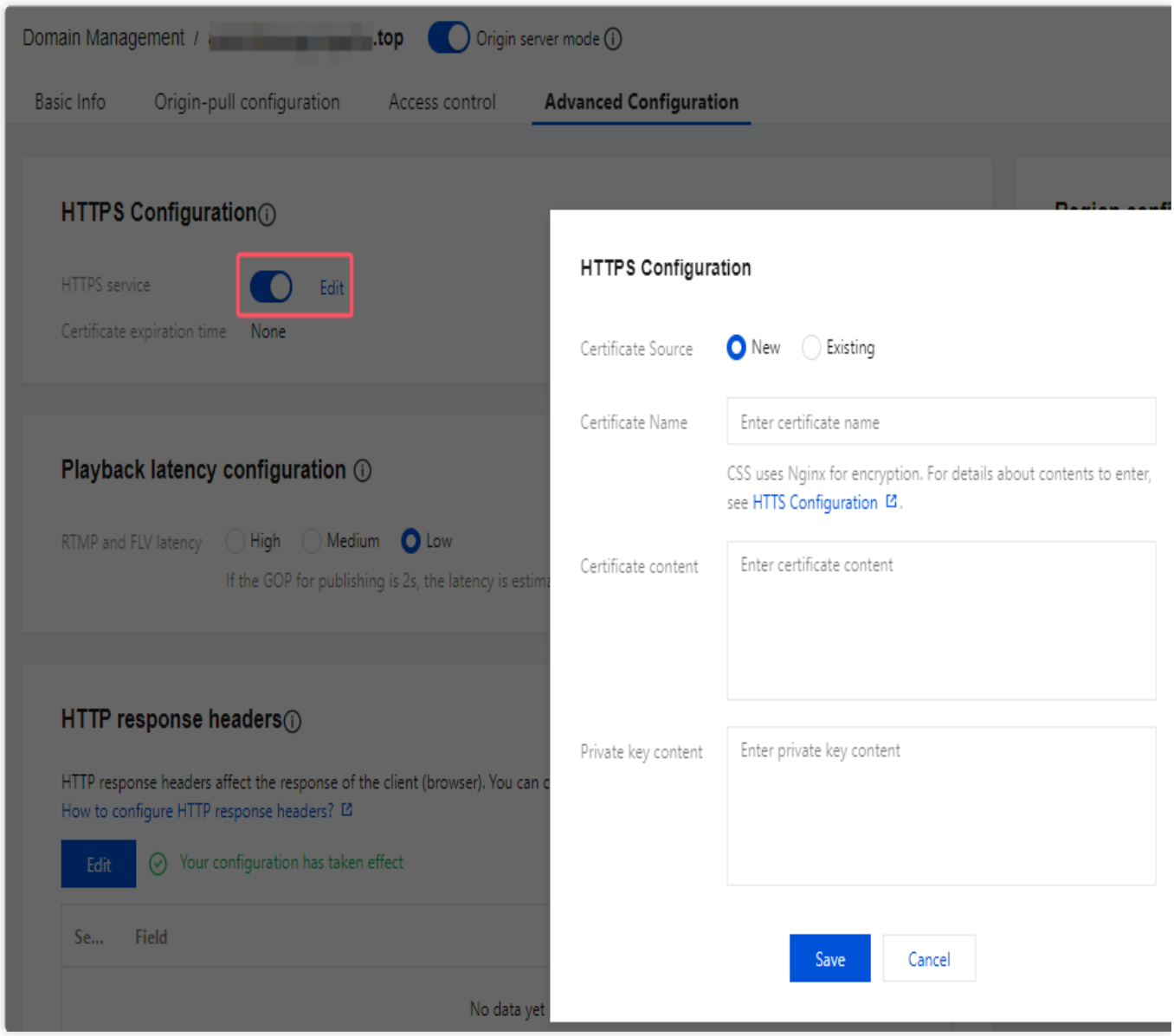
Step 2. Verify the configuration

The HTTPS configuration will take effect in about 2 hours. Please visit the domain name about 2 hours after the certificate is submitted. If HTTPS is displayed in the address bar of the browser, the configuration is successful.



Step 3. Modify the configuration

The configuration can be modified if the HTTPS function is turned on. If this feature is turned off, editing will not be possible. Once it is disabled, CSS will no longer provide HTTPS service for the domain name. If the certificate has expired, it should be replaced with a new valid one.



FAQs

HTTP/2 Configuration

Last updated：2024-10-30 16:02:45

Overview

HTTP/2 (HTTP/2.0) is upgraded from HTTP/1.1. Compared with HTTP/1.1, it introduces a range of optimization features, including binary framing, multiplexing, header compression, and server push. These features greatly optimize web performance and reduce data exchange latency. Before enabling HTTP/2 configuration, you need to configure an HTTPS certificate.

Prerequisites

You have logged in to the CSS console.
You have added a playback domain name.
To enable HTTP/2, ensure that HTTPS is correctly configured and enabled, as HTTP/2 depends on HTTPS. Complete the SSL certificate configuration and enable HTTPS before setting HTTP/2. For details, see HTTPS Configuration.
Note:
If you are configuring an HTTPS certificate for the first time, wait until the certificate configuration is completed and takes effect before enabling HTTP/2.
If you disable the HTTPS certificate feature, the HTTP/2 settings will be automatically disabled and cannot be enabled.
When HTTP/2 is enabled, if the HTTPS certificate feature is disabled, HTTP/2 will be automatically disabled.

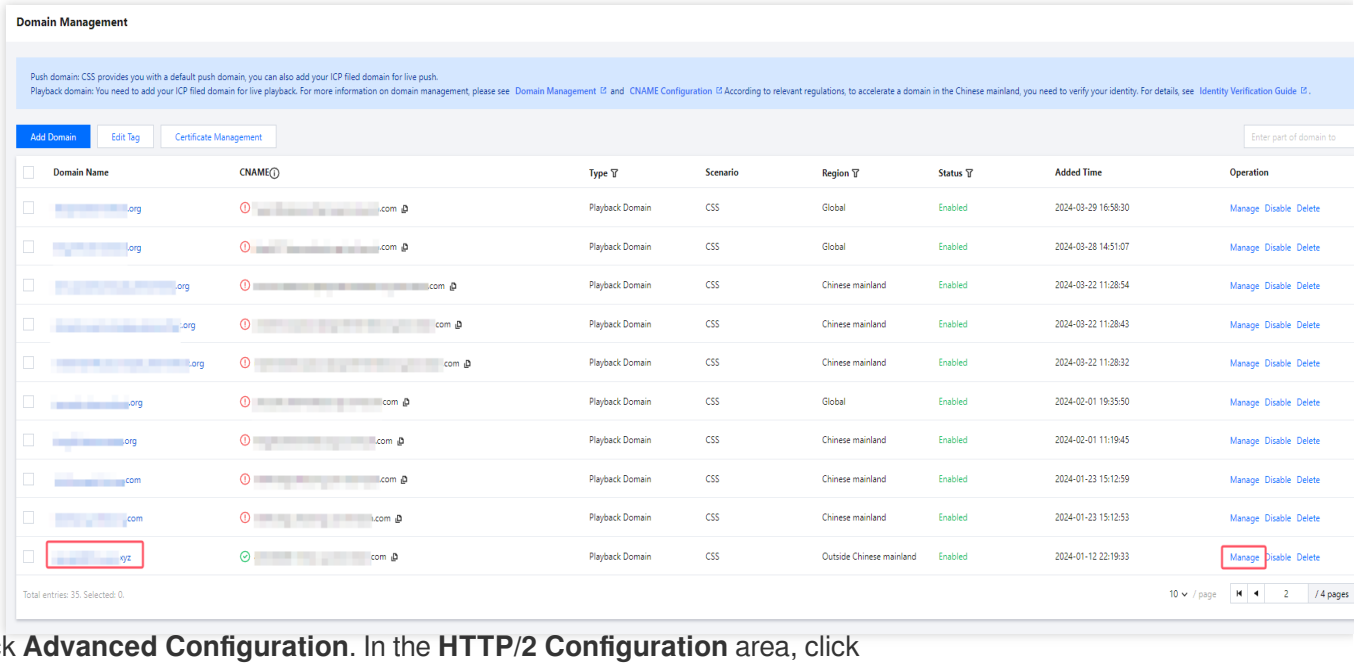
Notes

Currently, only HTTP/2 access is supported. HTTP/2 origin-pull is not supported.
If the domain name's service region is global, the HTTP/2 configuration will take effect globally. Separate configurations inside and outside the Chinese mainland are not supported.

Configuration Guide

Enabling or Disabling HTTP/2 Configuration

1. Enter Domain Management, click the **playback domain name** you want to configure or **Manage** on the right to enter the domain name detail page.



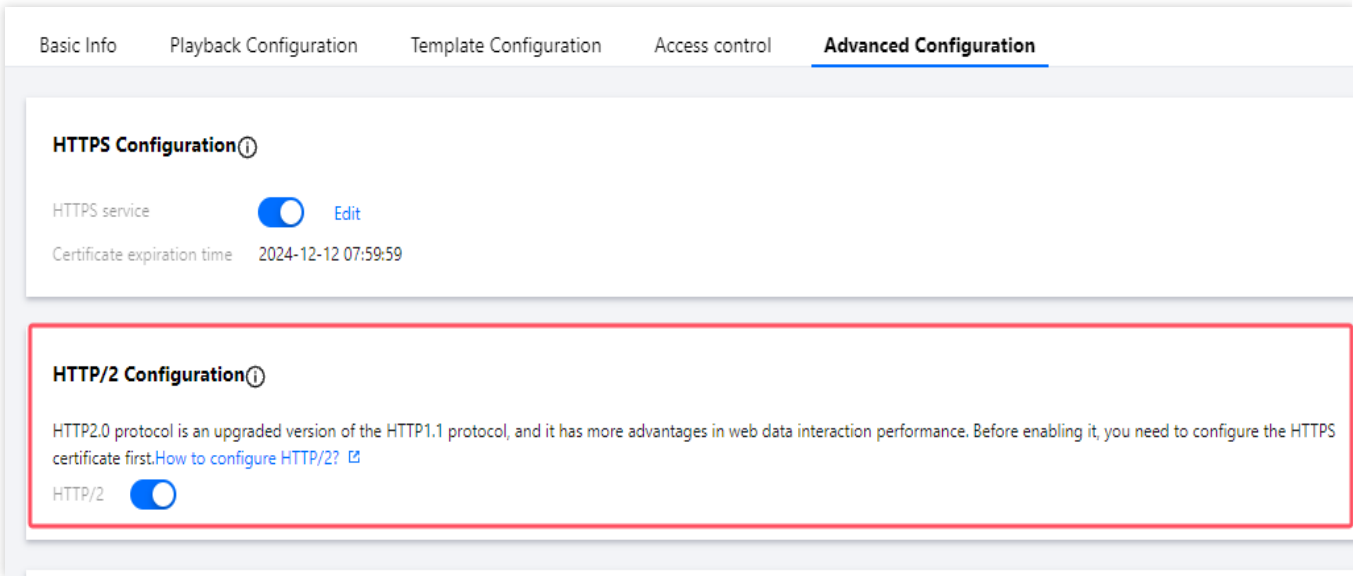
2. Click **Advanced Configuration**. In the **HTTP/2 Configuration** area, click

to enable or disable the **HTTP/2** feature.

Note:

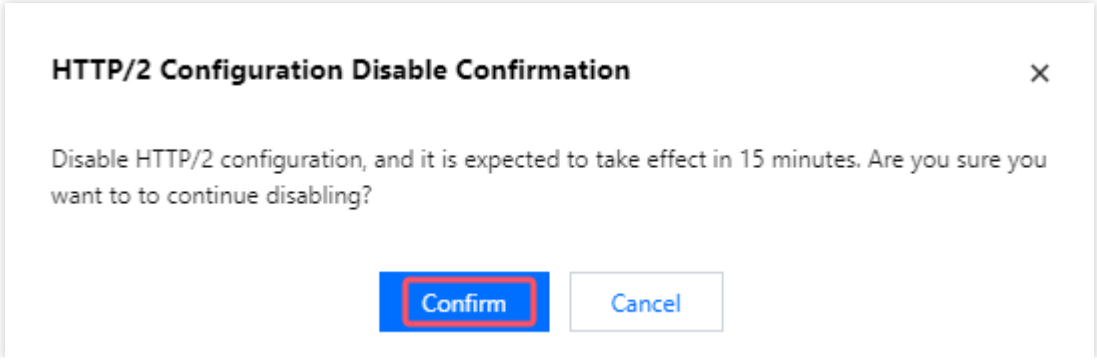
Complete the SSL certificate configuration and enable HTTPS before enabling HTTP/2 in the **HTTP/2 Configuration** area.

The HTTP/2 feature will take effect approximately 15 minutes after configuration.



When you highlight the switch, **HTTP/2** is enabled.

When you turn the switch gray, **HTTP/2** is disabled and the **HTTP/2** configuration is automatically invalidated.


HTTP/2 Configuration Disable Confirmation
Disable HTTP/2 configuration, and it is expected to take effect in 15 minutes. Are you sure you want to to continue disabling?
Confirm
Cancel

TLS Version Configuration

Last updated：2024-12-25 14:42:51

Background

The Transport Layer Security (TLS) protocol aims to ensure the security and confidentiality of data exchanged between two applications. Currently, four versions of the TLS protocol are available, including TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. Earlier versions are more compatible but less secure, while later versions are more secure but less compatible.

Description of TLS Protocol Versions

TLS Protocol Version	Supported Mainstream Browser
TLS 1.0	IE6+
	Chrome 1+
	Firefox 2+
TLS 1.1	IE 11+
	Chrome 22+
	Firefox 24+
	ME 12+
	Safari 7+
	Opera 12.1+
TLS 1.2	IE 11+
	Chrome 30+
	ME 12+
	Firefox 27+
	Safari 7+
	Opera 16+
TLS 1.3	Chrome 70+

	Firefox 63+
	ME 79+
	Safari 14+
	Opera 57+

Using More Secure TLS Encryption Feature of Updated Version to Encrypt Network Connections at Transport Layer

Version	Description
TLS 1.3 (Recommended)	RFC 8446, published in 2018. TLS 1.3 is faster and more secure than TLS 1.2.
TLS 1.2 (Recommended)	RFC 5246, published in 2008. It adopted a strong encryption technology to provide higher security protection.
TLS 1.1	RFC 4346, published in 2006. It fixed several vulnerabilities in TLS 1.0.
TLS 1.0	RFC 2246, published in 1999 based on SSL v3.0. This version is susceptible to various attacks, such as BEAST and POODLE.

Overview

When you have enabled HTTPS configuration, Cloud Streaming Services (CSS) supports multiple TLS versions by default to meet the access needs of various user terminals. Generally, there is no need to modify this configuration. If you have higher security requirements for your website and need to prevent user access by using TLS versions of lower security, you can customize the SSL/TLS versions. CSS supports TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3 by default. You can disable/enable specific TLS versions based on your business needs.

Prerequisites

You have logged in to the CSS console.
You have added a playback domain name.
To modify the TLS version configuration, you need to first ensure that HTTPS is correctly configured and enabled, as the TLS version configuration depends on HTTPS. Before setting the TLS version, complete the SSL Certificates configuration and enable HTTPS. For operation methods, refer to HTTPS Configuration.

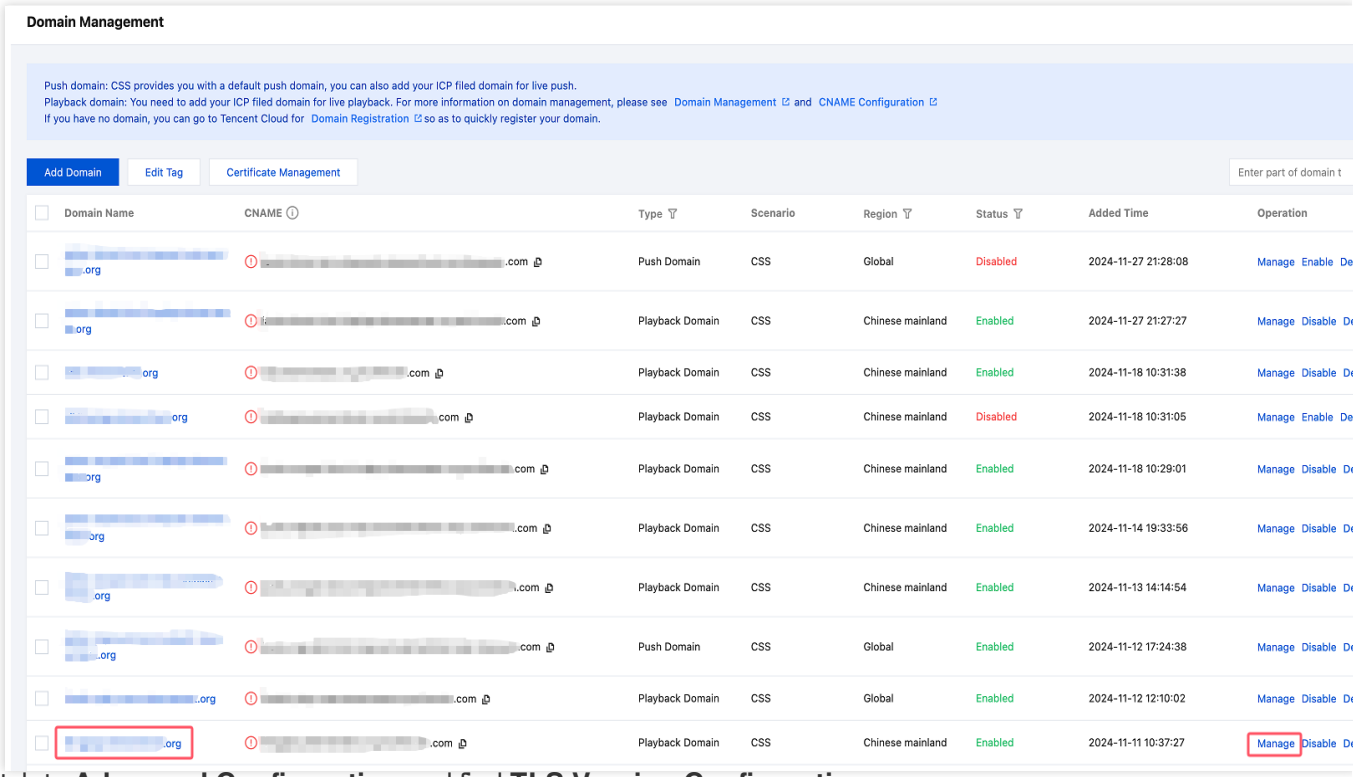
Notes

The TLS version configuration will take effect approximately 15 minutes after completion.
Downgrading the TLS version (for example, from TLS 1.2 to TLS 1.1 or TLS 1.0) or disabling the TLS version configuration may cause security and compliance issues. Proceed with caution.
TLS 1.3 is enabled by default and cannot be disabled.
After the HTTPS configuration is disabled, the console will hide the TLS version configuration.
Disabling the HTTPS configuration will lead the TLS version configuration failure.
If you change the TLS version after enabling the HTTPS configuration, and then disable the HTTPS configuration, the TLS version will remain as the previously selected version upon re-enabling of HTTPS next time.

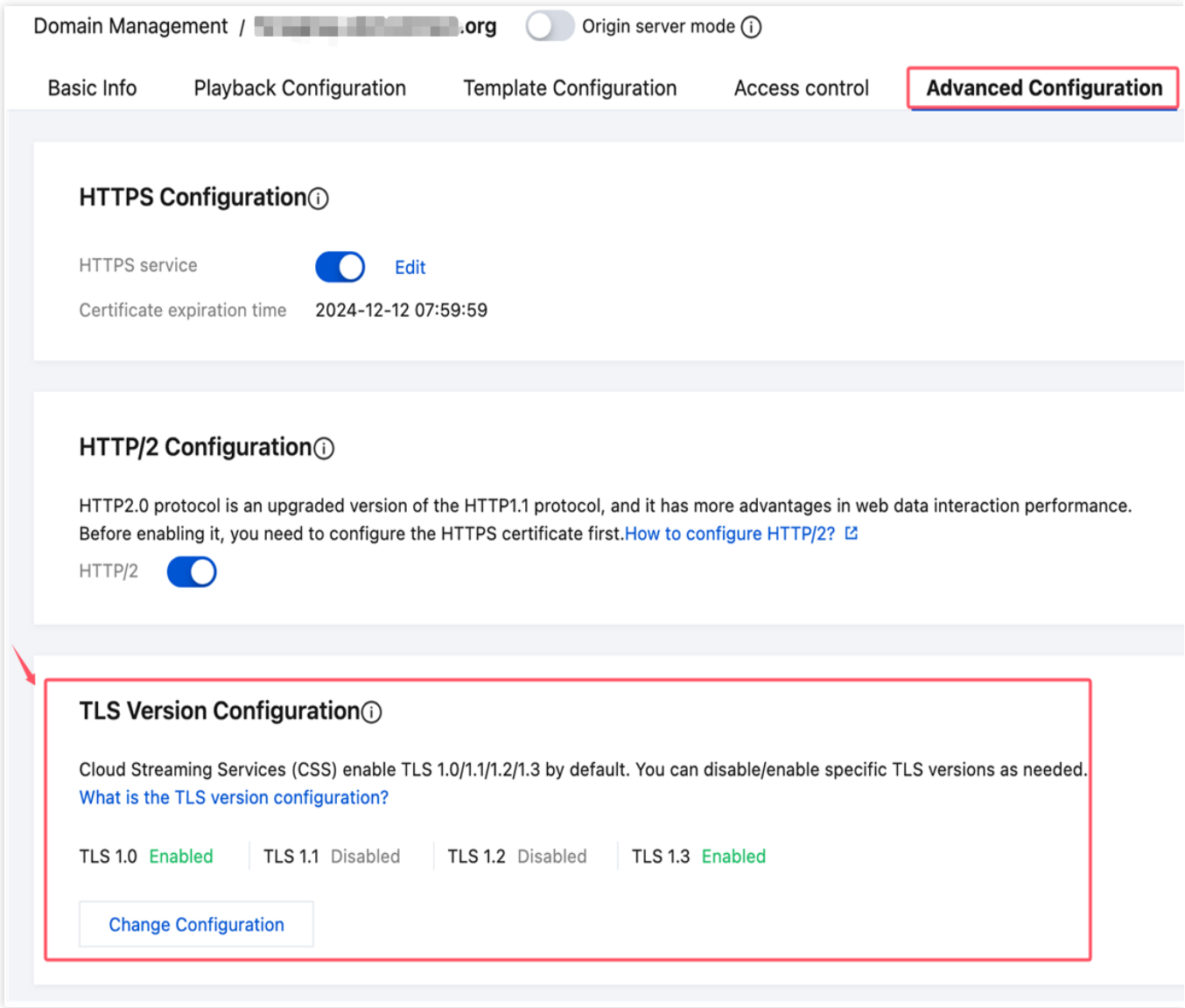
Configuration Guide

Viewing TLS Version Configuration

1. Enter Domain Management, and click the **playback domain** you want to configure or **Manage** on the right to enter the domain detail page.

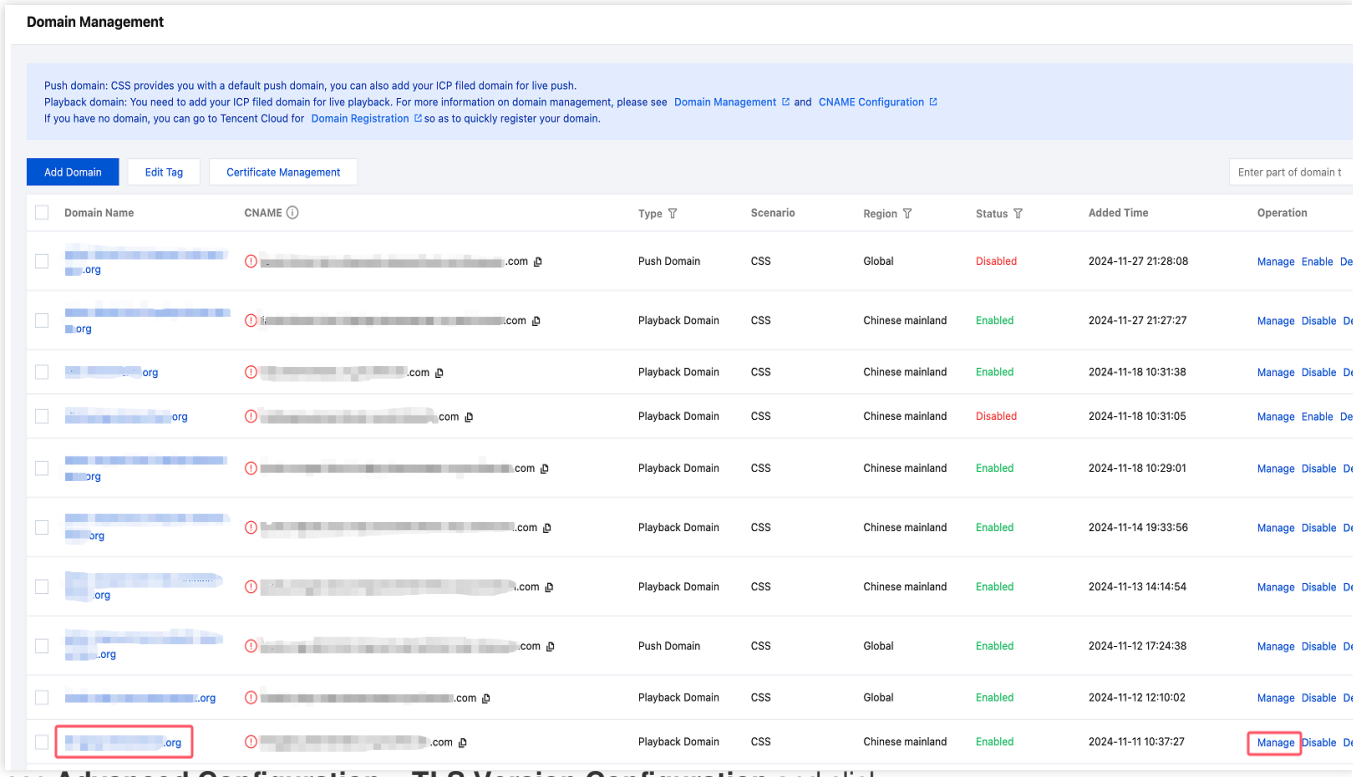


2. Switch to **Advanced Configuration** and find **TLS Version Configuration**.

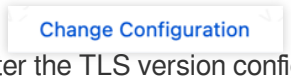


Modifying TLS Version Configuration

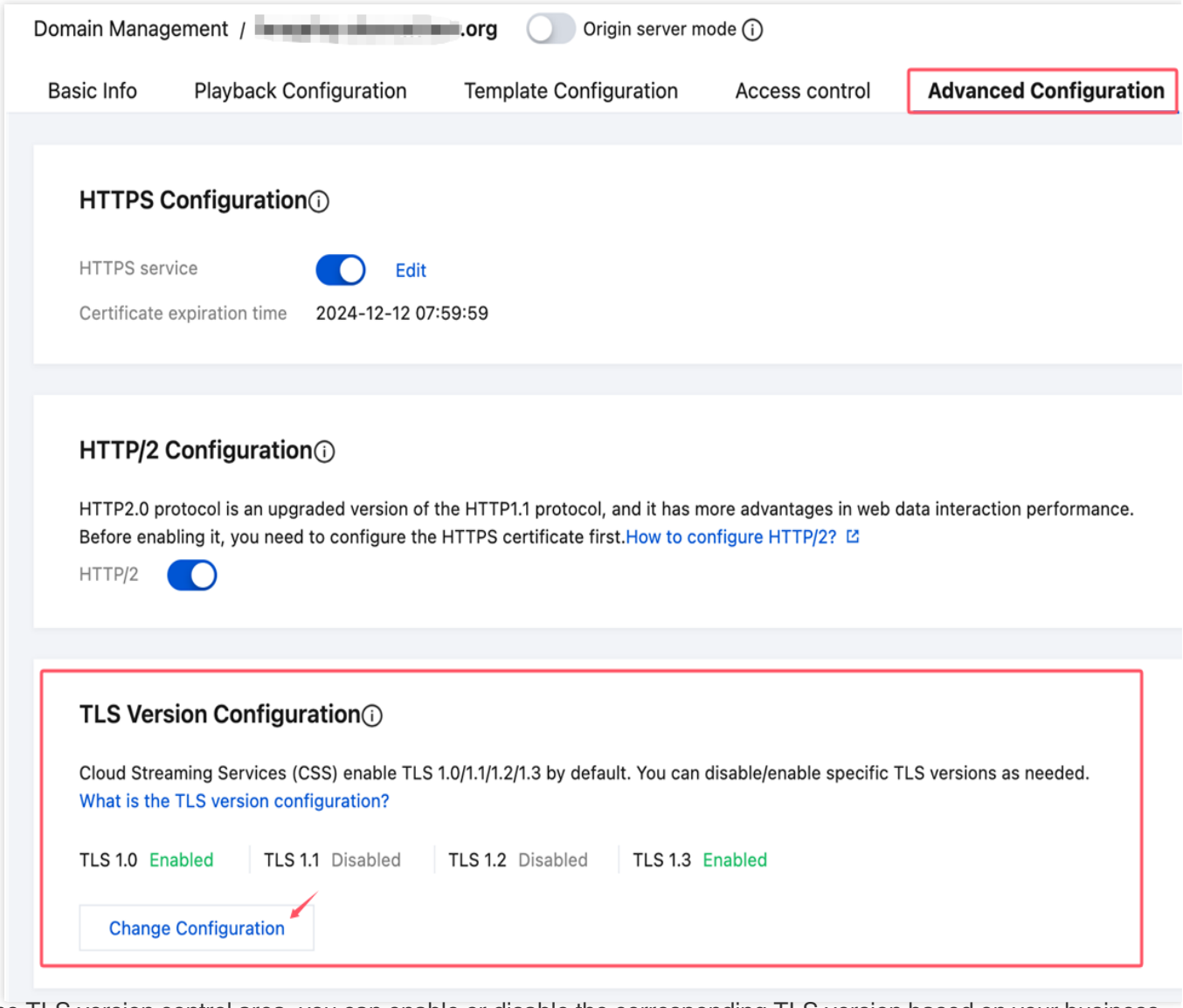
1. Enter Domain Management, and click the **playback domain** you want to configure or **Manage** on the right to enter the domain detail page.



2. Choose **Advanced Configuration** > **TLS Version Configuration** and click



to enter the TLS version configuration modification page.

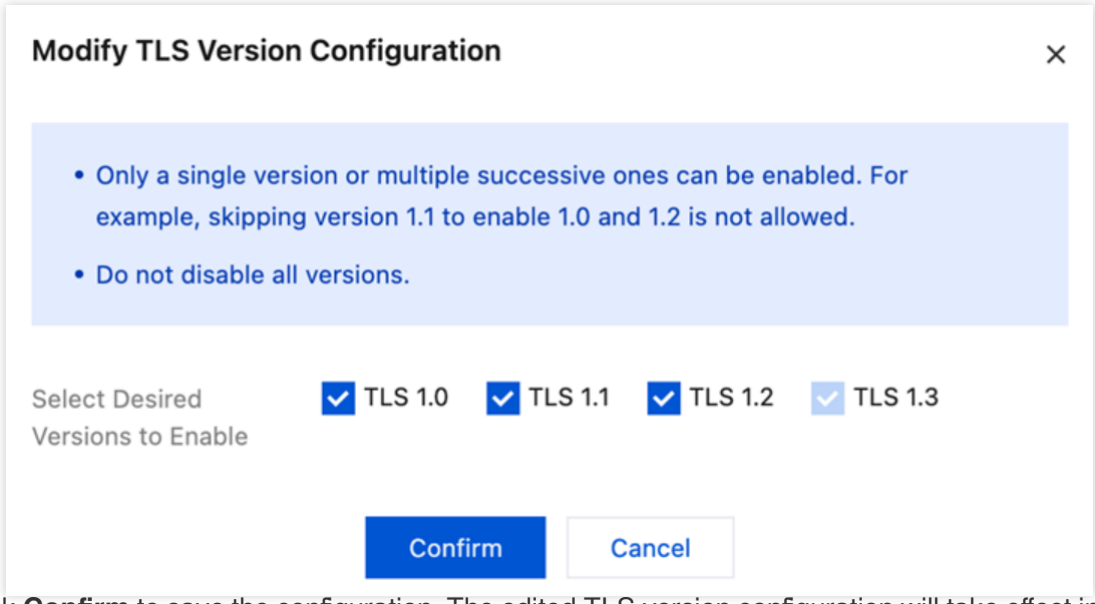


3. In the TLS version control area, you can enable or disable the corresponding TLS version based on your business needs.

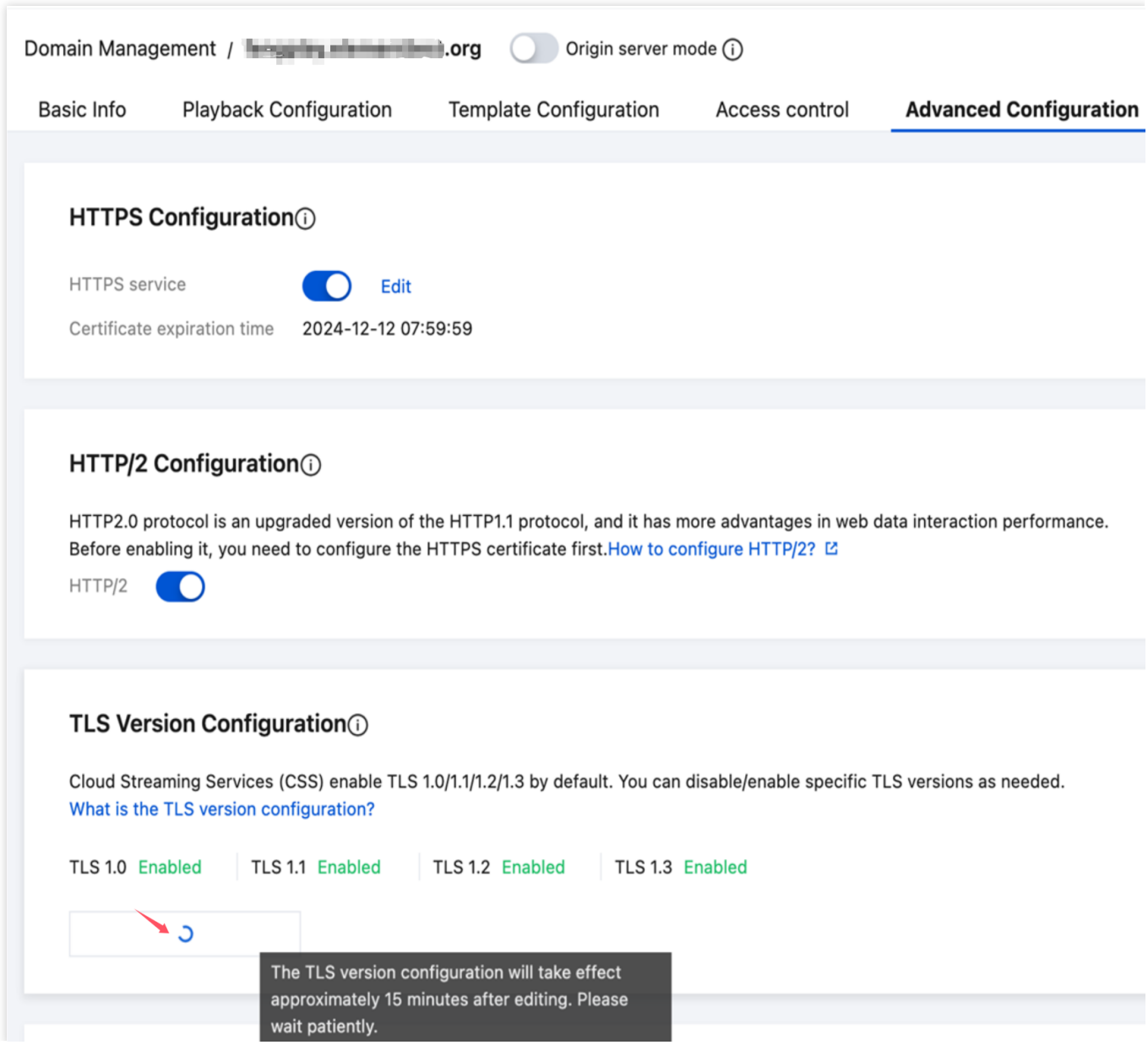
Note:

You can enable a single version or multiple consecutive ones. For example, you can concurrently enable versions 1.0, 1.1, and 1.2, but not versions 1.0 and 1.2.

You cannot disable all versions.



4. Click **Confirm** to save the configuration. The edited TLS version configuration will take effect in about 15 minutes. Please be patient.


Domain Management / .org
Origin server mode
Basic Info
Playback Configuration
Template Configuration
Access control
Advanced Configuration
HTTPS Configuration
HTTPS service
Edit
Certificate expiration time
2024-12-12 07:59:59
HTTP/2 Configuration
HTTP2.0 protocol is an upgraded version of the HTTP1.1 protocol, and it has more advantages in web data interaction performance. Before enabling it, you need to configure the HTTPS certificate first.How to configure HTTP/2?
HTTP/2
TLS Version Configuration
Cloud Streaming Services (CSS) enable TLS 1.0/1.1/1.2/1.3 by default. You can disable/enable specific TLS versions as needed.
What is the TLS version configuration?
TLS 1.0 Enabled
TLS 1.1 Enabled
TLS 1.2 Enabled
TLS 1.3 Enabled
The TLS version configuration will take effect approximately 15 minutes after editing. Please wait patiently.

Region Configuration

Last updated：2025-04-10 17:24:47

To use content delivery, acceleration, and playback services in a different region, you can change the acceleration region for your playback domain in the CSS console.

Prerequisites

You have logged in to the CSS console.
You have added a **playback domain name**.
Note:
In the process of adding a new domain and selecting a playback domain, please choose the acceleration region required for live broadcast distribution, such as "Chinese mainland". Subsequently, fill in the domain name and tag information optionally. Click on **Add Domain and proceed to the next step**.

Notes

CSS pricing differs inside and outside the Chinese mainland. For details, see Billing Overview**.**
A playback domain cannot be used outside its acceleration region.
If the accelerated region includes the Chinese mainland, you need to apply for ICP filing for your playback domain.
Changing the acceleration region will reset the bandwidth cap. You need to configure it again.

Directions

1. Go to Domain Management. Click the name of your **playback domain** or **Manage** on the right.

2. Select the **Advanced Configuration** tab and find **Region configuration**.
3. Click **Edit**. In the pop-up window, you can change the acceleration region to **Chinese mainland**, **Global**, or **Outside Chinese mainland**.

4. Click **Save**.

Acceleration Region	ICP Filing Required	Description
Chinese mainland	Yes	Cannot handle requests outside the Chinese mainland.
Global	Yes	Acceleration is supported globally, but prices differ inside and outside the Chinese mainland.
Outside Chinese mainland	No	Cannot handle requests inside the Chinese mainland. Prices differ inside and outside the Chinese mainland.

Origin Server Configuration

Last updated：2025-01-15 17:45:21

If you have a self-built origin server and live streaming source, CSS can pull streams from your origin server and distribute the content for you. This document describes how to configure origin server information for a playback domain in the CSS console.

Limits

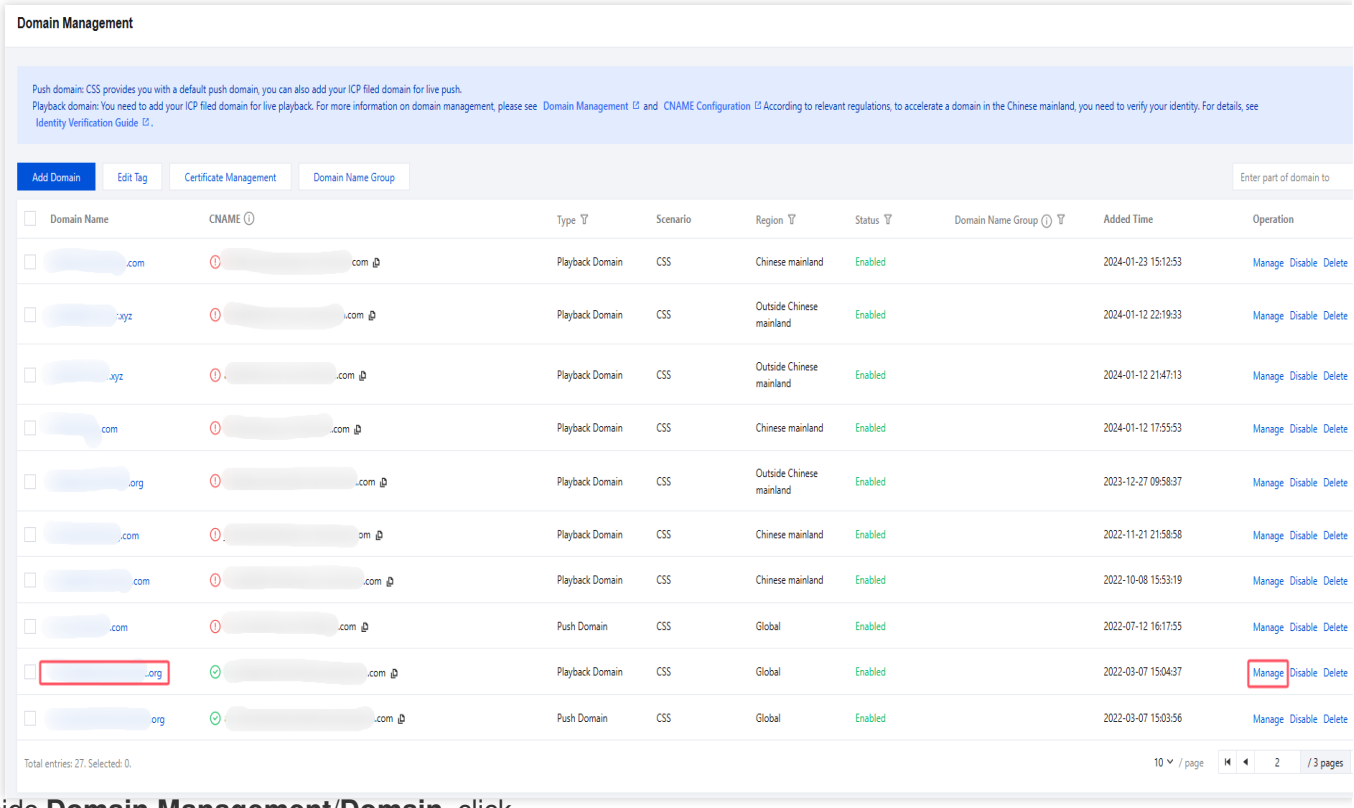
Origin server configuration takes effect about one hour after configuration is complete.
After configuring an origin server for a playback domain, you can no longer bind a push domain to the playback domain by specifying a `StreamName`. Nor can you configure watermarking, transcoding, recording, screenshot, or porn detection tasks for the playback domain.
Upon completing the origin-pull configuration in the console, should you require to further set a whitelist for the service IP during Tencent Cloud Live's origin-pull process, please submit a ticket to obtain the list of origin-pull IP ranges. Additionally, provide the relevant domain names (estimated usage) for backend assessment and configuration.

Prerequisites

You have logged in to the CSS console.
You have built a live streaming origin server.
You have added a **playback domain name**.

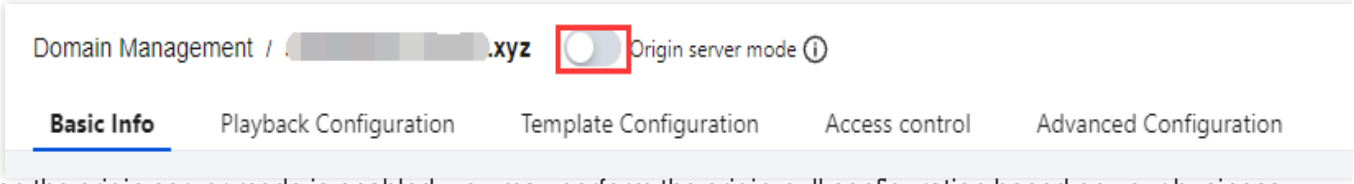
Origin-Pull Configuration

You can edit a domain's origin server information, including the basic information, protocol, and host in the console.
1. In the CSS console, select Domain Management on the left sidebar. Click the name of your **Playback Configuration** or click **Manage** on the right.

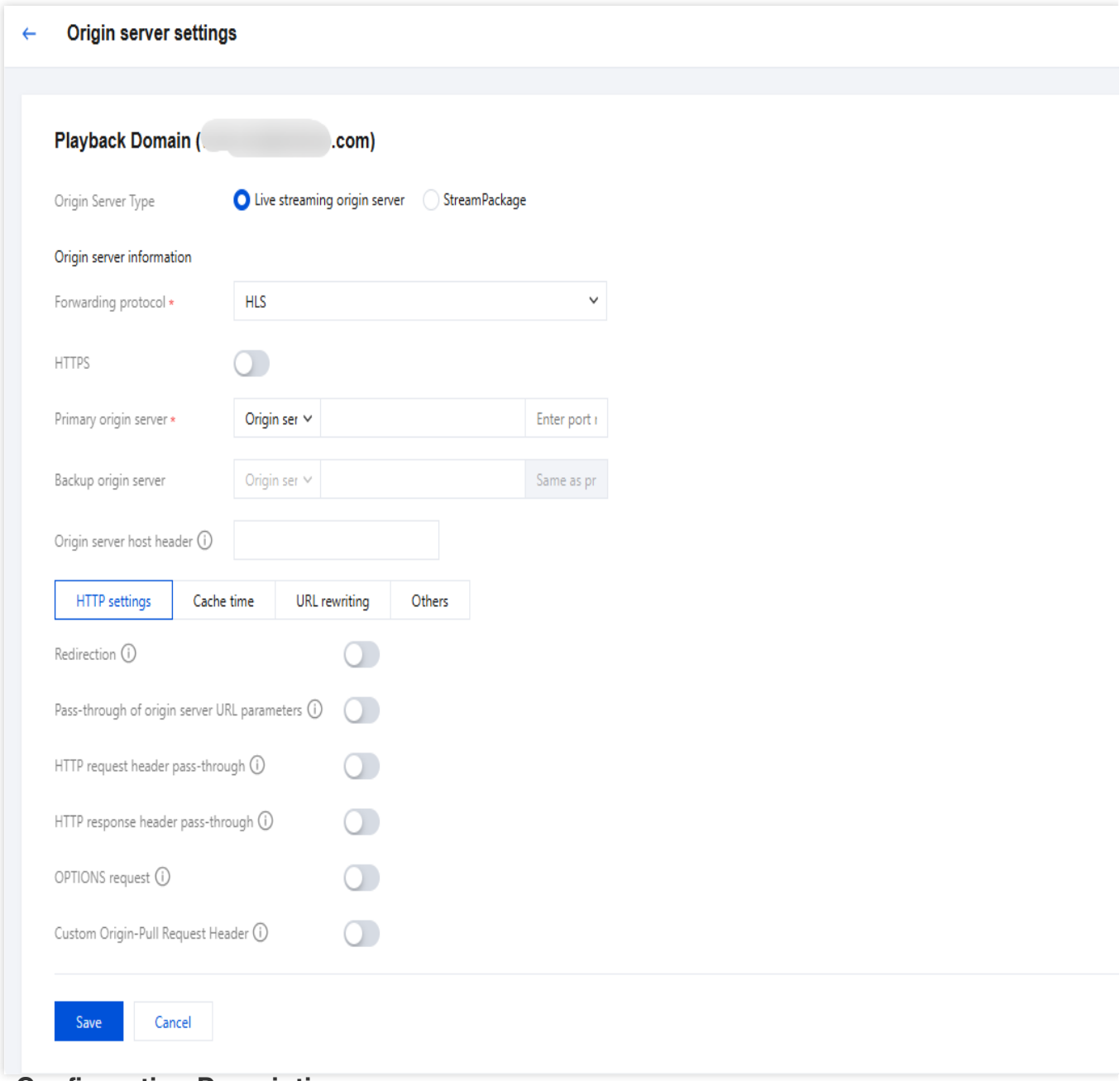


2. Beside **Domain Management/Domain**, click

to enable or disable **Origin server mode**.



3. When the origin server mode is enabled, you may perform the origin-pull configuration based on your business requirements.

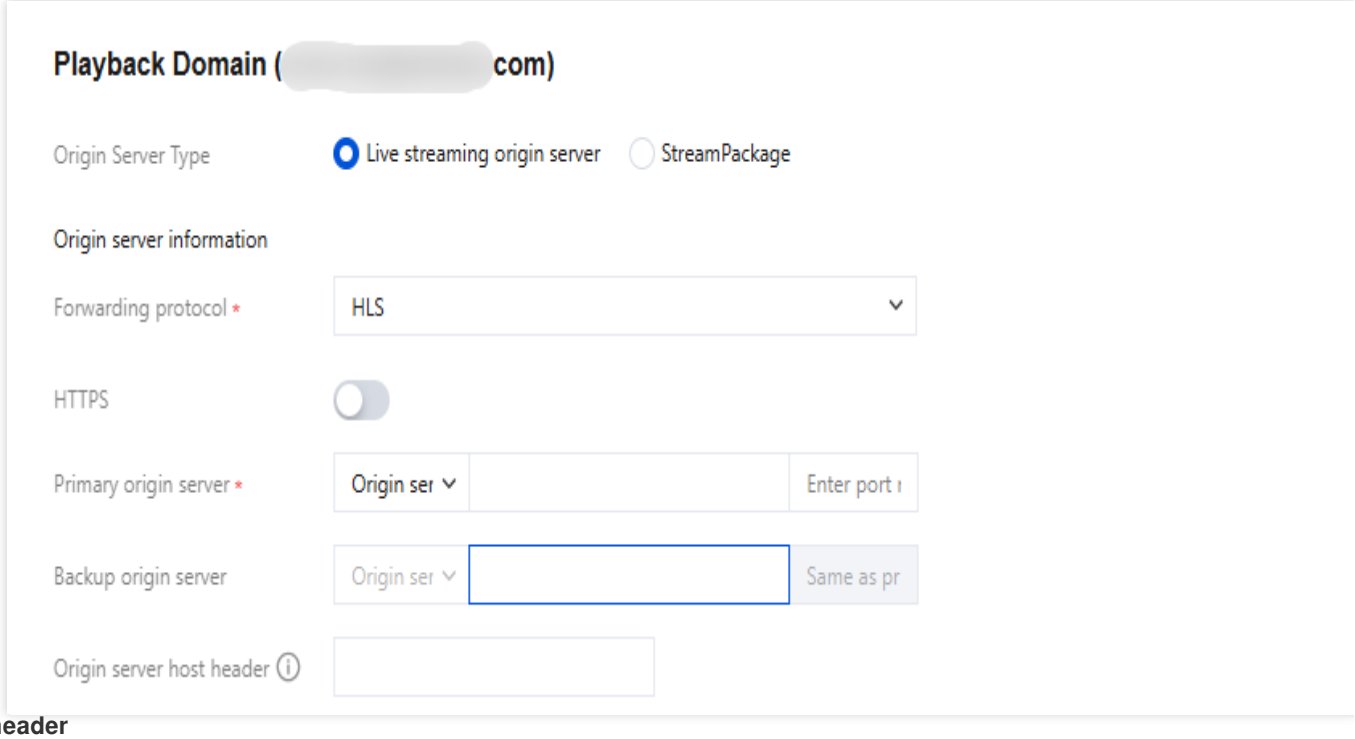


Basic Configuration Description

Origin server information

Origin Server Information	Description
Origin Server Type	Supports two types: Live Streaming Origin Server and StreamPackage.
Forwarding protocol	Supports RTMP, HTTP-FLV, and HLS protocols.
HTTPS	If the FLV or HLS protocol is used, you can enable HTTPS. If you enable HTTPS, port 443 will be used. Post-redirection HTTPS is also supported. There are no port restrictions.

Primary origin server	The address of the primary origin server, which can be an IP address or domain. You can also configure a backup origin server. The addresses will be polled.
Backup origin server	The address of the backup origin server (optional).
Origin server host header	By default, the origin server address is used as the Host header if it is not configured.



Host header

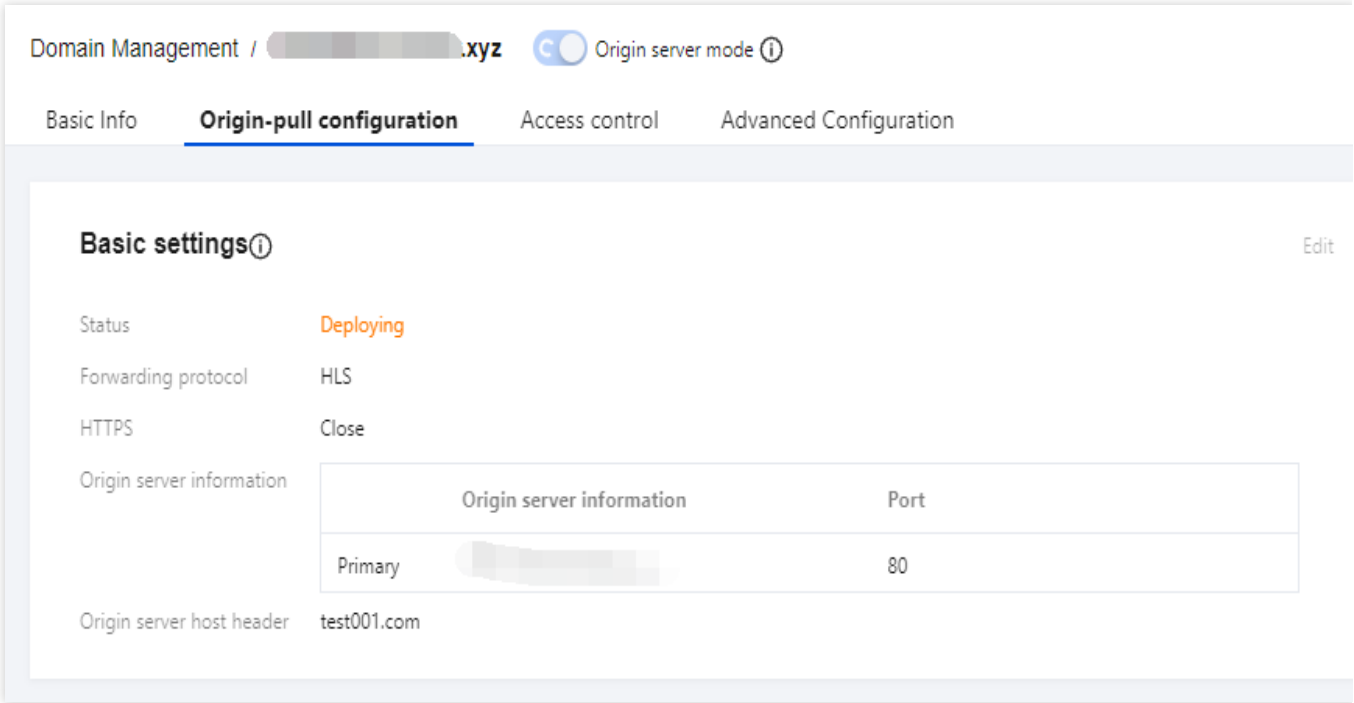
If the FLV or HLS protocol is used, you can configure an HTTP host header that specifies the exact domain that CSS accesses when pulling from the origin server. If not configured, the origin address is used as the Host header by default.

Notes

The difference between an origin server address and a host header is as follows:
An origin server address is the IP address an origin-pull request is sent to.
A host header specifies the domain of the origin server address a request is sent to.

Configuration example

1. An origin server is configured for the playback domain `xx001.elementtest.org` as follows:



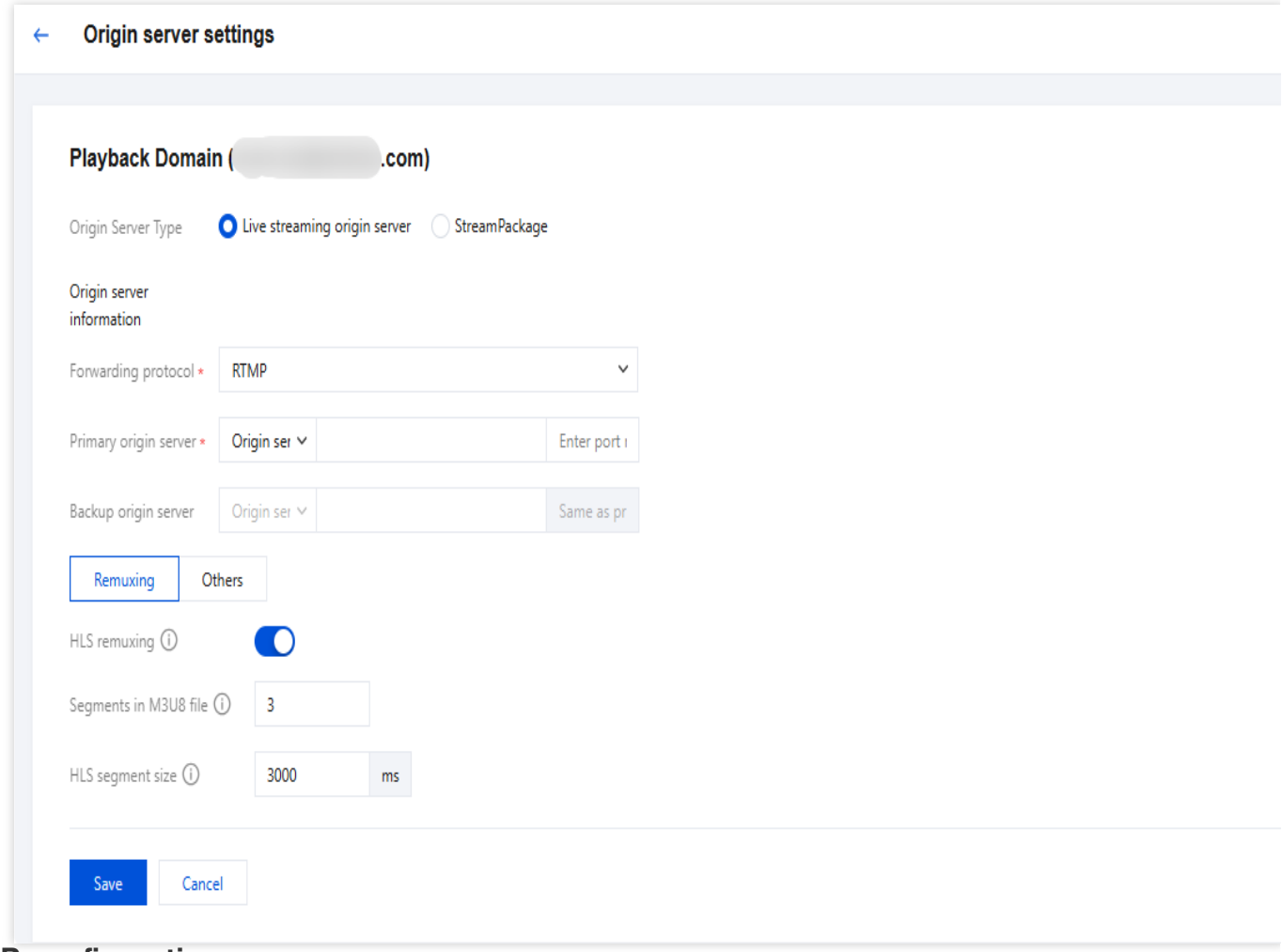
2. The process of pulling from the origin server would be as follows:
When the user accesses the resource by opening `http://xx001.elementtest.org/index.m3u8` , because the resource is not yet cached in Tencent Cloud, CSS will resolve the domain `test001.com` to get the server address of the origin server. Suppose it is `1.1.1.1` . CSS will access the `1.1.1.1` server, find the `index.m3u8` file in the web server `test002.com` , and then return the resource to the user.

Remuxing

If the RTMP or HTTP-FLV protocol is used, you can enable HLS remuxing. Below are the formats of an RTMP, HTTP-FLV, and HLS address.
RTMP: `rtmp://Playback domain/AppName/StreamName`
FLV: `http://Playback domain/AppName/StreamName.flv`
M3U8: `http://Playback domain/AppName/StreamName.m3u8`

Notes

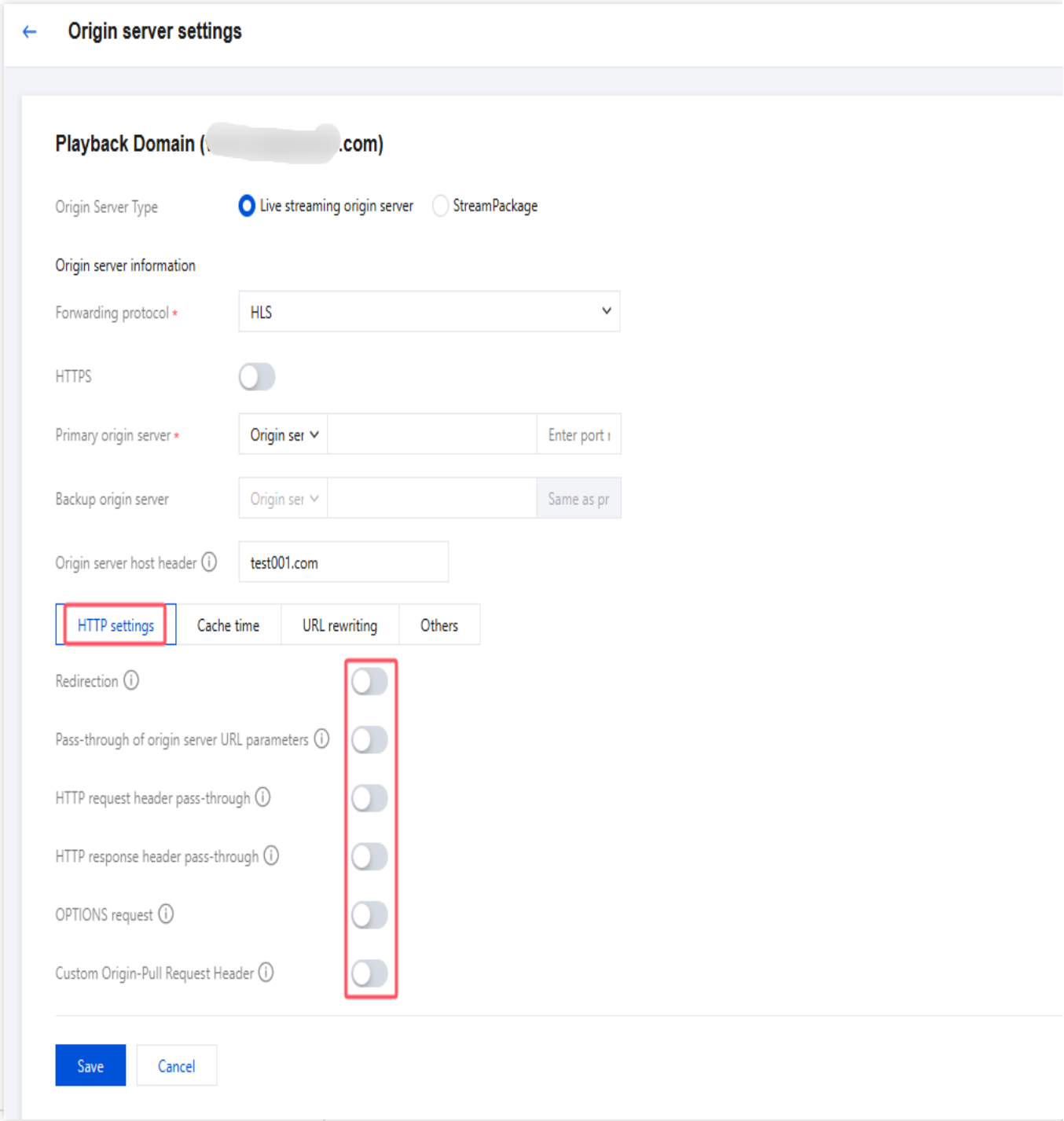
Number of HLS segments: Three by default. Value range: 3 - 10.
HLS segment size: Three seconds by default. Value range: 3 - 10. The actual segments generated will not be smaller than the GOP size.



HTTP configuration

When the origin-pull protocol is HLS, you may configure the **HTTP settings** . Based on your business requirements, click

to enable the corresponding features.



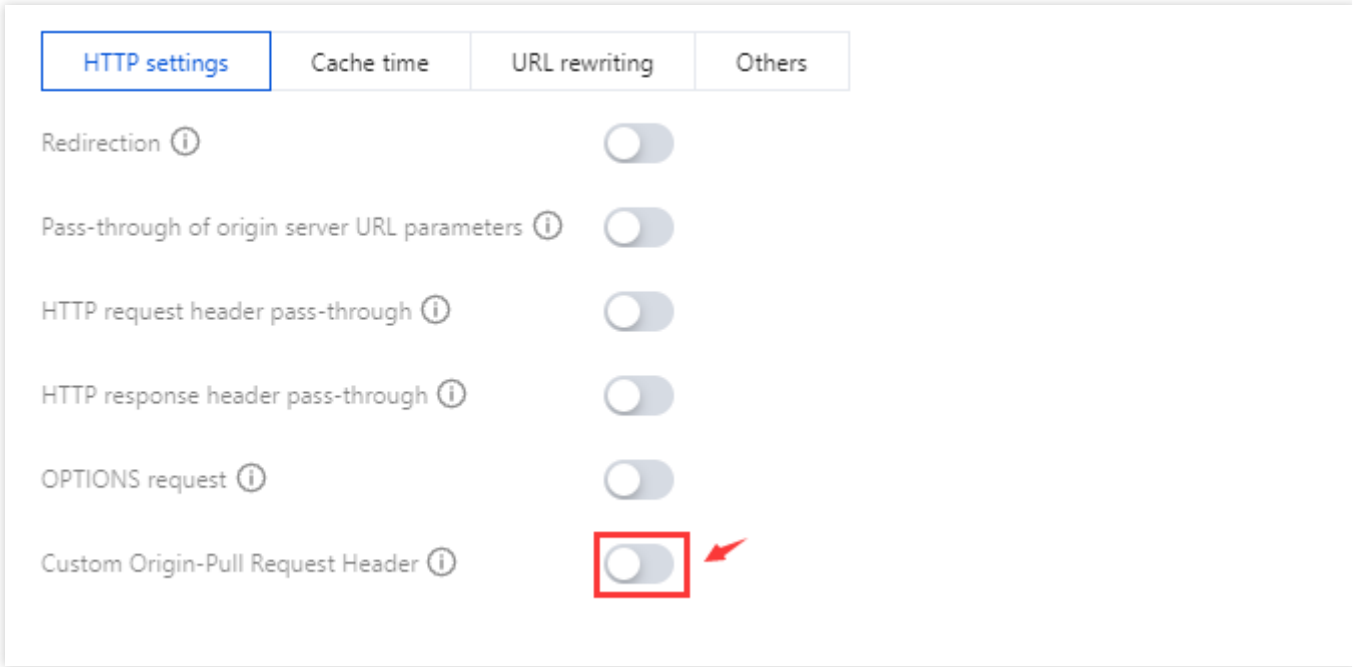
Item	Description
Redirection	If you enable this, Tencent Cloud will not cache the 301 or 302 status code. When 301 or 302 is returned by the origin server, Tencent Cloud will automatically redirect until it obtains the requested resource (max 10 redirects) and return the resource to the user. No redirects are needed on the user end. If you disable redirection, Tencent Cloud will return the 301 or 302 status code to the user end, which will redirect to get the resource.
Pass-through of origin server URL	By default, URL parameters are not passed through. If you enable this,

parameters	parameters may be added to the URL without performing URL encoding or decoding.
HTTP request header pass-through	By default, HTTP request headers are not passed through. You can enable this to pass through the headers. Duplicate headers (case-insensitive) are not supported currently.
HTTP response header pass-through	By default, HTTP response headers are not passed through. You can enable this to pass through the headers. Duplicate headers (case-sensitive) are supported currently.
OPTIONS request	By default, GET request is supported, and Option request is supported after enabling it.
Custom Origin-pull Request Header	When performing the origin-pull request, add the required headers to carry the client IP, port, label, etc. By default, the index request header is selected for the configuration item, with support for switching to the slice request header. Header parameter: It consists of uppercase and lowercase letters, numbers, and hyphens (-), with a length supported of 1-100 characters and no spaces allowed. Header value: Chinese characters are not supported, and it cannot start with $, with a length supported of 1-100 characters and no spaces allowed. By default, the system enables synchronization options, and automatically synchronizes index and slice request header configurations when a single addition is made. Adding multiple entries is supported, with a maximum of 10 custom origin-pull request headers for index and slice respectively.

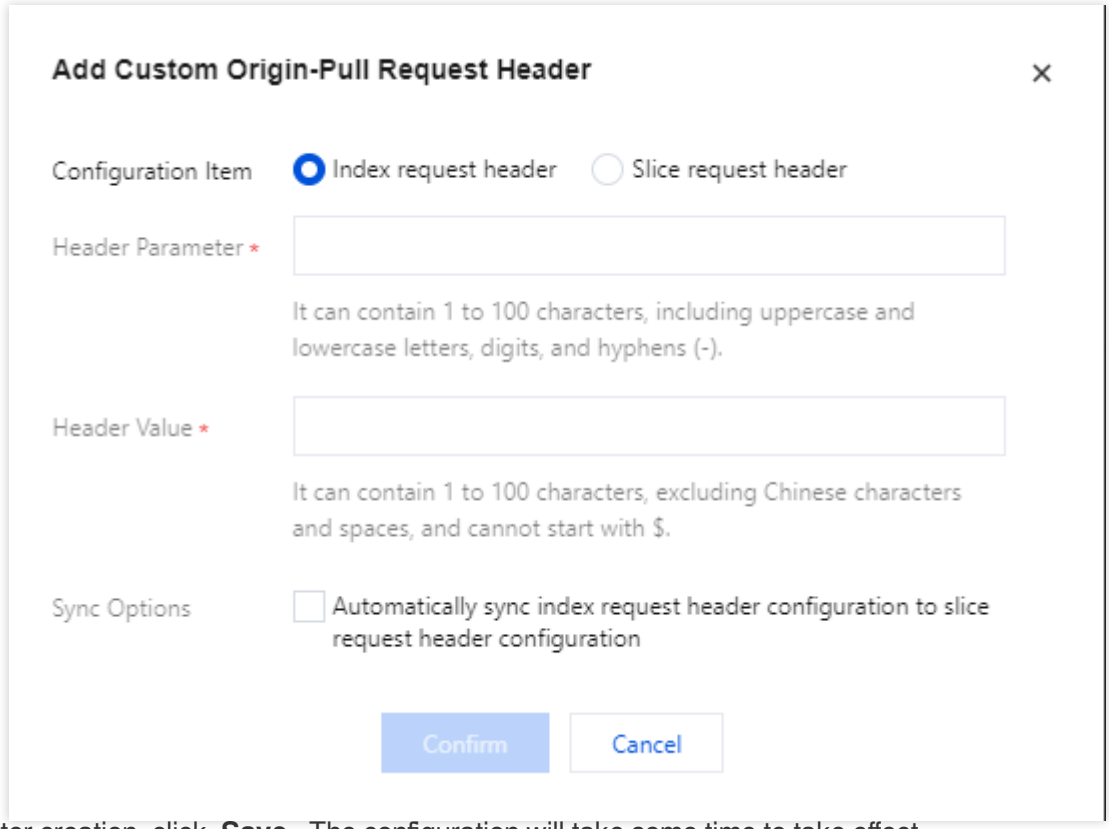
Custom Origin-pull Request Header Configuration

1. **Add the Custom Origin-pull Request Header**

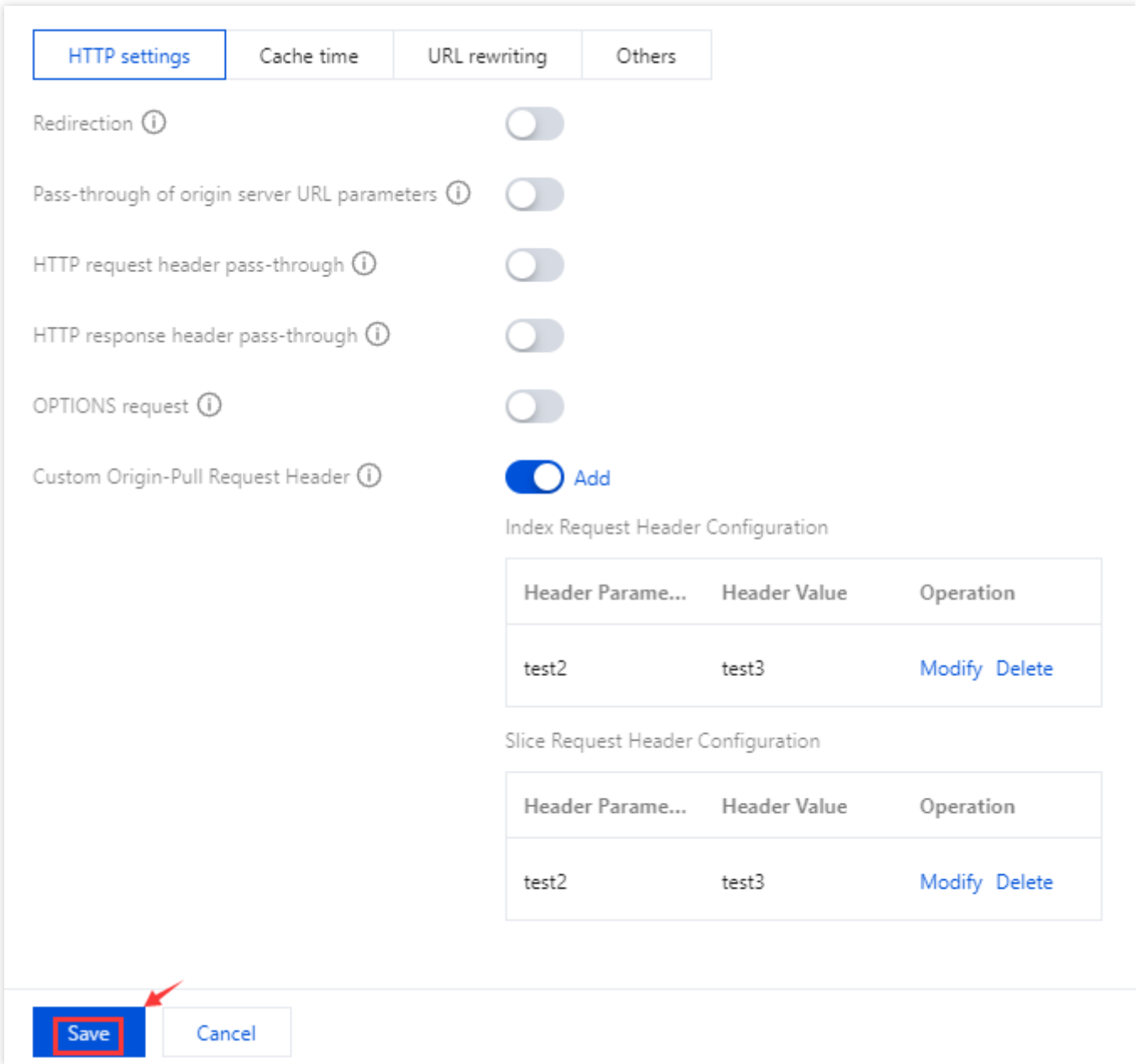
1.1 Click  to turn on the Custom Origin-pull Request Header switch and add the custom origin-pull request header configuration.



1.2 After completing the configuration, click **Confirm** to finish the creation.



1.3 After creation, click **Save** . The configuration will take some time to take effect.

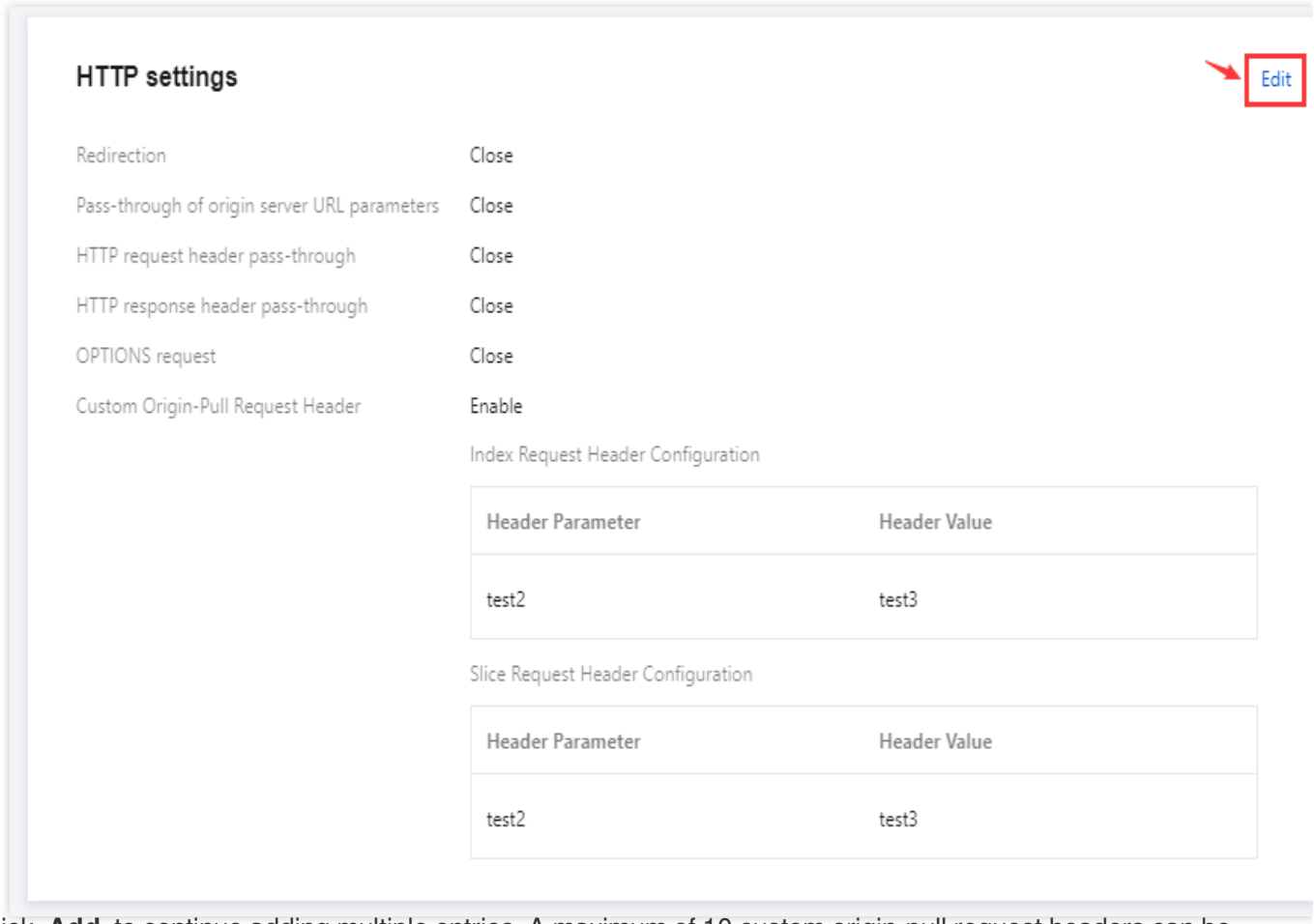


2. **Modify the Custom Origin-pull Request Header**

Note:

After deleting the custom origin-pull request header, the configuration will no longer be effective. Operate with care.

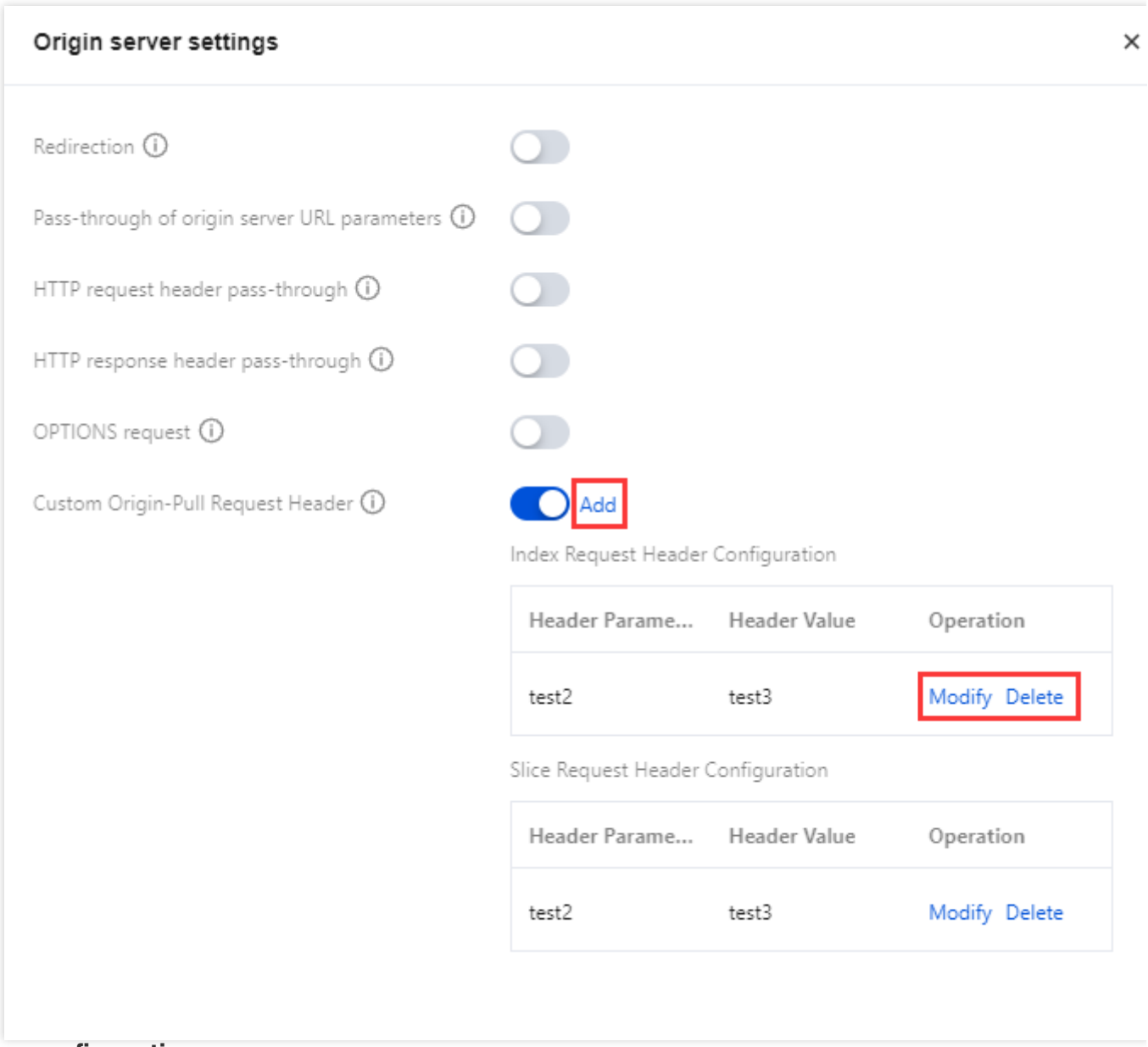
2.1 Based on your business requirements, you can click **Edit** to modify, add, or delete the configured custom origin-pull request header.



2.2 Click **Add** to continue adding multiple entries. A maximum of 10 custom origin-pull request headers can be configured.

2.3 Click **Modify** to modify the configured custom origin-pull request header.

2.4 Click **Delete** to delete the configured custom origin-pull request header. Once all custom origin-pull request header configurations are deleted, click **Save** . The system will automatically disable the custom origin-pull request header configuration feature.

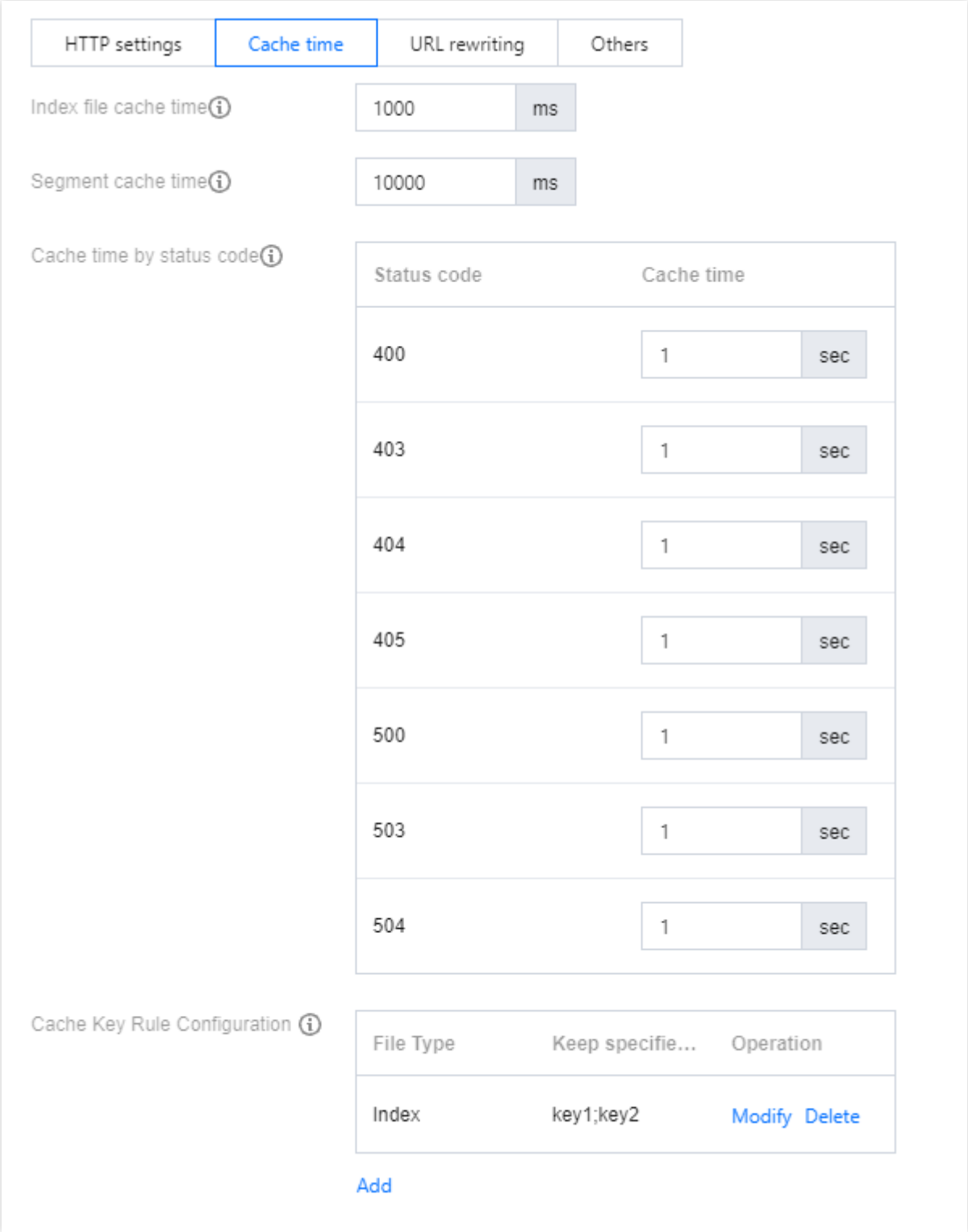


Cache configuration

If the HLS protocol is used, you can configure the resource cache time. After Tencent Cloud obtains the requested resource successfully from the origin server (status code 200), it will cache the index file and segments as configured.

Item	Description
Index file cache time	The time to cache the index file when the origin server returns the 200 status code. The default cache time is 1,000 ms. The maximum time that can be set is 60,000 ms.
Segment cache time	The time to cache the TS/M4S/MP4 segments when the origin server returns the 200 status code. The default cache time is 1,000 ms. The maximum time that can be set is 60,000 ms.
Cache time by status code	According to the status code corresponding to the configured cache, if the same request is received within the cache time, there is no need to visit the origin

	server, and the status code can be returned directly. The default cache time is 1s. When the origin server returns a non-200 status code, if it is unable to handle it immediately, and you don't want to pass through all subsequent requests to the origin server, you can cache the status code and return it directly to the user. This can reduce the load on the origin server. Currently, the following status codes can be cached, regardless of the file type: 4XX: 400, 403, 404, 405 5XX: 500, 503, 504
Cache key rule configuration	For the cache key rule configuration, retain the parameters that have an impact on the resource content as the cache key, convert a category of requests for the same resource into a unified cache key and hit the same cache to improve the hit rate. **File Type** Choose file types. There are options of index or shard, Index is selected by default. **Retain specified parameters** Only English, characters and numbers can be entered. Multiple parameters are separated by ";". Up to 30 groups of parameters are supported. Each parameter name should not exceed 20 characters. If a parameter is specified, even if the parameter does not have a value, it will be cached separately from the parameters with the same name that have value. **Note:** You must enable the origin-pull URL parameter passthrough in HTTP settings before configuring the cache key rules.



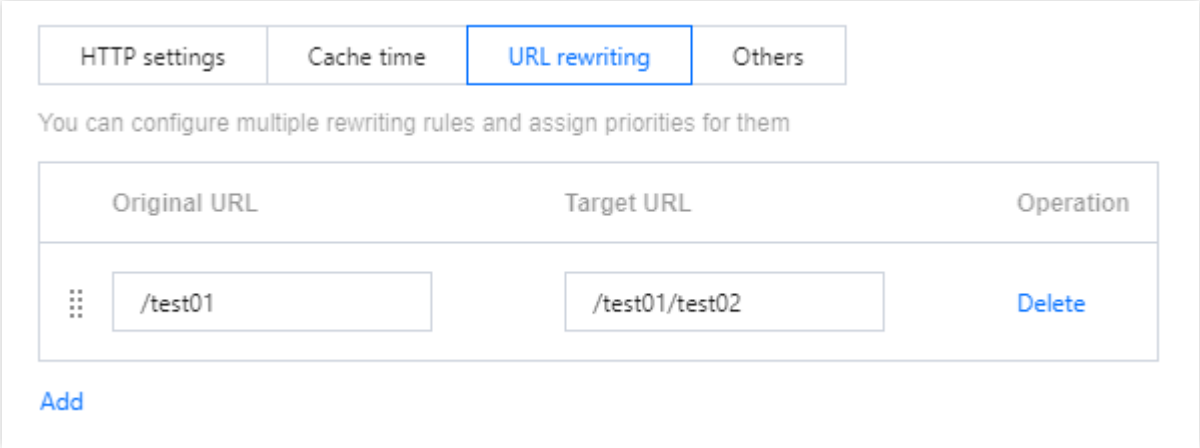
URL rewriting

If the HLS protocol is used, you can configure URL rewriting.

Tencent Cloud allows you to rewrite the actual URL CSS pulls from to a URL that better matches your origin server. Currently, you can only rewrite the URL path.

Notes

Original URL: Requests are matched by prefix. For example, if you enter `/test01`, the rewriting rule will be applied to all requests under `/test01`. Regular expressions are not supported currently.
Target URL: Requests are matched by prefix. For example, if you enter `/test01/test02`, all requests under `/test` will be rewritten to `/test01/test02`. Regular expressions are not supported currently.

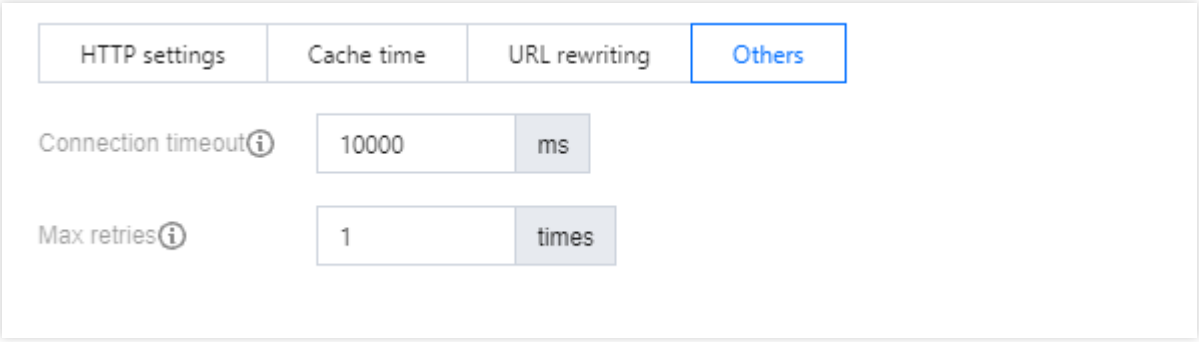


Limits

You can configure at most 10 rewriting rules for each playback domain.
Spaces and the following special characters are not supported: < > " # { } | \\ ^ ~ [ ] `
You can re-arrange the rules to adjust their priorities. Rules at the top have higher priorities.

Others

Item	Description
Connection timeout	The timeout period for establishing a TCP connection. The default time is 10,000 ms, and the value range is 2000-60000 (ms). Please set the timeout period according to your origin server conditions and network conditions. If the timeout period is too short, when a pull request fails due to network issues, CSS may switch origin servers too frequently. If the timeout period is too long, CSS may wait a long time before it tries a different origin server, causing playback failure at the client end.
Max retries	The maximum number of retry attempts. If multiple origin server addresses have been configured, when a request fails, CSS will try a different address. Value range: 1 - 10.


HTTP settings
Cache time
URL rewriting
Others
Connection timeout
10000
ms
Max retries
1
times

Bandwidth Cap Configuration

Last updated：2024-05-28 10:25:05

CSS allows you to set a bandwidth cap for your playback domain. In the acceleration region of your domain, if the peak downstream bandwidth in a reference period hits the cap you set, a 403 error will be returned to playback requests. This feature is disabled by default.

Note:

If the bandwidth cap configuration is enabled, the scanning granularity is 5 minutes. If there is a sudden increase in usage within a short period of time, the previous scan may not have triggered the threshold, and the next scan may directly exceed the threshold. In this scenario, there will be a certain delay (approximately 5 minutes) in the access interception operation, and the consumption during this period will be billed normally.

Prerequisites

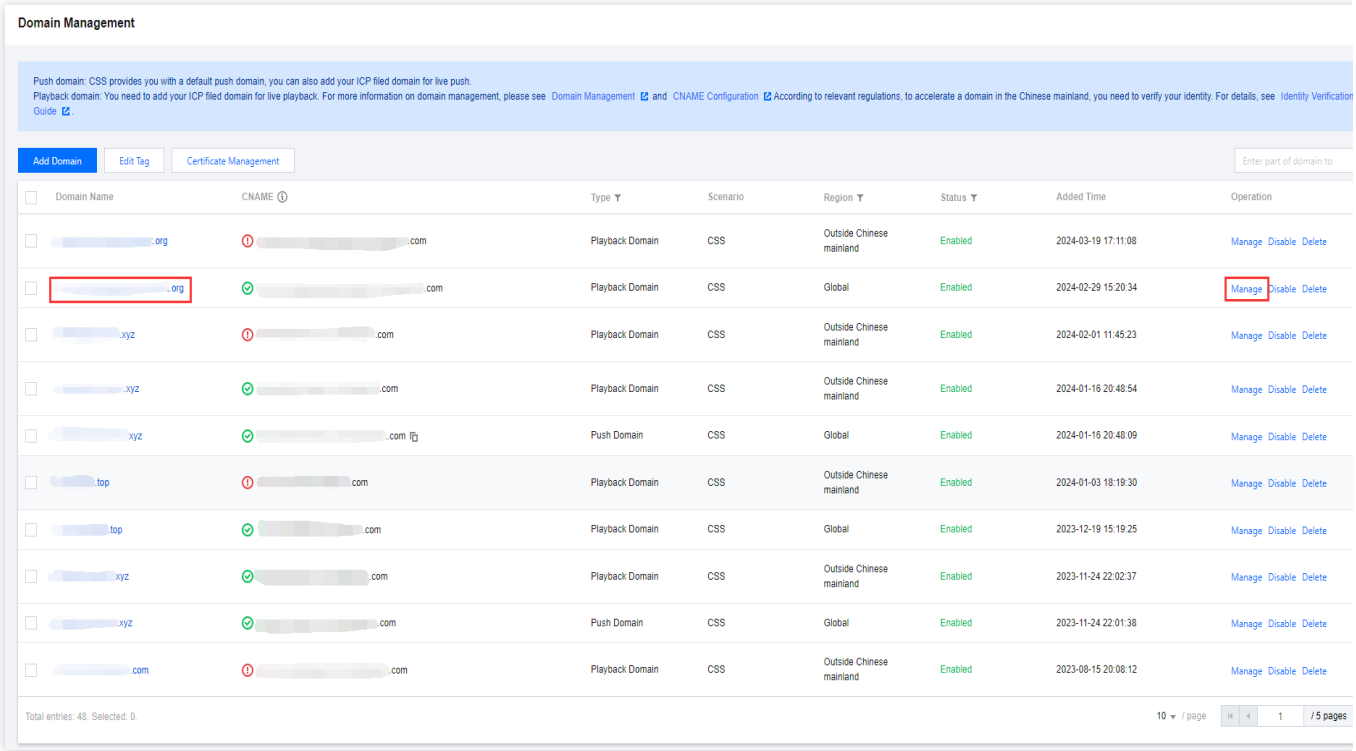
You have logged in to the CSS console.
You have added a playback domain name.

Limits

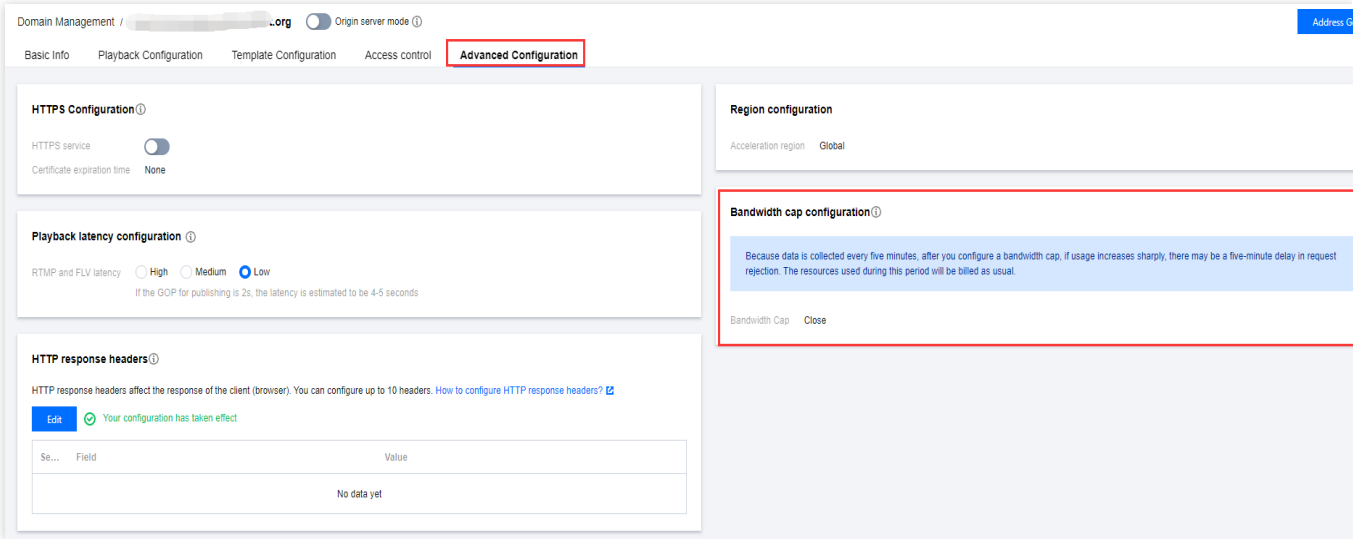
Acceleration Region	Default Bandwidth Capping Region	Remarks
Chinese mainland	Chinese mainland	You can only set a cap for the Chinese mainland.
Outside the Chinese mainland	Outside the Chinese mainland	You can only set a cap for outside the Chinese mainland.
Global acceleration	Global acceleration	You can set different caps for inside and outside the Chinese mainland. You can also set a global cap.

Configuring Bandwidth Cap

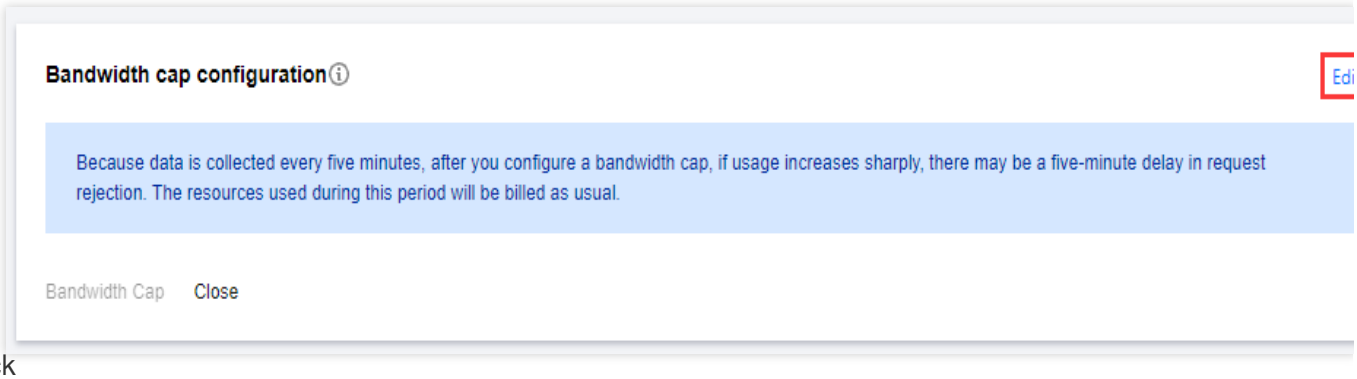
1. Go to Domain Management. Click the name of your playback domain or **Manage** on the right.



2. Select **Advanced Configuration** > **Bandwidth cap configuration** to view the **Bandwidth cap configuration** tab.



3. Click **Edit** in the upper-right corner of the tab to enter the bandwidth cap configuration page.

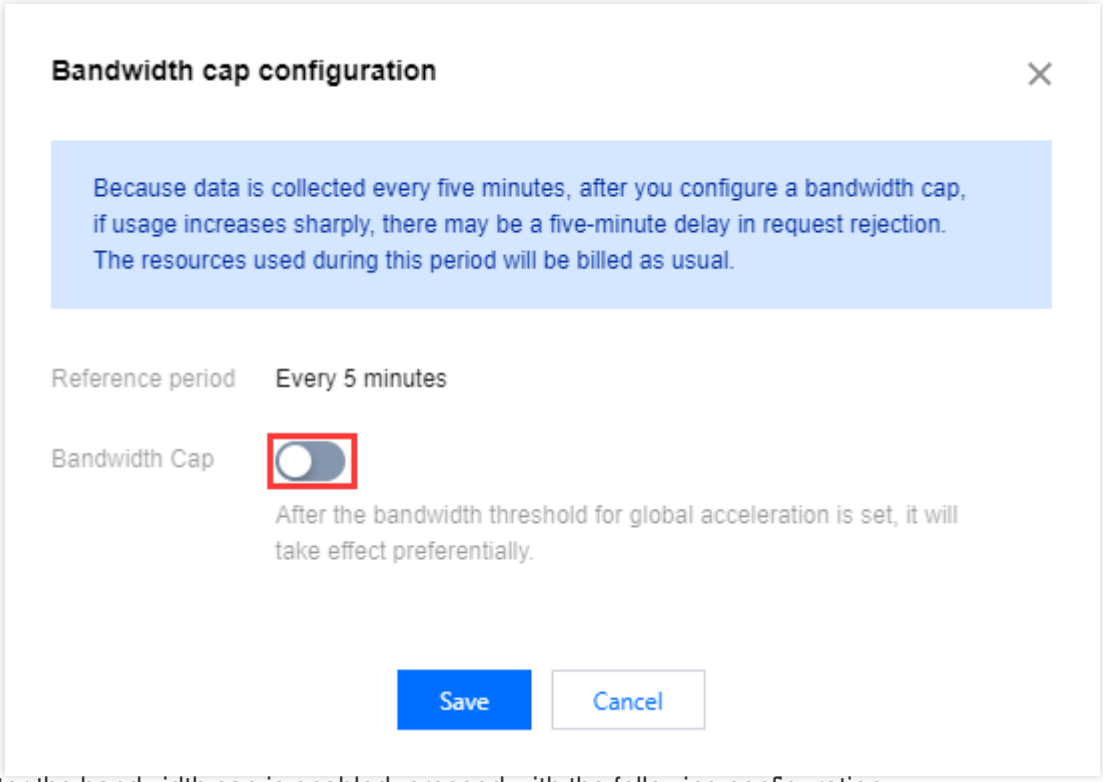


4. Click

to enable **Bandwidth Cap** .

Note:

After the bandwidth threshold for global acceleration is configured, it will take effect preferentially.

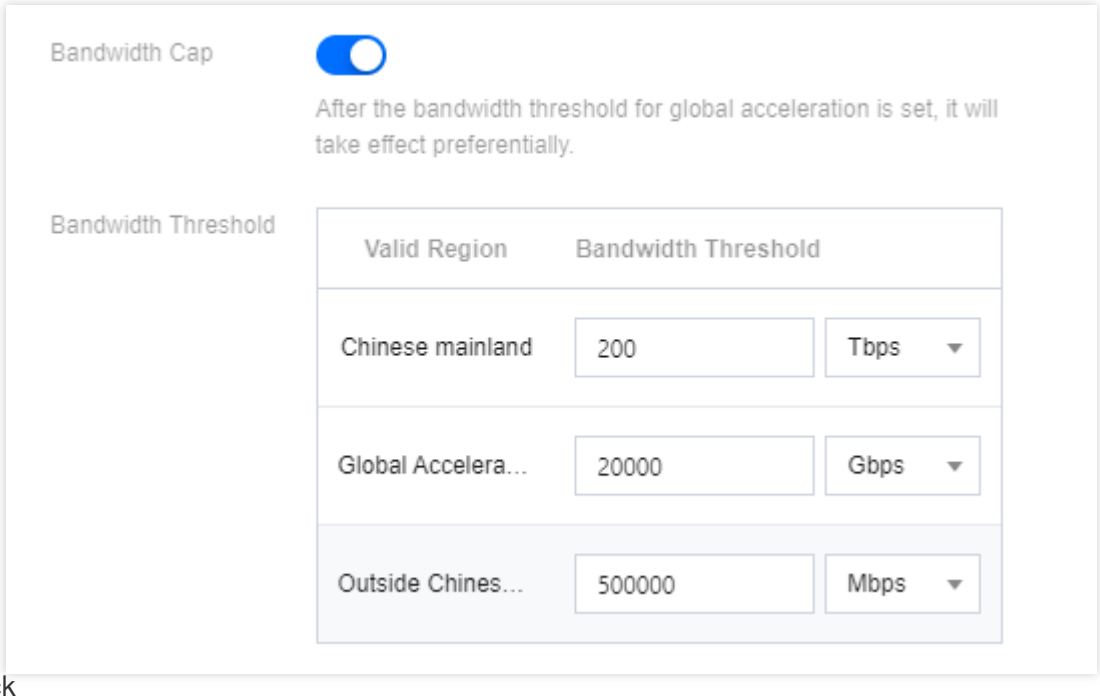


4.1 After the bandwidth cap is enabled, proceed with the following configuration:

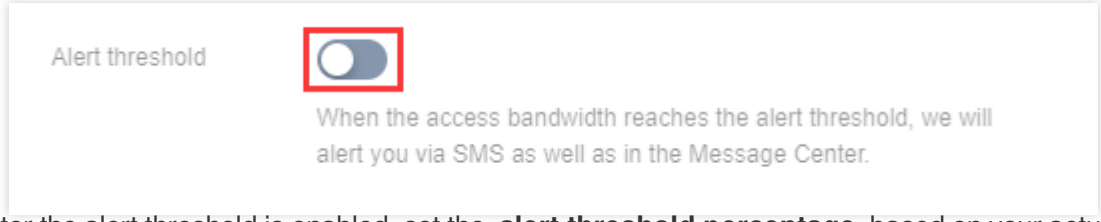
Bandwidth Threshold

Valid Region is determined based on the acceleration region type of the playback domain name. For related configuration rules, refer to Limits.

Fill in the bandwidth threshold based on your actual business needs. Choose the threshold unit as Mbps, Gbps, or Tbps.

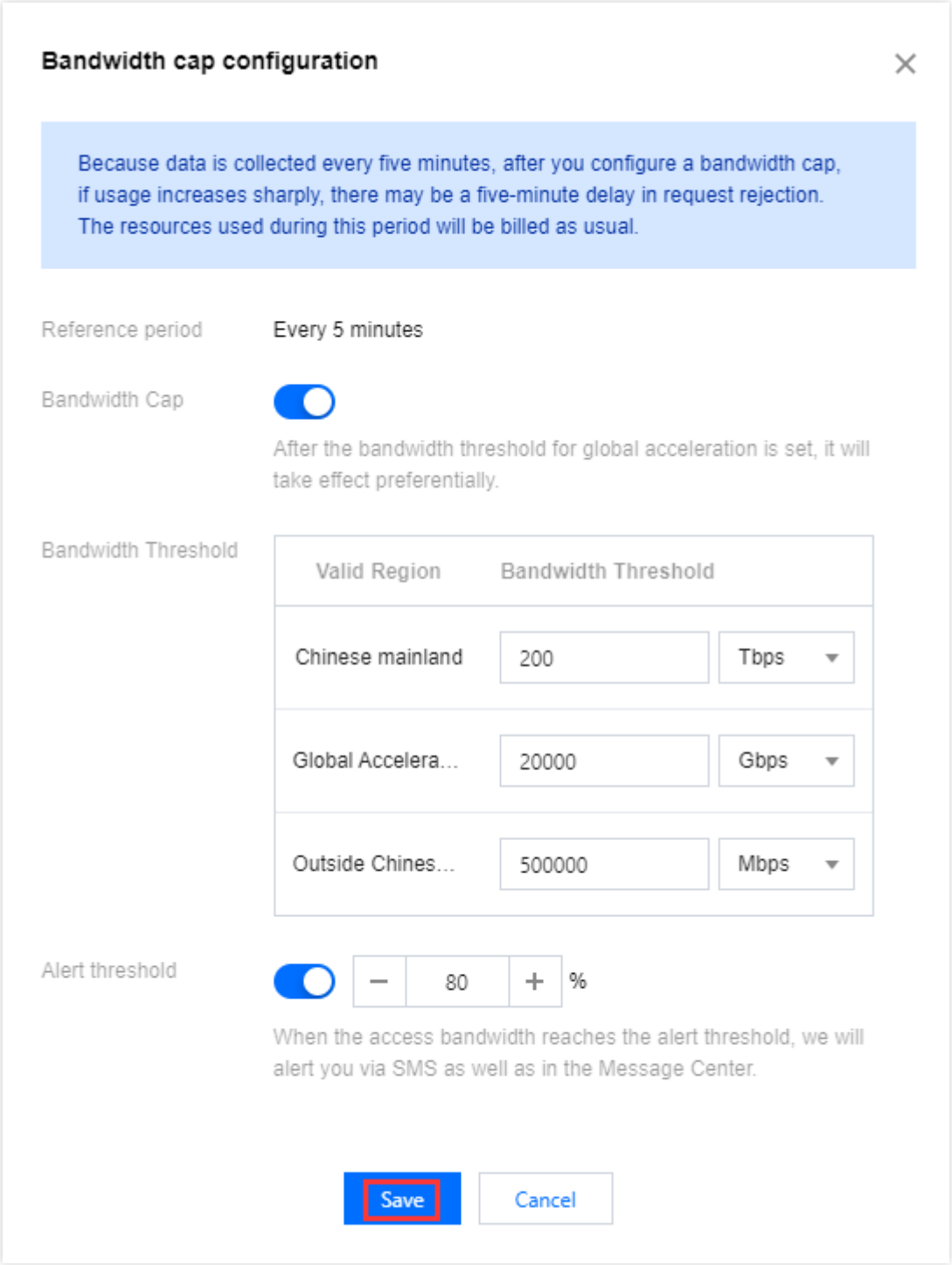


5. Click  to enable **Alert threshold** .



5.1 After the alert threshold is enabled, set the **alert threshold percentage** based on your actual business needs. When the access bandwidth/bandwidth threshold reaches the alert threshold, the system will alert you through the Message Center and other methods.

6. Click **Save**.



Note:

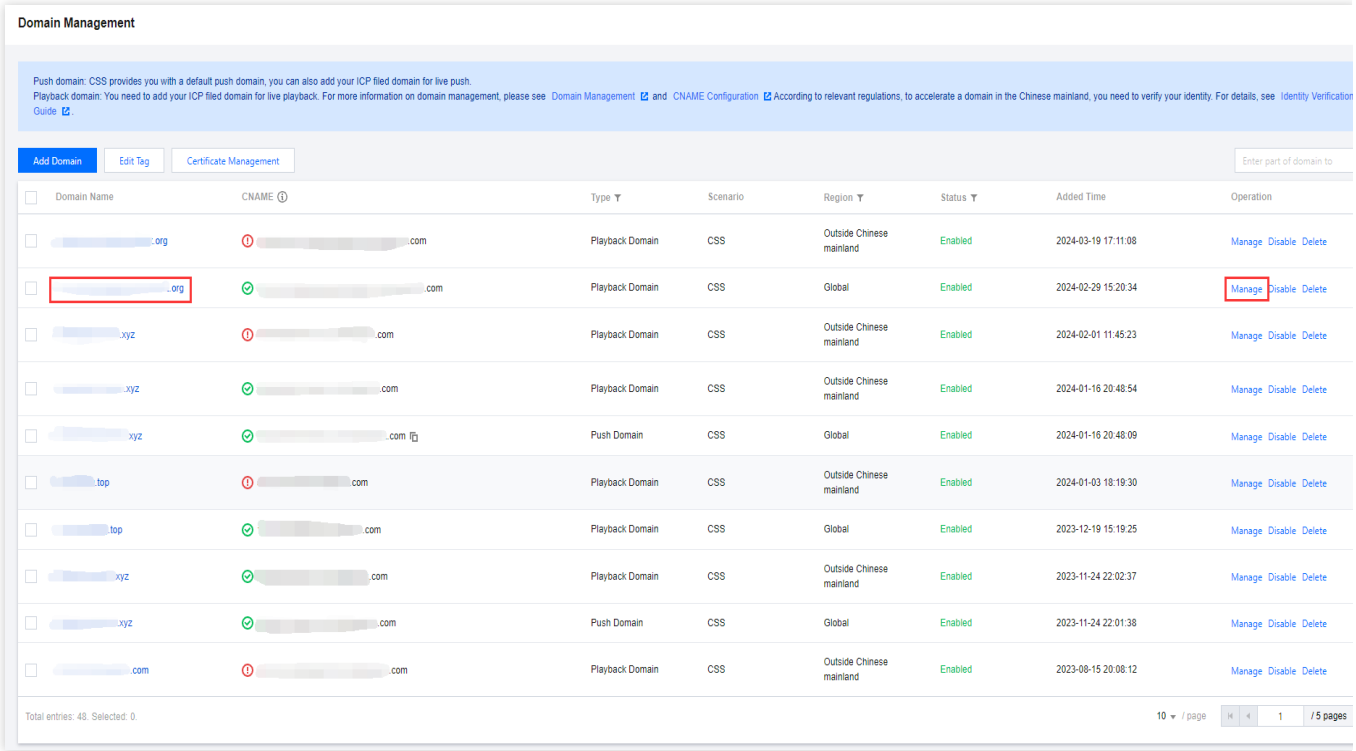
The conversion factor between the bandwidth units is 1,000: 1 Tbps = 1,000 Gbps; 1 Gbps = 1,000 Mbps.

If you change the acceleration region for your domain, you need to configure the bandwidth cap again.

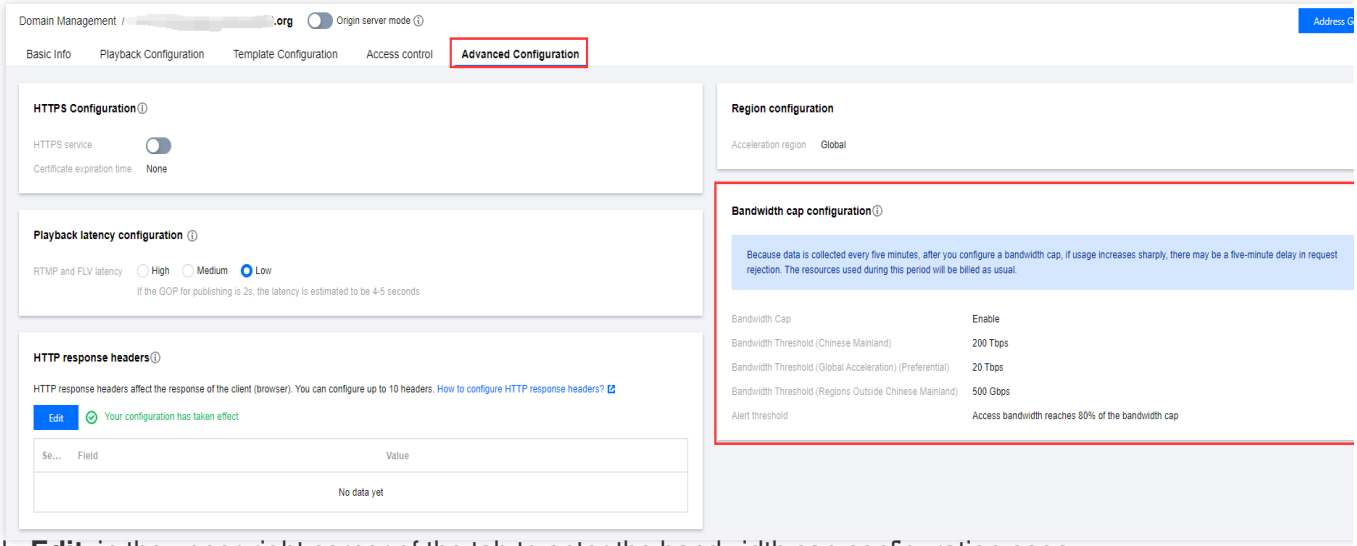
The default alert threshold is 80% of the bandwidth cap. Value range: 0-100.

Disabling Bandwidth Cap

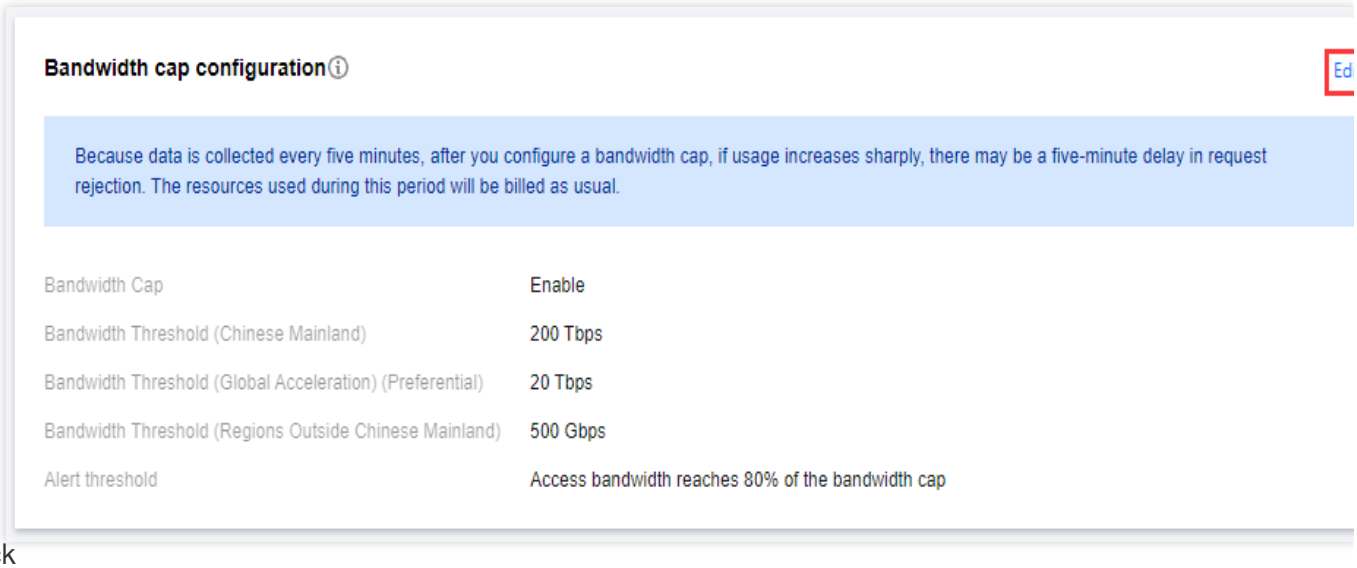
1. Go to Domain Management. Click the name of your playback domain or **Manage** on the right.



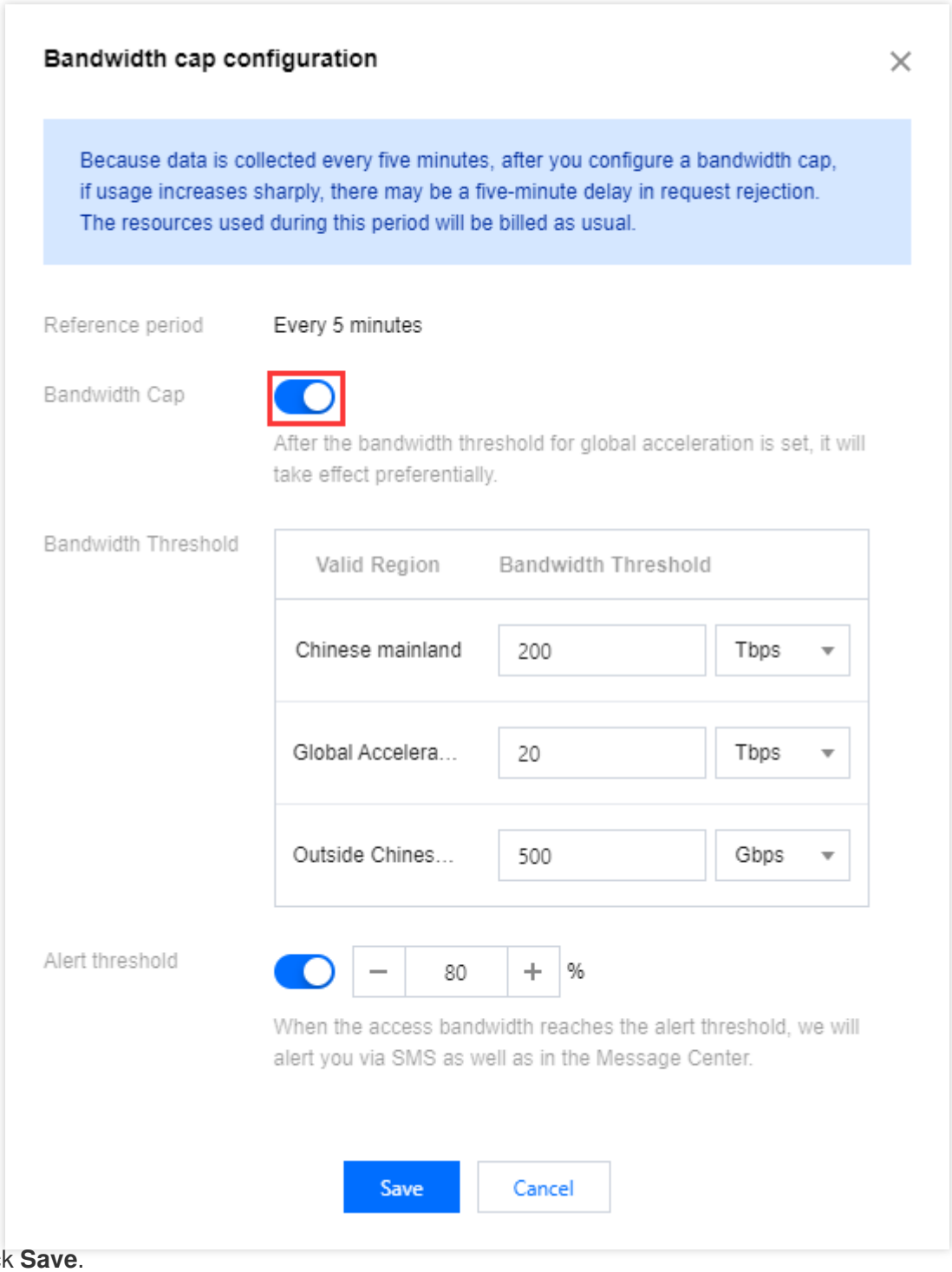
2. Select the **Advanced Configuration** tab to view the **Bandwidth cap configuration** tab.



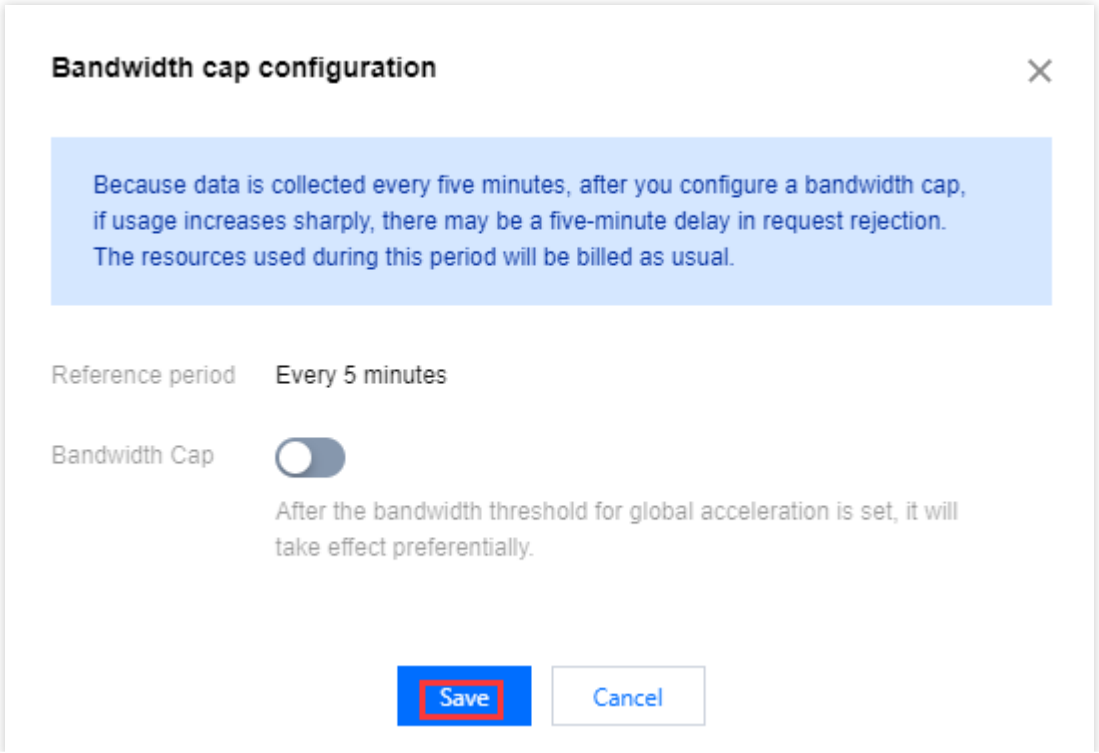
3. Click **Edit** in the upper-right corner of the tab to enter the bandwidth cap configuration page.



4. Click  to disable **Bandwidth Cap** .


Bandwidth cap configuration
Because data is collected every five minutes, after you configure a bandwidth cap, if usage increases sharply, there may be a five-minute delay in request rejection. The resources used during this period will be billed as usual.
Reference period
Every 5 minutes
Bandwidth Cap
After the bandwidth threshold for global acceleration is set, it will take effect preferentially.
Bandwidth Threshold
Valid Region
Bandwidth Threshold
Chinese mainland
200
Tbps
Global Accelera...
20
Tbps
Outside Chines...
500
Gbps
Alert threshold
80
%
When the access bandwidth reaches the alert threshold, we will alert you via SMS as well as in the Message Center.
Save
Cancel

5. Click **Save**.


Bandwidth cap configuration
Because data is collected every five minutes, after you configure a bandwidth cap, if usage increases sharply, there may be a five-minute delay in request rejection. The resources used during this period will be billed as usual.
Reference period
Every 5 minutes
Bandwidth Cap
After the bandwidth threshold for global acceleration is set, it will take effect preferentially.
Save
Cancel

IP Blocklist/Allowlist Configuration

Last updated：2024-06-05 15:41:31

This document shows you how to configure an IP allowlist/blocklist to filter requests and control access to streaming content.

How It Works

IP **allowlist**: Only IP addresses on the list can access your streaming content.
IP **blocklist**: IP addresses on the list cannot access your streaming content.

Must-Knows

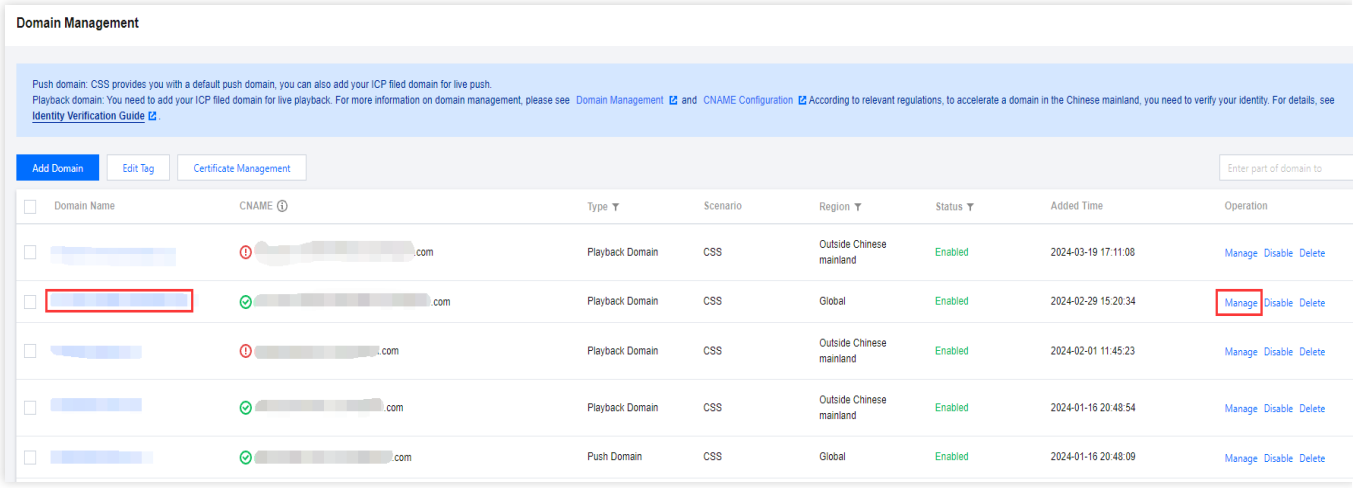
An IP allowlist/blocklist takes effect about ten minutes after configuration.

Prerequisites

You have activated CSS and logged in to the CSS console.
When both IP Blocklist/Allowlist and Playback Region Management (Regional Block/Allowlist) are enabled at the same time, the system's judgment logic is as follows:
1.1 **First, check the IP Blocklist/Allowlist**:
If the IP is in the allowlist, it is directly allowed.
If the IP is in the blocklist, access is directly denied.
If the IP is not in the blocklist/allowlist, go to the next step.
1.2 **Then, check the Regional Block/Allowlist** (only when the IP is not in the IP Block/Allowlist):
If the region is in the allowlist, then allow access; otherwise, deny access.
If the region is in the blocklist, then deny access; otherwise, allow access.

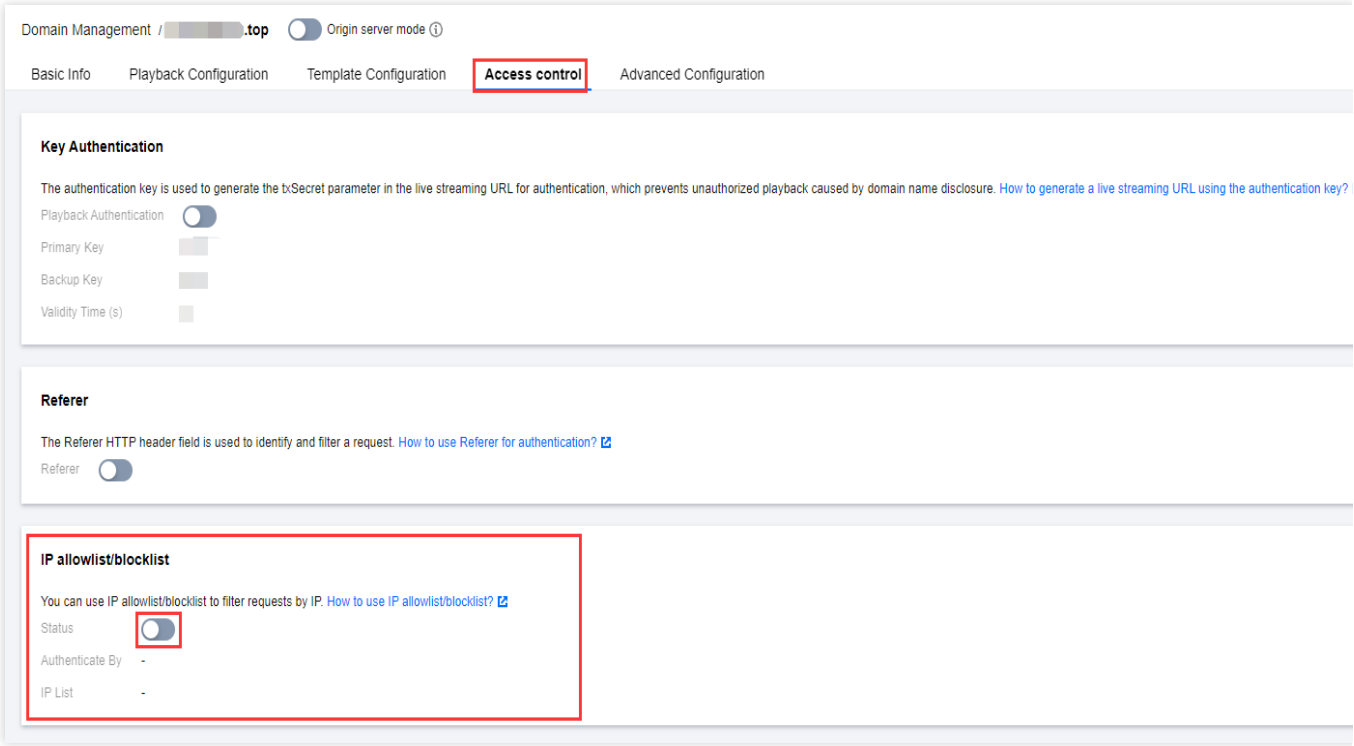
Configuring an IP Allowlist/Blocklist

1. Select Domain Management on the left sidebar, and click the target **playback domain** or click **Manage** on the right to enter the domain management page.



2. Within the **Access Control**> **IP allowlist/blocklist**, click on

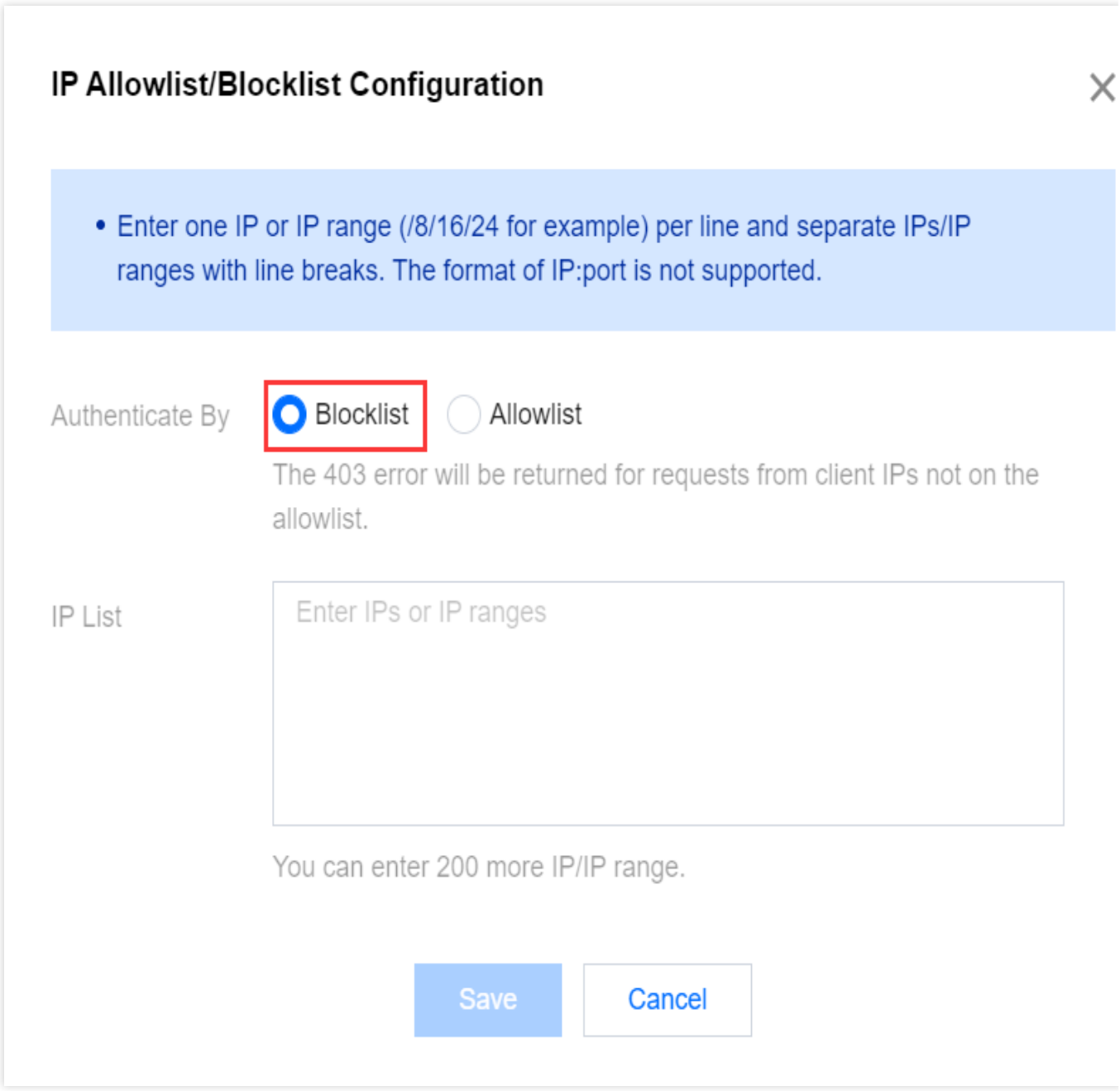
to enable the IP Allowlist/Blocklist.

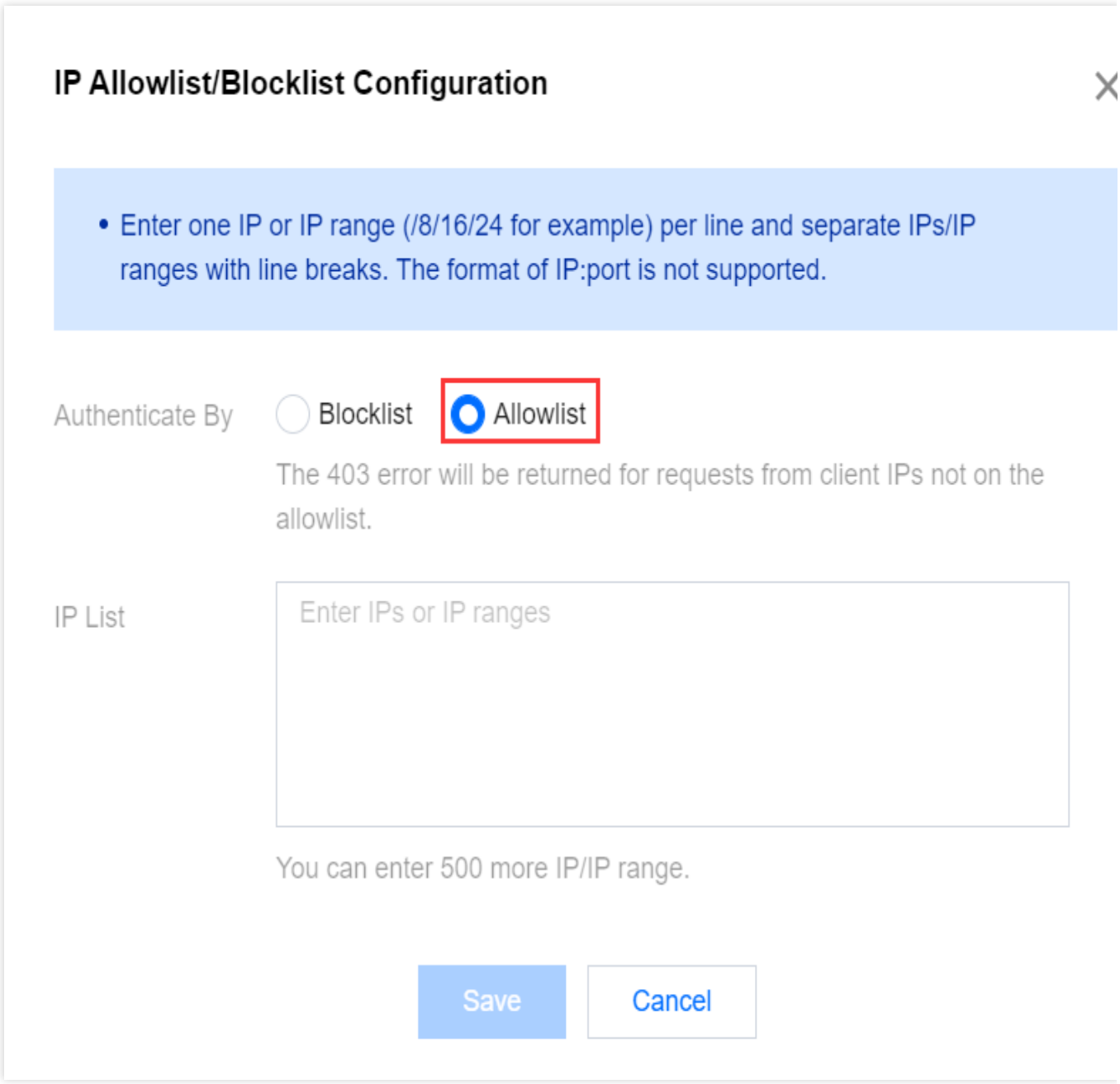


3. After enabling the **IP Allowlist/Blocklist** , enter the **IP Allowlist/Blocklist** configuration page and perform the following configuration:

Blocklist

Allowlist

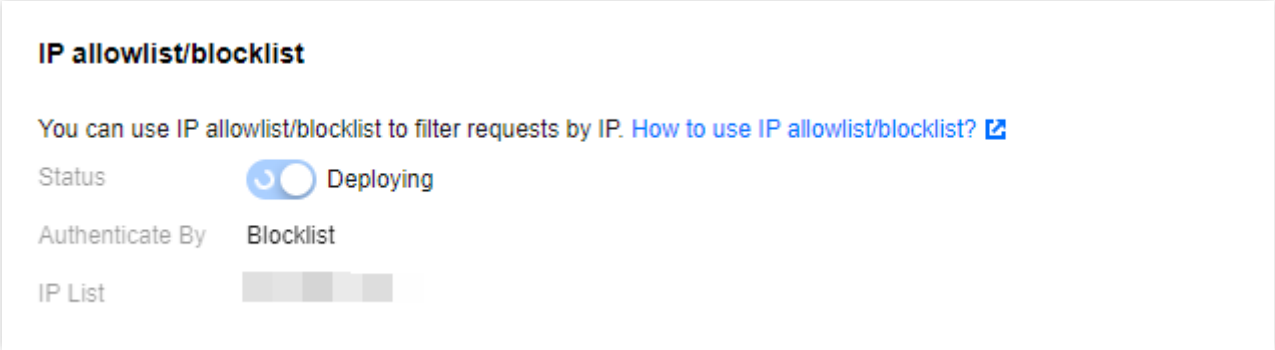

IP Allowlist/Blocklist Configuration
• Enter one IP or IP range (/8/16/24 for example) per line and separate IPs/IP ranges with line breaks. The format of IP:port is not supported.
Authenticate By
Blocklist
Allowlist
The 403 error will be returned for requests from client IPs not on the allowlist.
IP List
Enter IPs or IP ranges
You can enter 200 more IP/IP range.
Save
Cancel



Configuration Item	Description
Authenticate By	Allowlist or blocklist: You cannot select both. If you configure an allowlist, only IP addresses on the list will be able to access your streaming content. If you configure a blocklist, IP addresses on the list cannot access your streaming content.
IP List	The IP blocklist supports a maximum configuration of 200 rules, and the IP allowlist supports up to 500 rules. Please separate entries with a newline character.

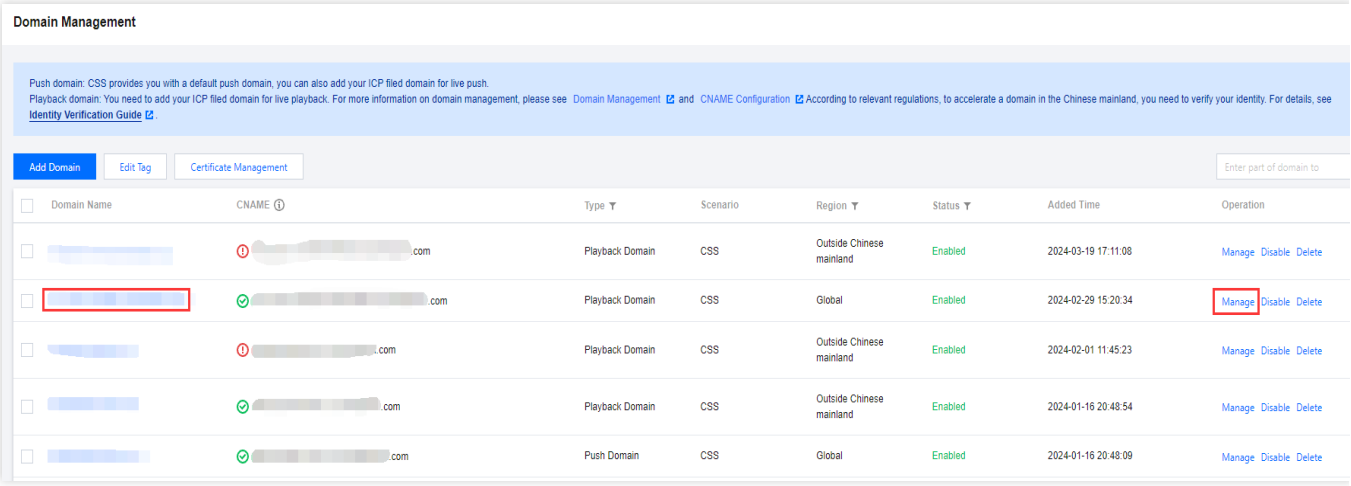
	You can enter IP addresses or IP ranges (/8/16/24). The “IP address: port number” format is not supported. IPv6 is not supported currently.

4. Click **Save** to save the configuration (it takes a while for the configuration to take effect).

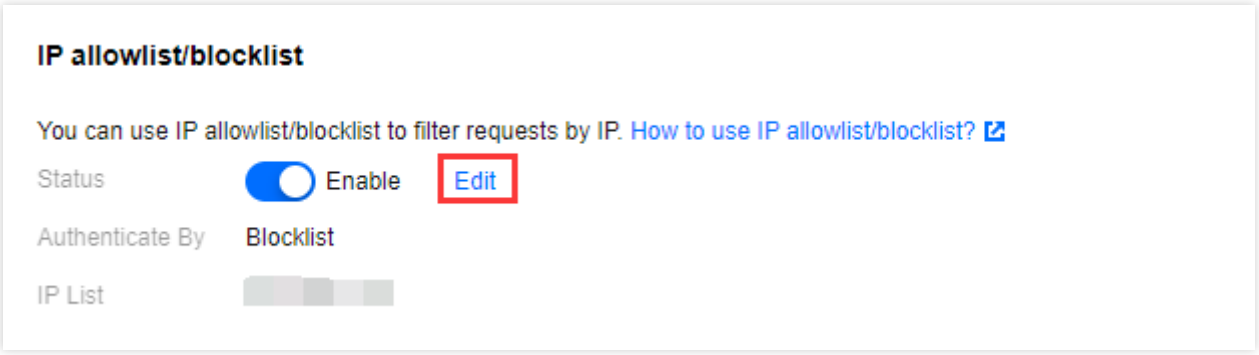


Modifying an IP Allowlist/Blocklist

1. Select Domain Management on the left sidebar, and click the target **playback domain** or click **Manage** on the right to enter the domain management page.



2. Click **Access Control** and, in the **IP Allowlist/Blocklist** area, click **Edit**.

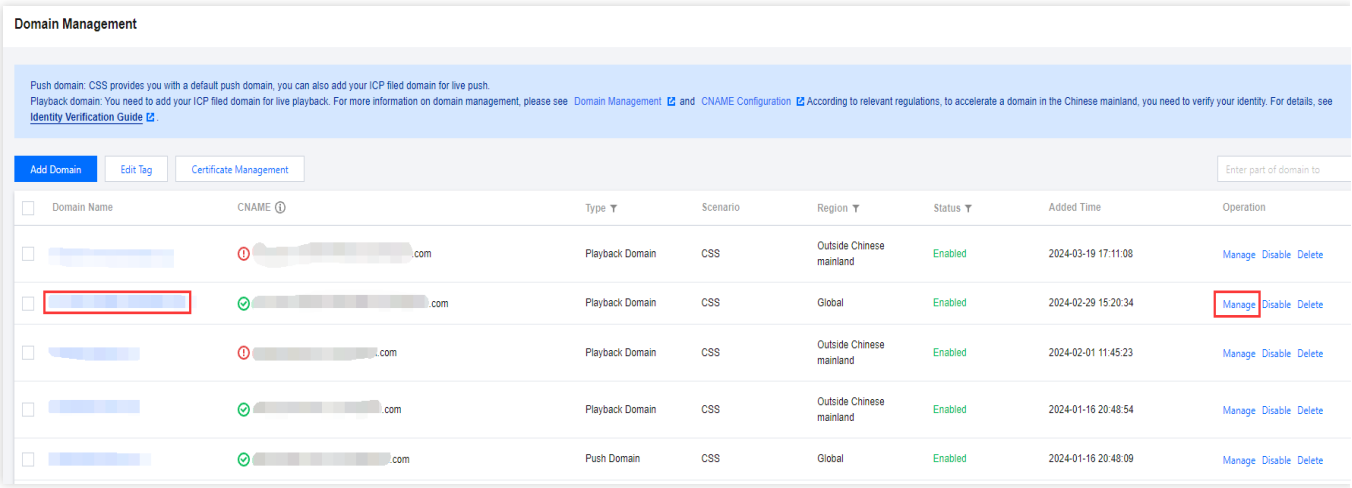


3. Modify the configuration and click **Save**.

Disabling IP Allowlist/Blocklist

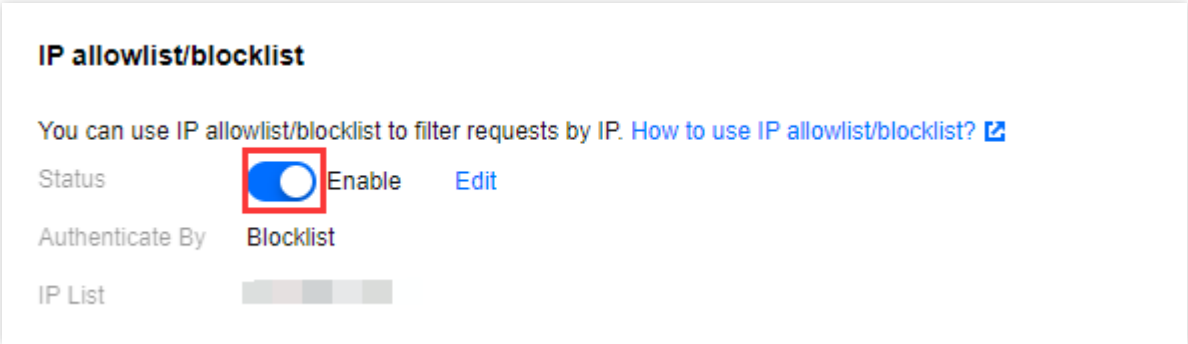
Follow the steps below to disable IP allowlist/blocklist:

1. Select Domain Management on the left sidebar, and click the target **playback domain** or click **Manage** on the right to enter the domain management page.



2. Select the **Access Control** tab. In the **IP allowlist/blocklist** area, click

to disable IP allowlist/blocklist.


IP allowlist/blocklist
You can use IP allowlist/blocklist to filter requests by IP. How to use IP allowlist/blocklist?
Status
Enable
Edit
Authenticate By
Blocklist
IP List

Blocking Playback by Protocol

Last updated：2024-07-11 17:53:34

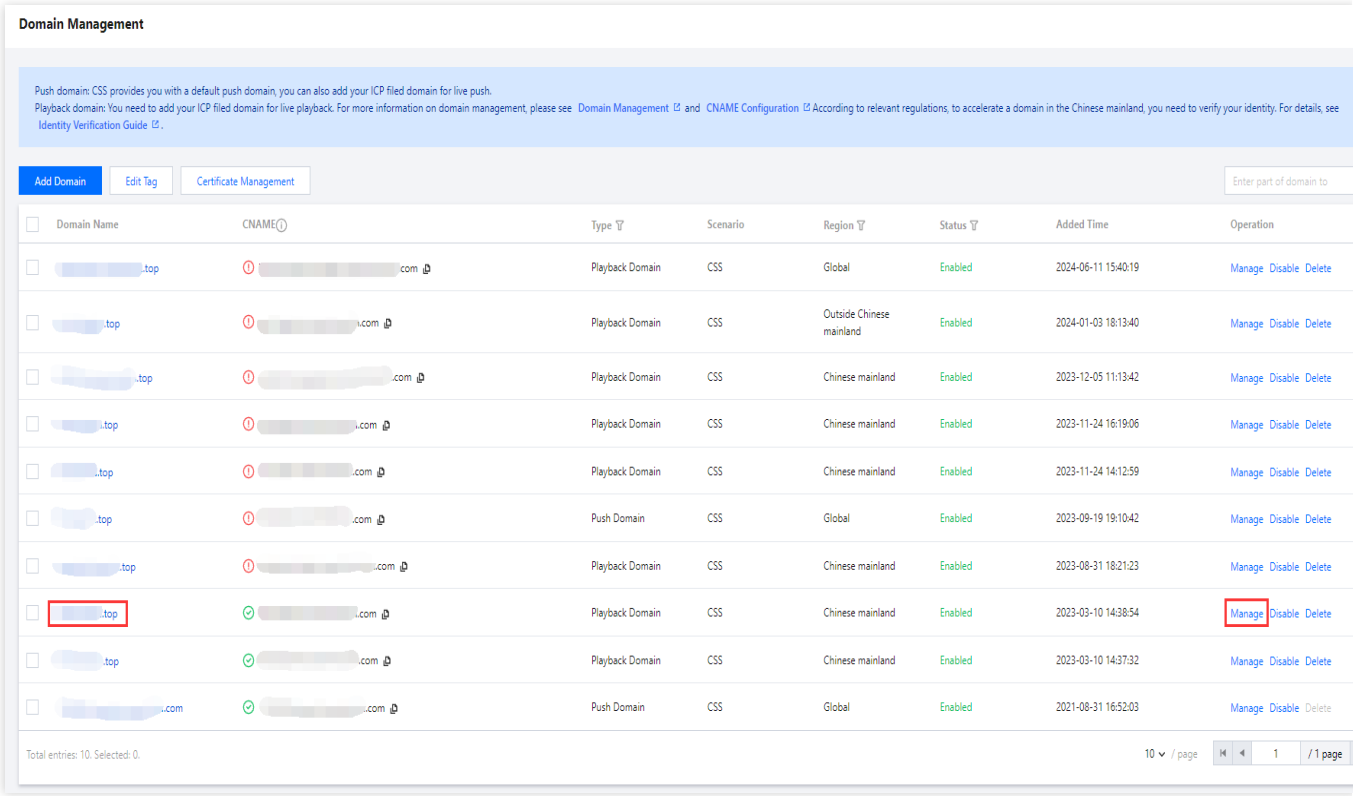
You can block playback for a domain by blocking specific protocols. Playback requests that use the blocked protocols will be rejected.

Prerequisites

You have activated CSS and logged in to the CSS console.
You have added a playback domain name.

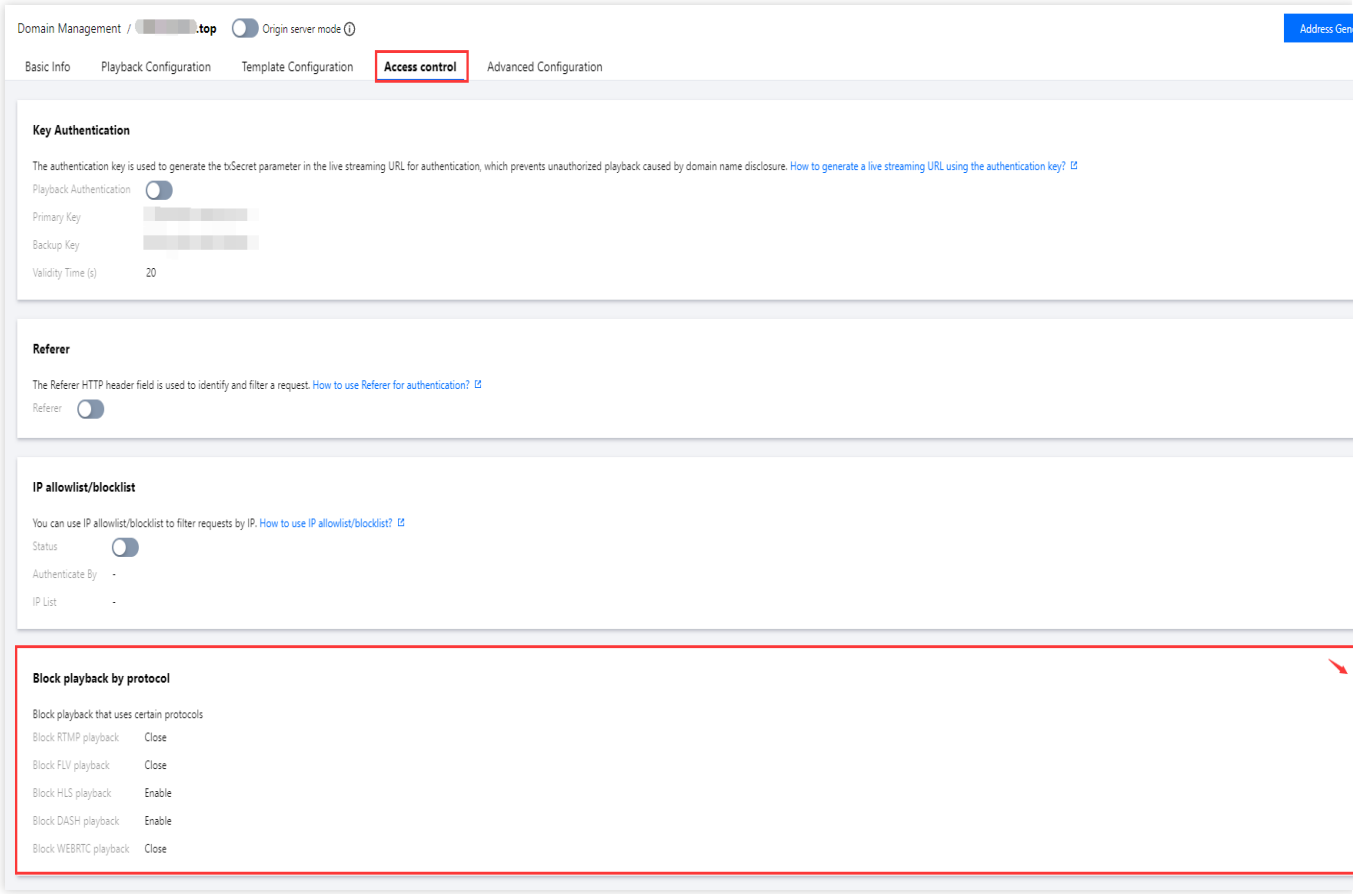
Blocking Protocols

1. Select Domain Management on the left sidebar. Click the name of the target playback domain or click **Manage** on the right to enter the domain management page.

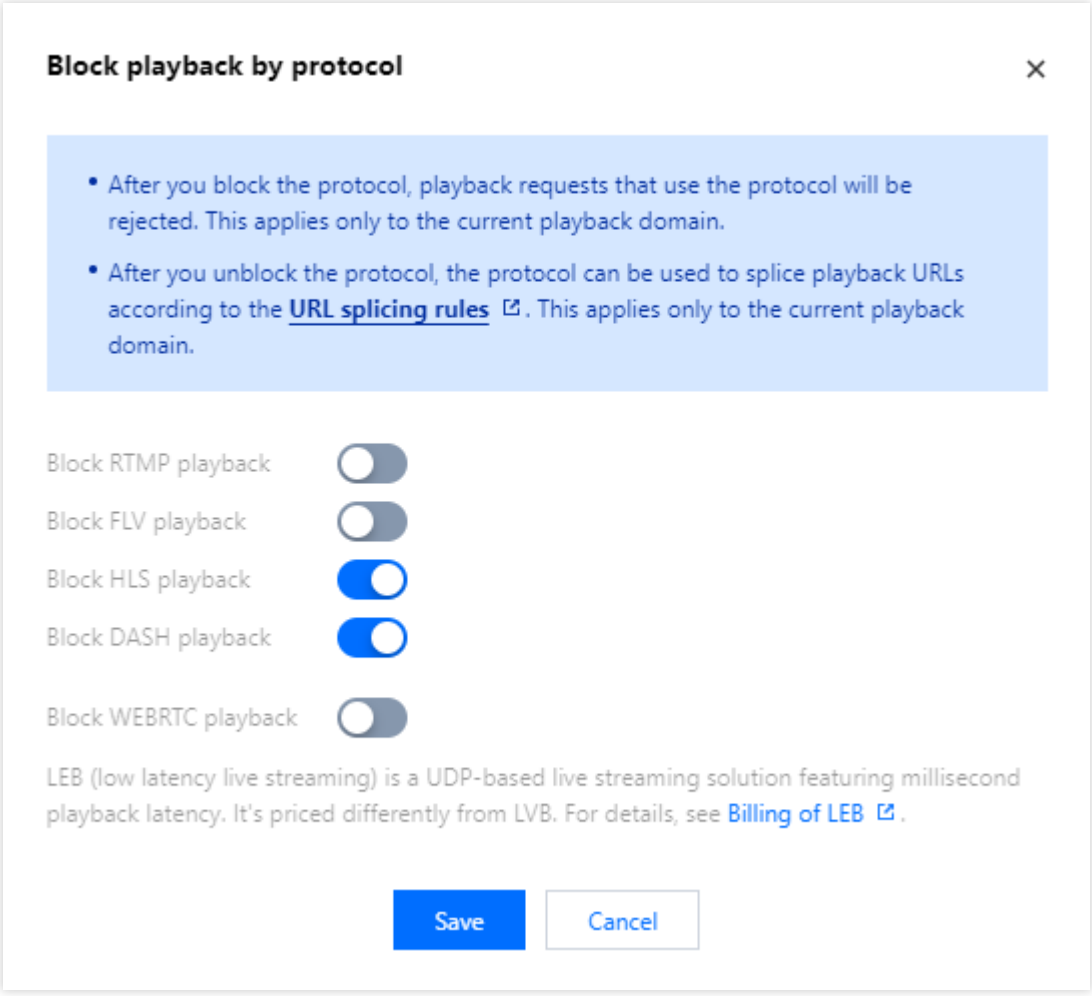


2. Select the **Access Control** tab. In the **Block playback by protocol** area, you can block playback that uses the RTMP, FLV, HLS, DASH, and WebRTC protocols.

3. Click **Edit** and toggle on the protocols you want to block.



4. Click **Save**.



Note:

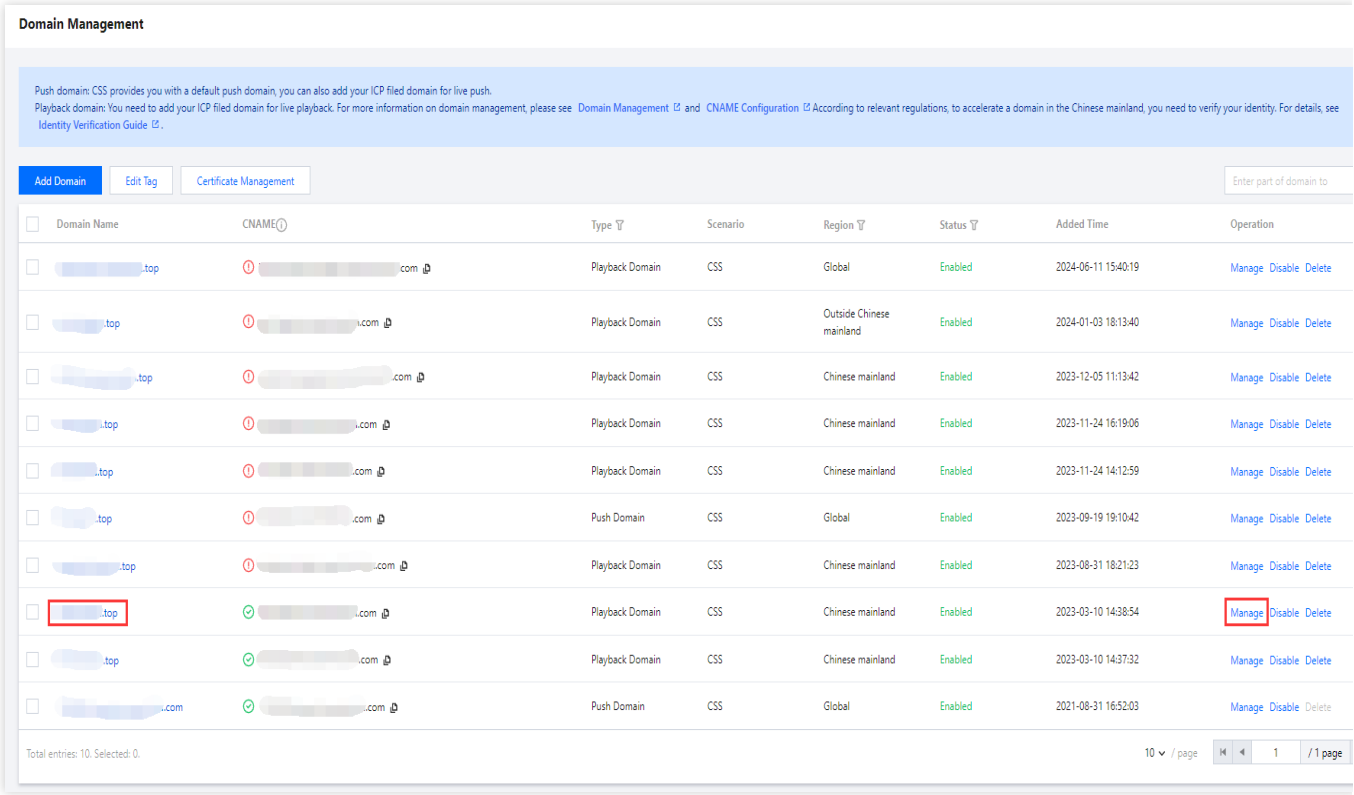
It takes a while for the blocking configuration to take effect. After configuring blocked protocols, please wait for the configuration to take effect before you block other protocols.

Except for HLS, protocol blocking only takes effect for new live streams. It does not affect ongoing streams.

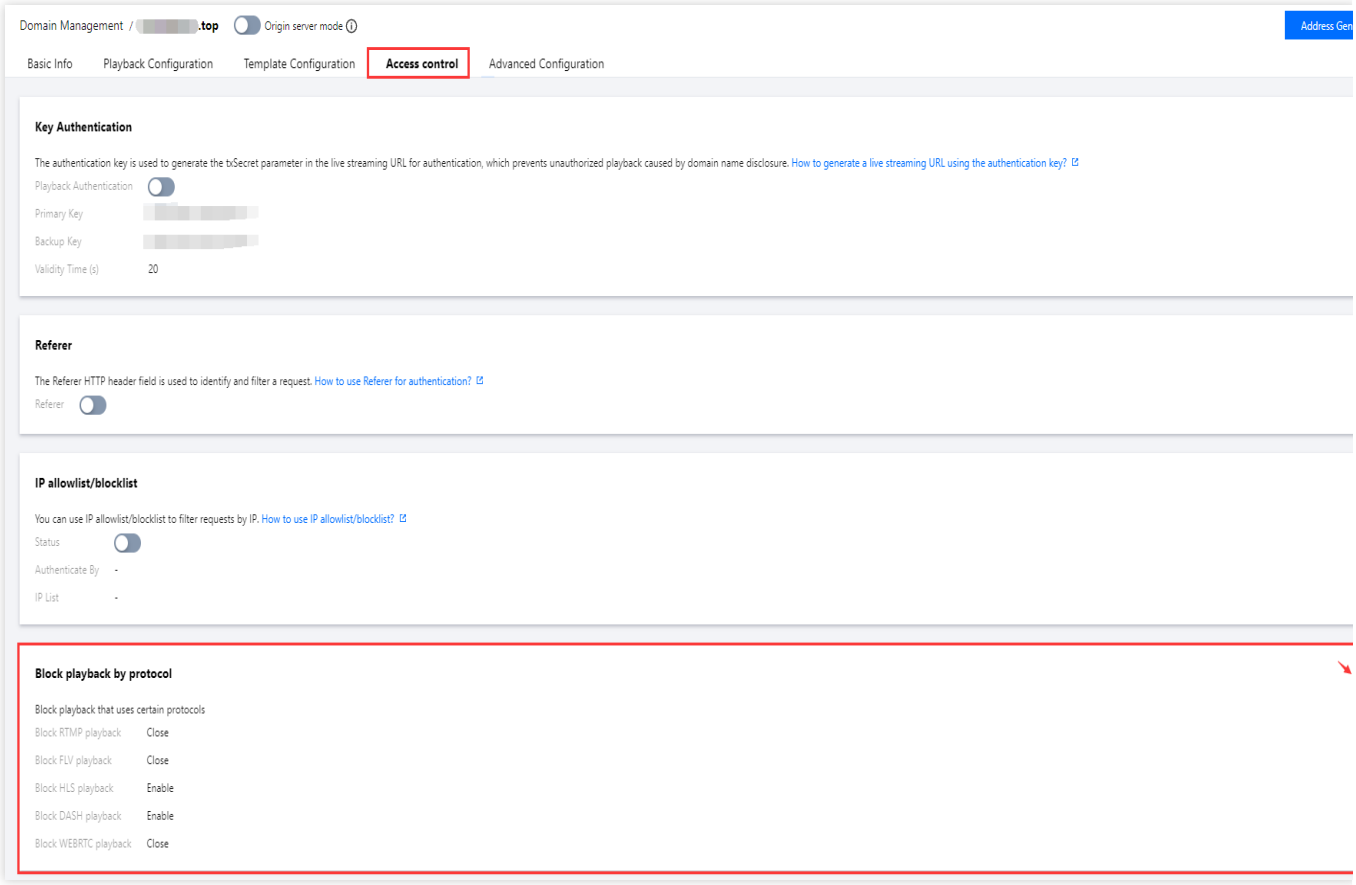
Unblocking Protocols

To unblock a blocked protocol, follow the steps below:

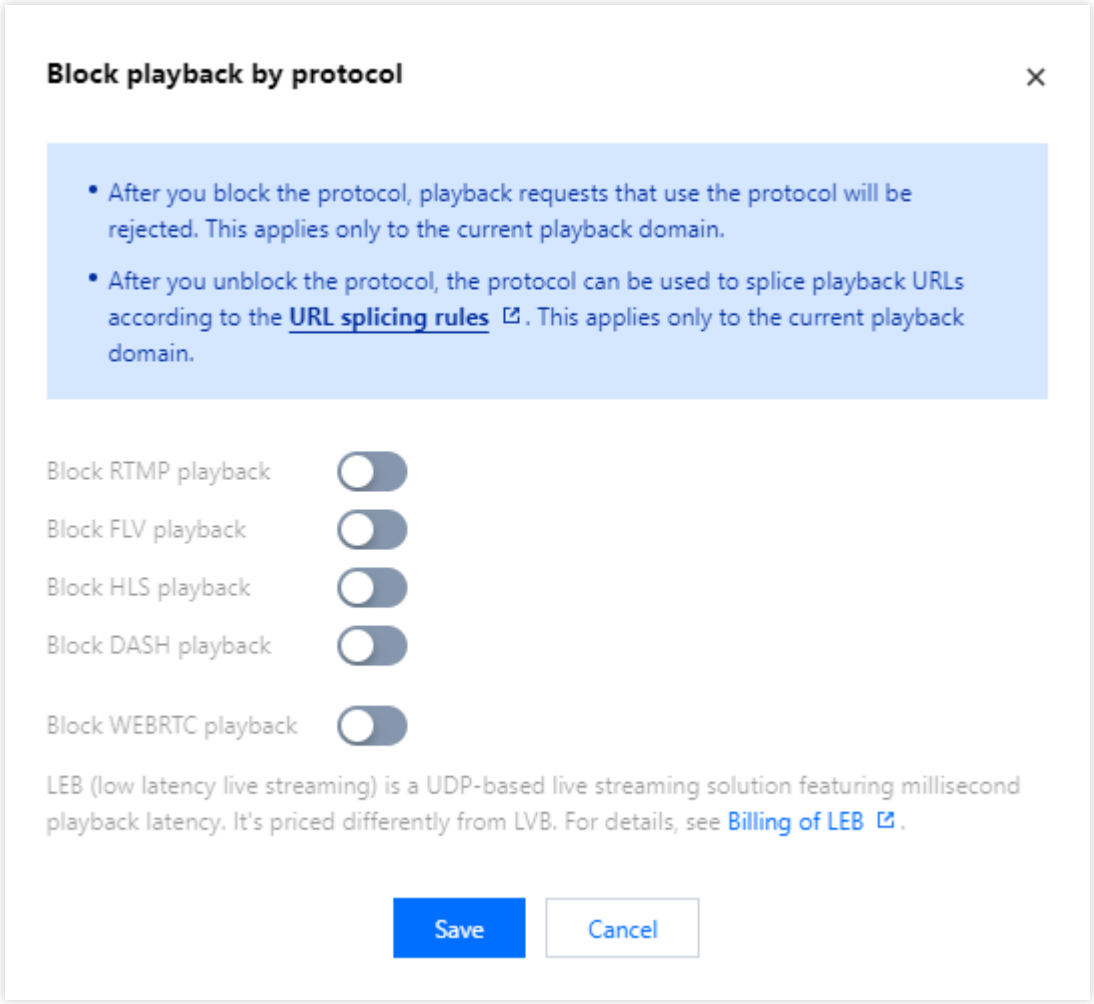
1. Select Domain Management on the left sidebar. Click the name of the target playback domain or click **Manage** on the right to enter the domain management page.



2. Select the **Access Control** tab. In the **Block playback by protocol** area, toggle off the protocol you want to unblock.


Domain Management / .top
Origin server mode
Address Gen
Basic Info
Playback Configuration
Template Configuration
Access control
Advanced Configuration
Key Authentication
The authentication key is used to generate the txSecret parameter in the live streaming URL for authentication, which prevents unauthorized playback caused by domain name disclosure. How to generate a live streaming URL using the authentication key?
Playback Authentication
Primary Key
Backup Key
Validity Time (s) 20
Referer
The Referer HTTP header field is used to identify and filter a request. How to use Referer for authentication?
Referer
IP allowlist/blocklist
You can use IP allowlist/blocklist to filter requests by IP. How to use IP allowlist/blocklist?
Status
Authenticate By -
IP List -
Block playback by protocol
Block playback that uses certain protocols
Block RTMP playback Close
Block FLV playback Close
Block HLS playback Enable
Block DASH playback Enable
Block WEBRTC playback Close

3. Click **Save**.


Block playback by protocol
After you block the protocol, playback requests that use the protocol will be rejected. This applies only to the current playback domain.
After you unblock the protocol, the protocol can be used to splice playback URLs according to the URL splicing rules. This applies only to the current playback domain.
Block RTMP playback
Block FLV playback
Block HLS playback
Block DASH playback
Block WEBRTC playback
LEB (low latency live streaming) is a UDP-based live streaming solution featuring millisecond playback latency. It's priced differently from LVB. For details, see Billing of LEB.
Save
Cancel

Latency Control

Last updated：2024-05-28 10:22:55

Set a latency that fits your needs. Note that setting the latency too low may cause playback to stutter.

Note

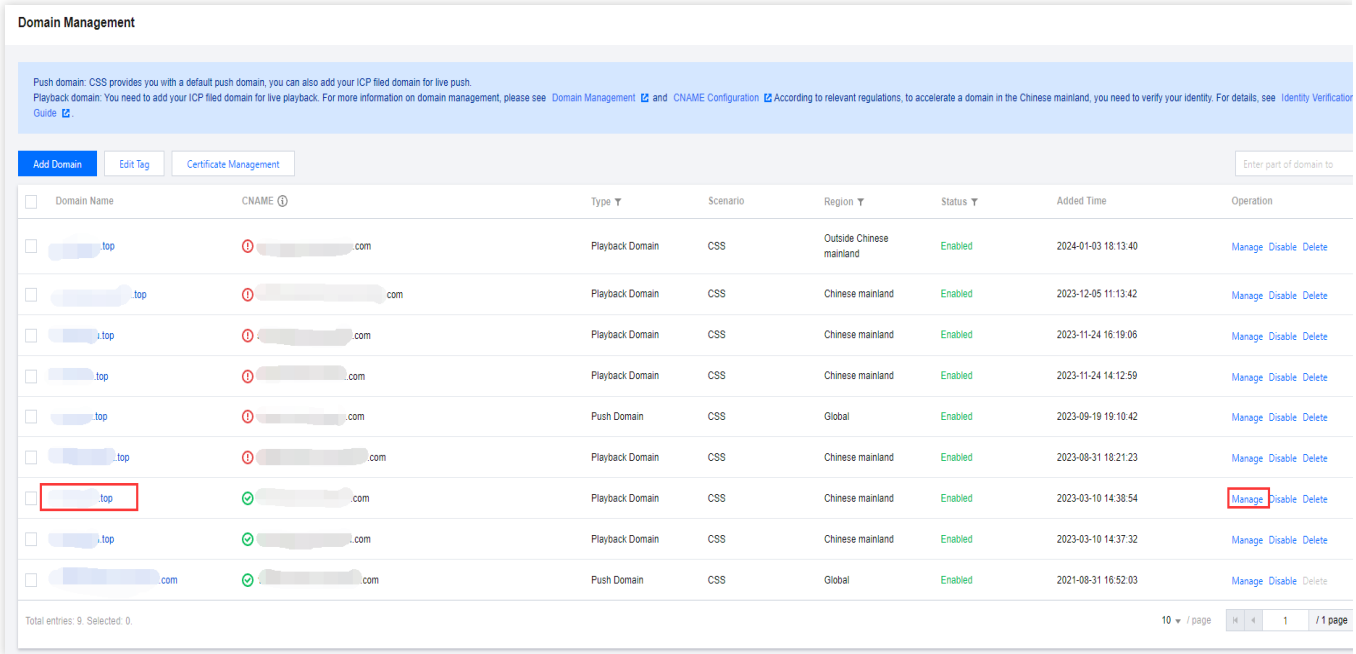
Latency configuration will take effect approximately 10 minutes after configuration.

Prerequisites

You have activated CSS and logged in to the CSS console.
You have added a playback domain name.

Latency control

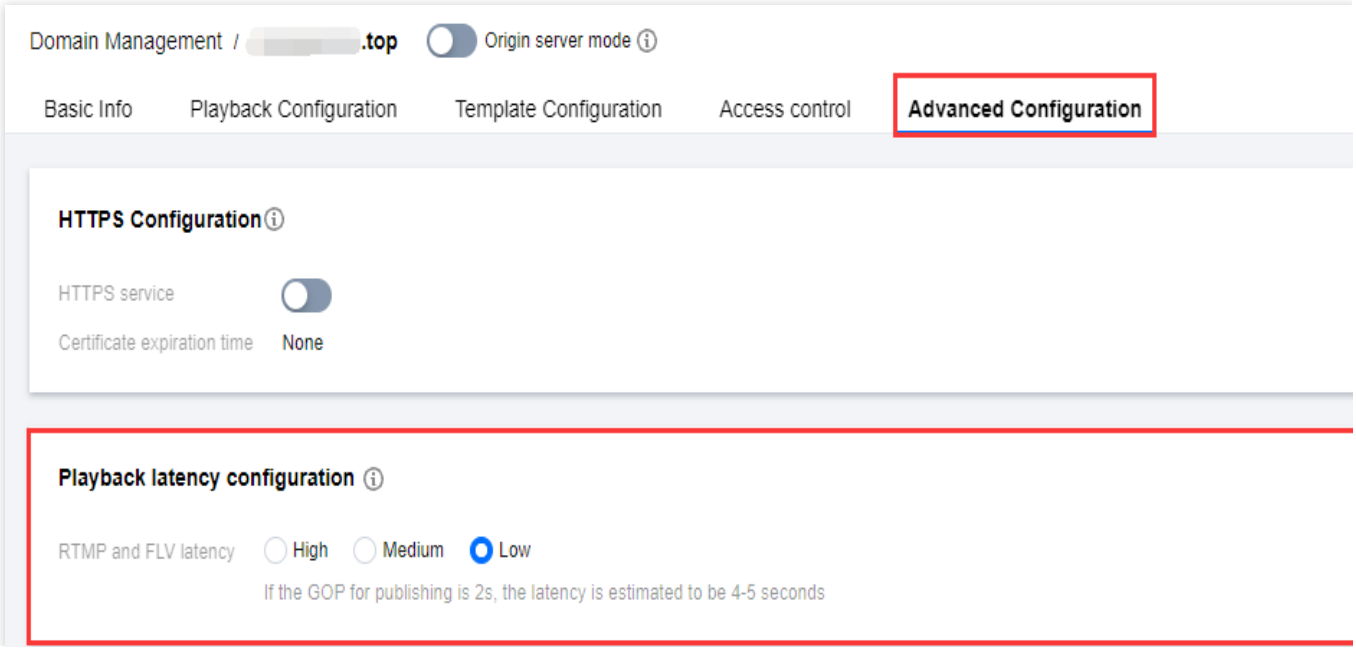
1. Select Domain Management on the left sidebar and click the **playback domain** for which you want to configure RTMP and FLV latency, or click **Manage** on the right to enter the details page.



2. In **Advanced Configuration** > **Playback latency configuration** , you can configure the latency for RTMP and FLV.

3. When live streaming latency parameters are configured, it is recommended to select appropriate latency parameters based on your actual business needs. It is advisable to set the GOP for publishing to 1-2s because the larger the GOP value, the greater the live streaming latency. Note that setting the latency too low may cause playback to stutter.
4. When GOP is set to two seconds, the latency is as follows:

Setting	High	Medium	Low
Estimated Latency	7-9s	5-7s	4-5s



HTTP Response Header Configuration

Last updated：2024-05-28 10:21:53

You can use HTTP headers to define fields that carry information about HTTP transactions. Header fields work on the domain level. This means the header fields you configure will take effect for all responses under your domain.

Prerequisites

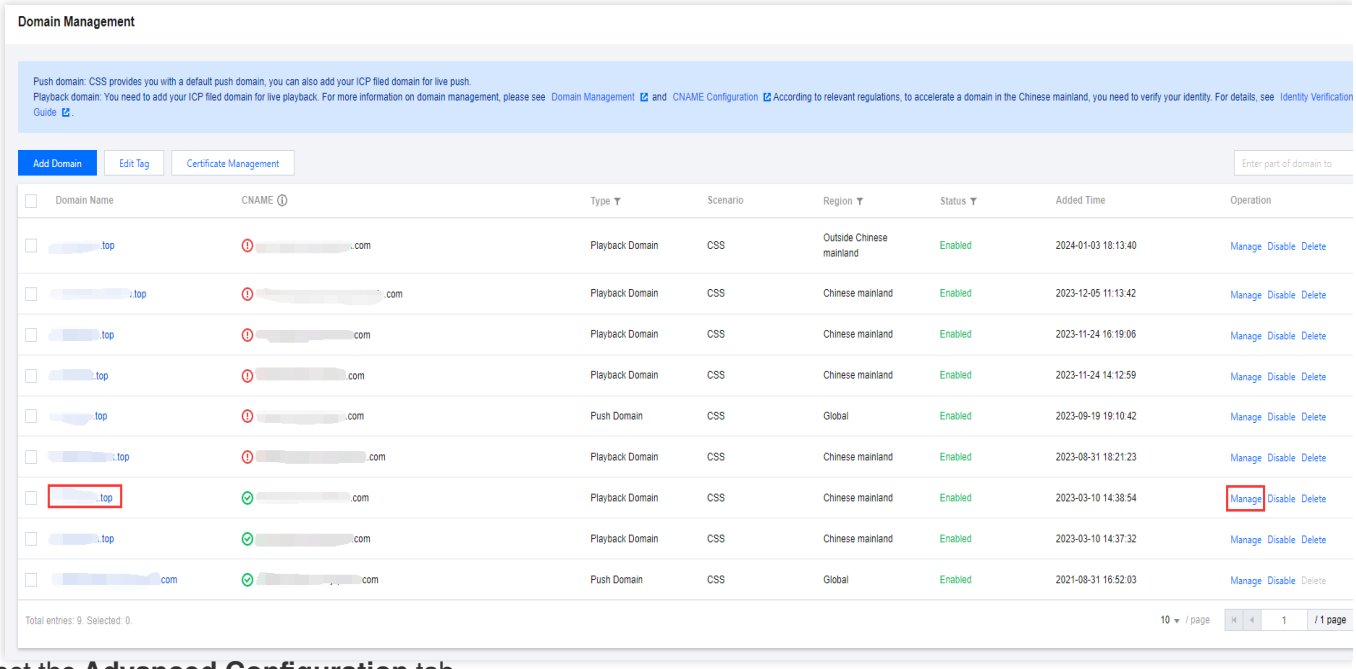
You have logged in to the CSS console.
You have added a playback domain name.

Use Limits

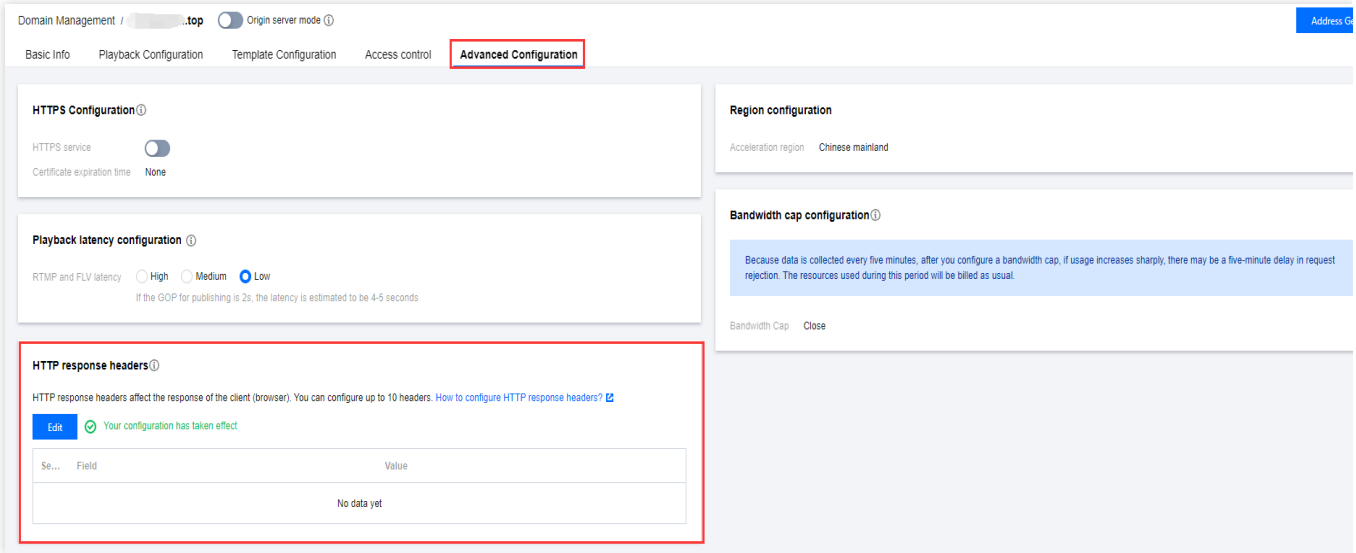
You can configure at most 10 header fields.
You cannot add two fields with the same name. To specify multiple values for a field, use this format: `value 1, value 2, value 3`.
If a field you configure is the same as a field used by the CSS backend, you will be asked to modify it.
A custom field can be 1-100 characters long and can contain letters, numbers, and hyphens (-).
The value of a field cannot be empty. It can be 1-1,000 characters long and cannot contain Chinese characters.

Configuring HTTP Response Header

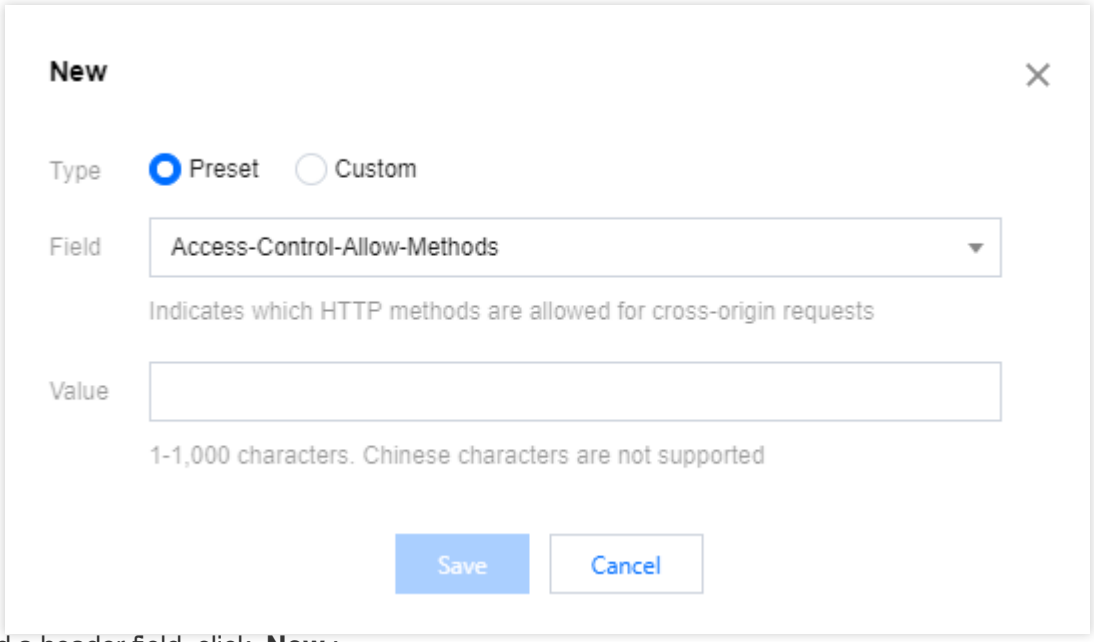
1. Go to Domain Management. Click the name of your **playback domain** or click **Manage** on the right.



2. Select the **Advanced Configuration** tab.

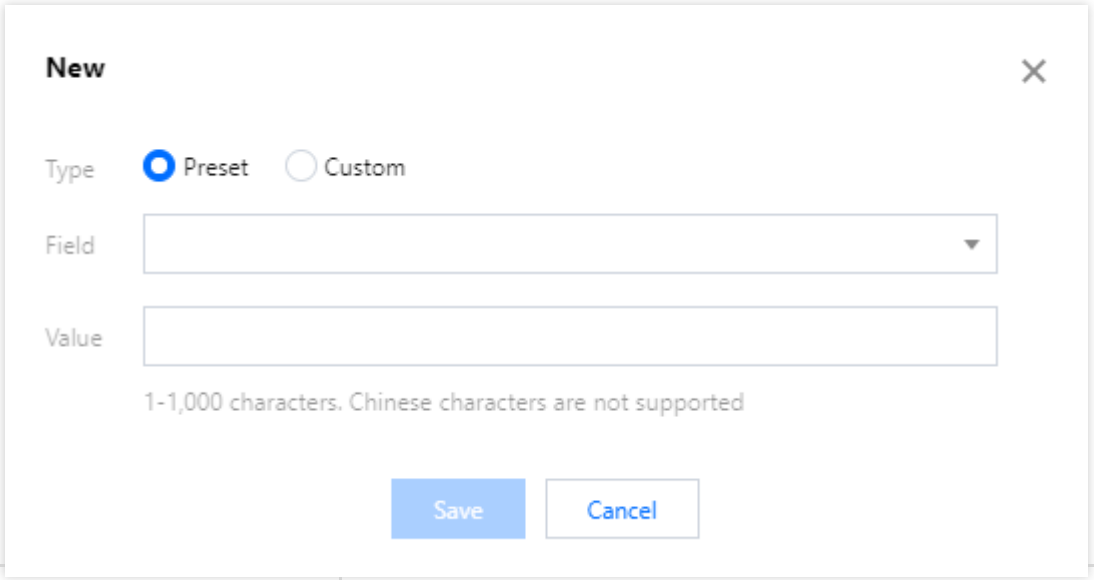


3. In the **HTTP response headers** area, click **Edit** to add new header fields or modify/delete existing header fields.



To add a header field, click **New** :

Select **Preset** to add a preset field: `Access-Control-Allow-Methods` , `Access-Control-Max-Age` , or `Access-Control-Expose-Headers` .



Field	Description
Access-Control-Allow-Methods	Indicates which HTTP methods are allowed for cross-origin requests. You can specify multiple methods at a time: Access-Control-Allow-Methods: POST, GET, OPTIONS.
Access-Control-Max-Age	Indicates how long (seconds) the results of a preflight request can be cached
Access-Control-Expose-Headers	Indicates which headers can be exposed to clients as part of the response

Select **Custom** to add a custom field.

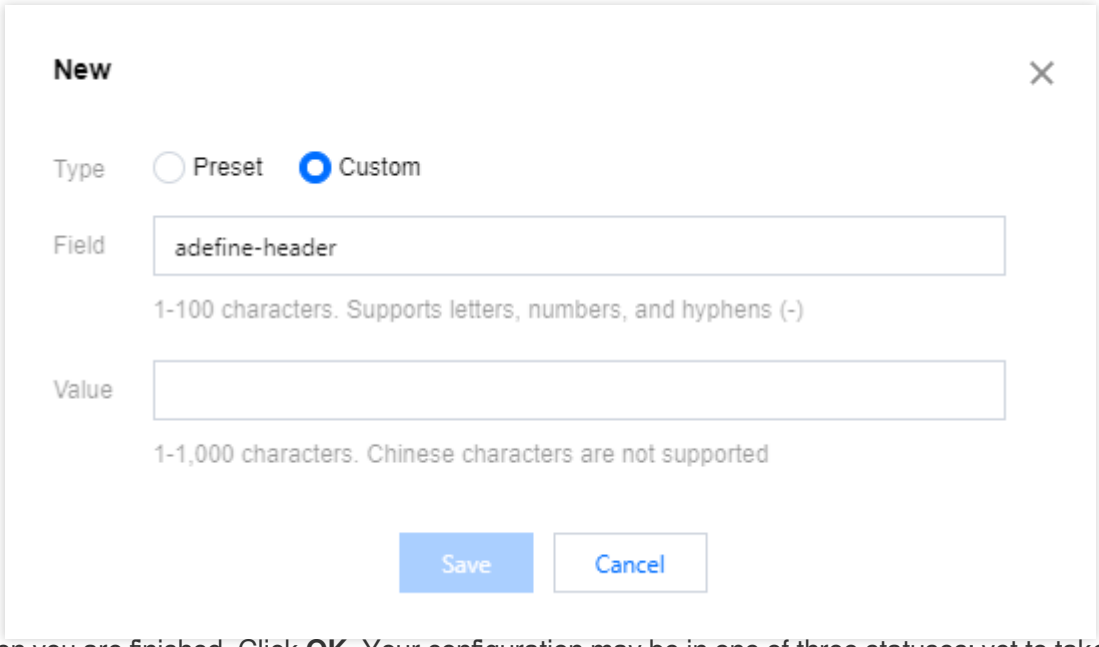
Note:

The name of a custom field can be 1-100 characters long and can contain letters, numbers, and hyphens. The value of a custom field can be 1-1,000 characters long and cannot contain Chinese characters.

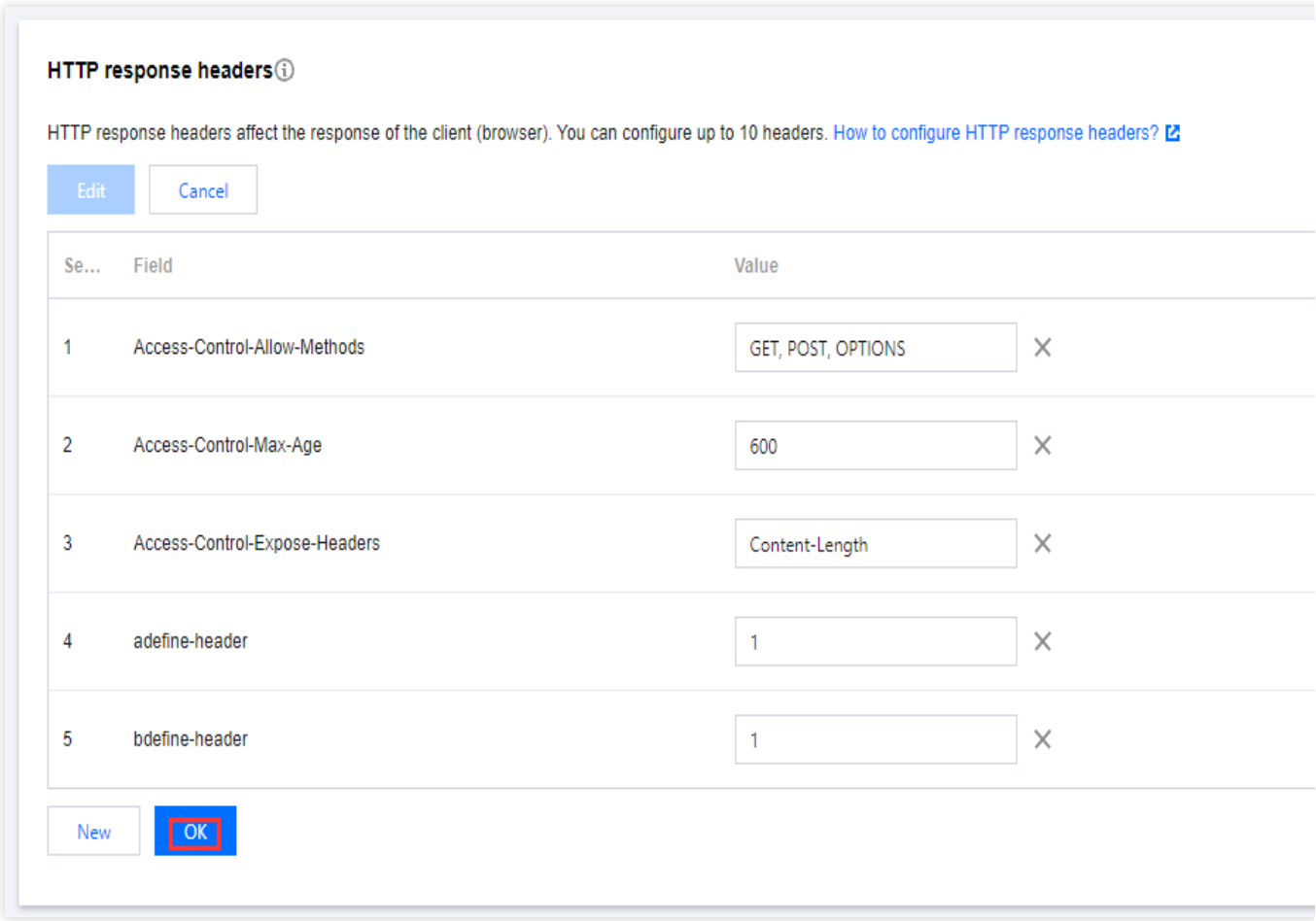
The system has default support for the header parameter Access-Control-Allow-Origin, which is used to enable cross-domain requests without the need for customization. There are two specific scenarios:

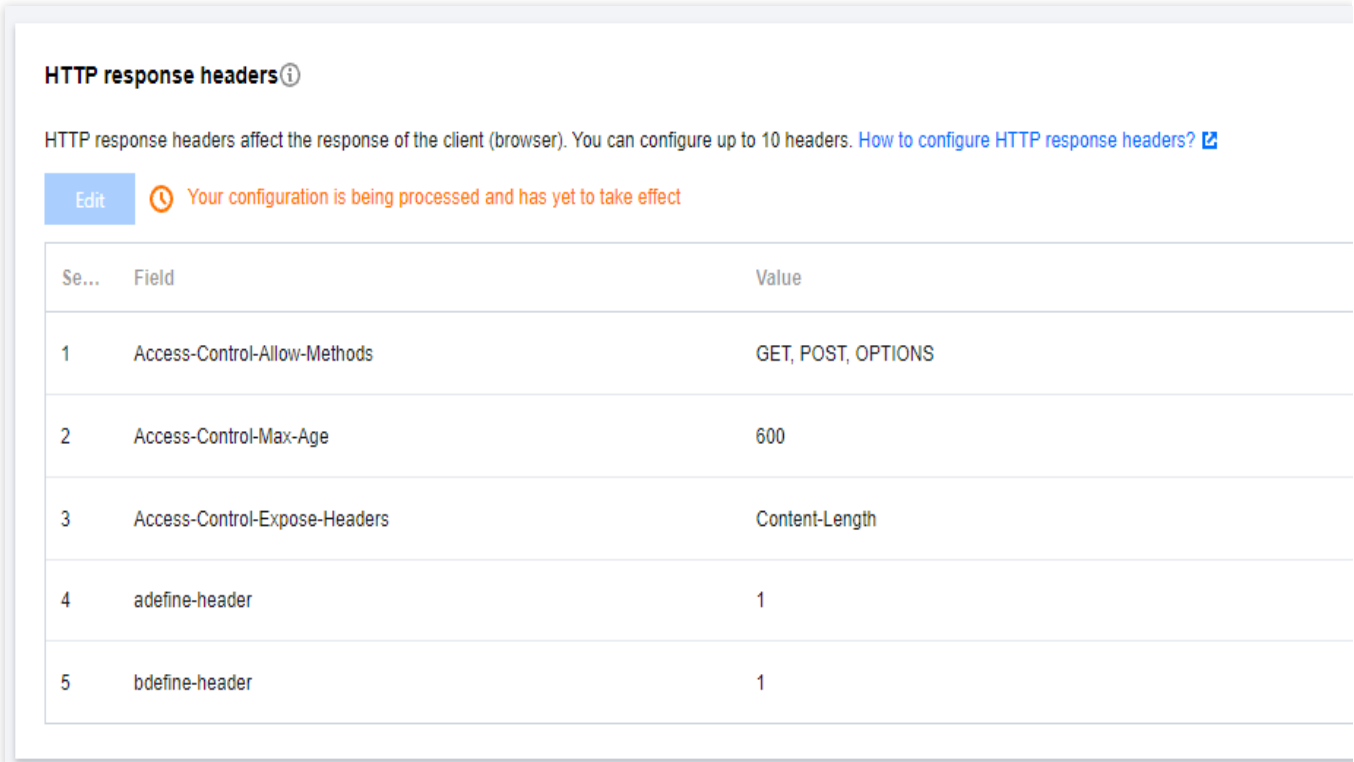
When the request header does not include Origin, the returned header will be 'Access-Control-Allow-Origin: *'.

When the request header includes 'Origin: ${Origin}', the returned header will be 'Access-Control-Allow-Origin: ${Origin}'. For example, when the request header has Origin: https://cloud.tencent.com, the returned header will be Access-Control-Allow-Origin: https://cloud.tencent.com.



4. When you are finished, Click **OK**. Your configuration may be in one of three statuses: yet to take effect, failed, or effective.


HTTP response headers
HTTP response headers affect the response of the client (browser). You can configure up to 10 headers. How to configure HTTP response headers?
Edit
Cancel
Se...
Field
Value
1
Access-Control-Allow-Methods
GET, POST, OPTIONS
2
Access-Control-Max-Age
600
3
Access-Control-Expose-Headers
Content-Length
4
adefine-header
1
5
bdefine-header
1
New
OK


HTTP response headers
HTTP response headers affect the response of the client (browser). You can configure up to 10 headers. How to configure HTTP response headers?
Edit
Your configuration is being processed and has yet to take effect
Se...
Field
Value
1
Access-Control-Allow-Methods
GET, POST, OPTIONS
2
Access-Control-Max-Age
600
3
Access-Control-Expose-Headers
Content-Length
4
adefine-header
1
5
bdefine-header
1

Access Control by Region Configuration

Last updated：2024-06-17 18:09:12

Access control by region lets you can manage a blocklist or allowlist for playback regions for the current domain, providing better control over content distribution in specific areas.

How It Works

If you are configuring a blocklist, requests from the selected regions are banned.
If you are configuring an allowlist, only requests from the selected regions are allowed.

Must-Knows

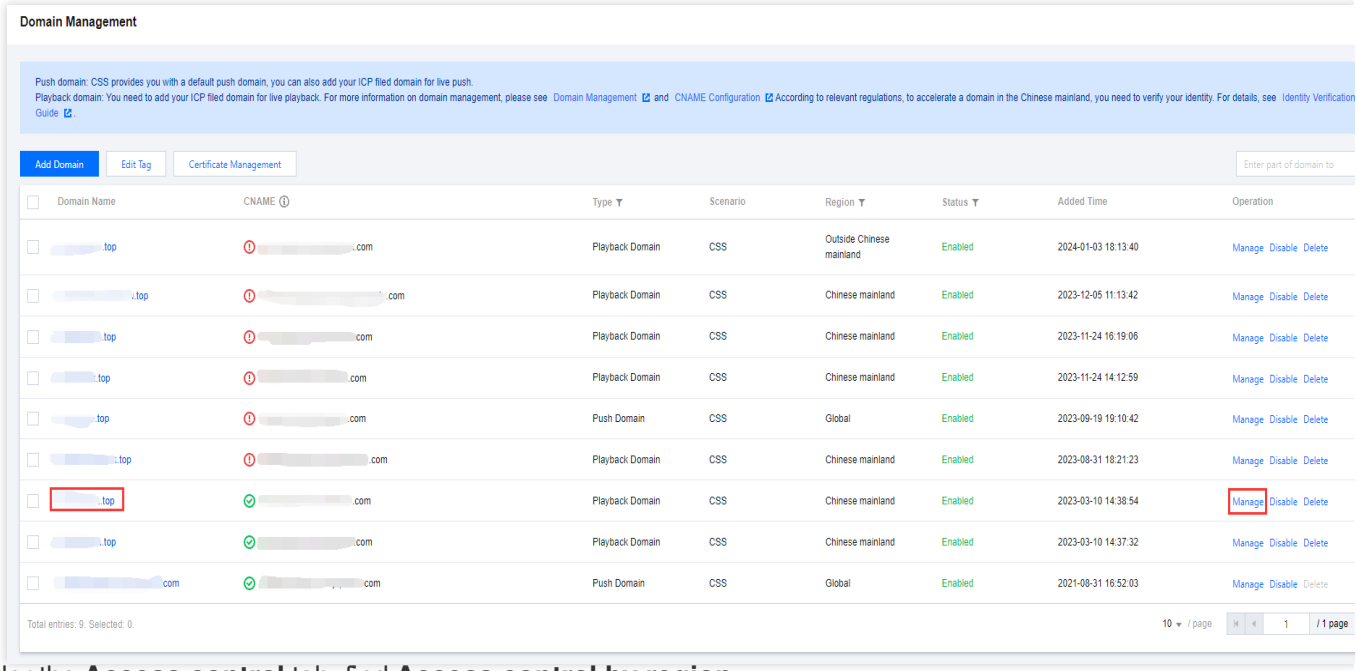
After you complete the configuration of the blocklist and allowlist for the playback region, it takes approximately 10 minutes to take effect.
If you have enabled both the IP Blocklist/Allowlist Configuration and playback region management features, note that the IP blocklist/allowlist takes precedence over playback region management.

Prerequisites

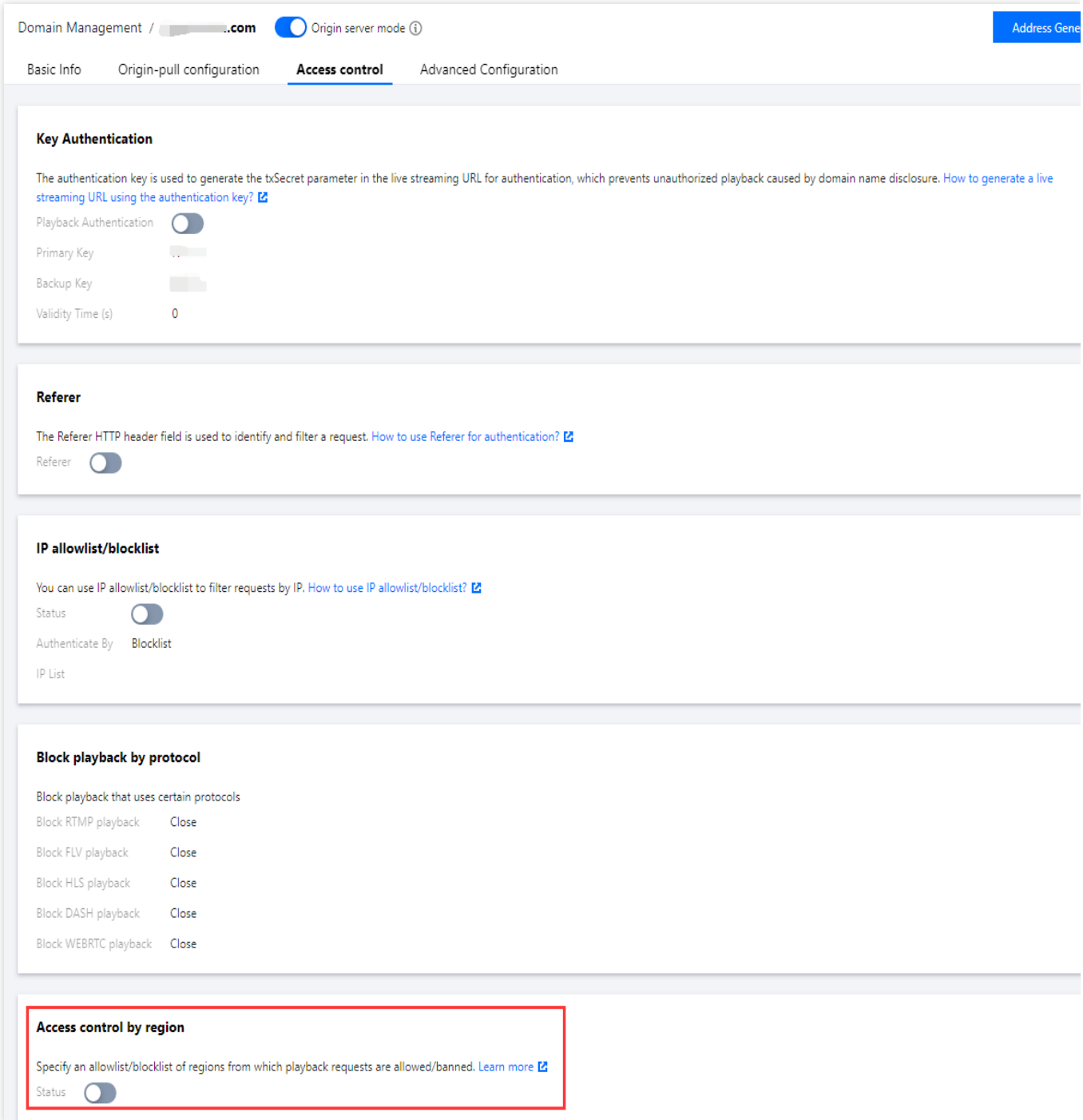
You have activated CSS and logged in to the CSS console.
You have added a playback domain.

Configuring Access Control by Region

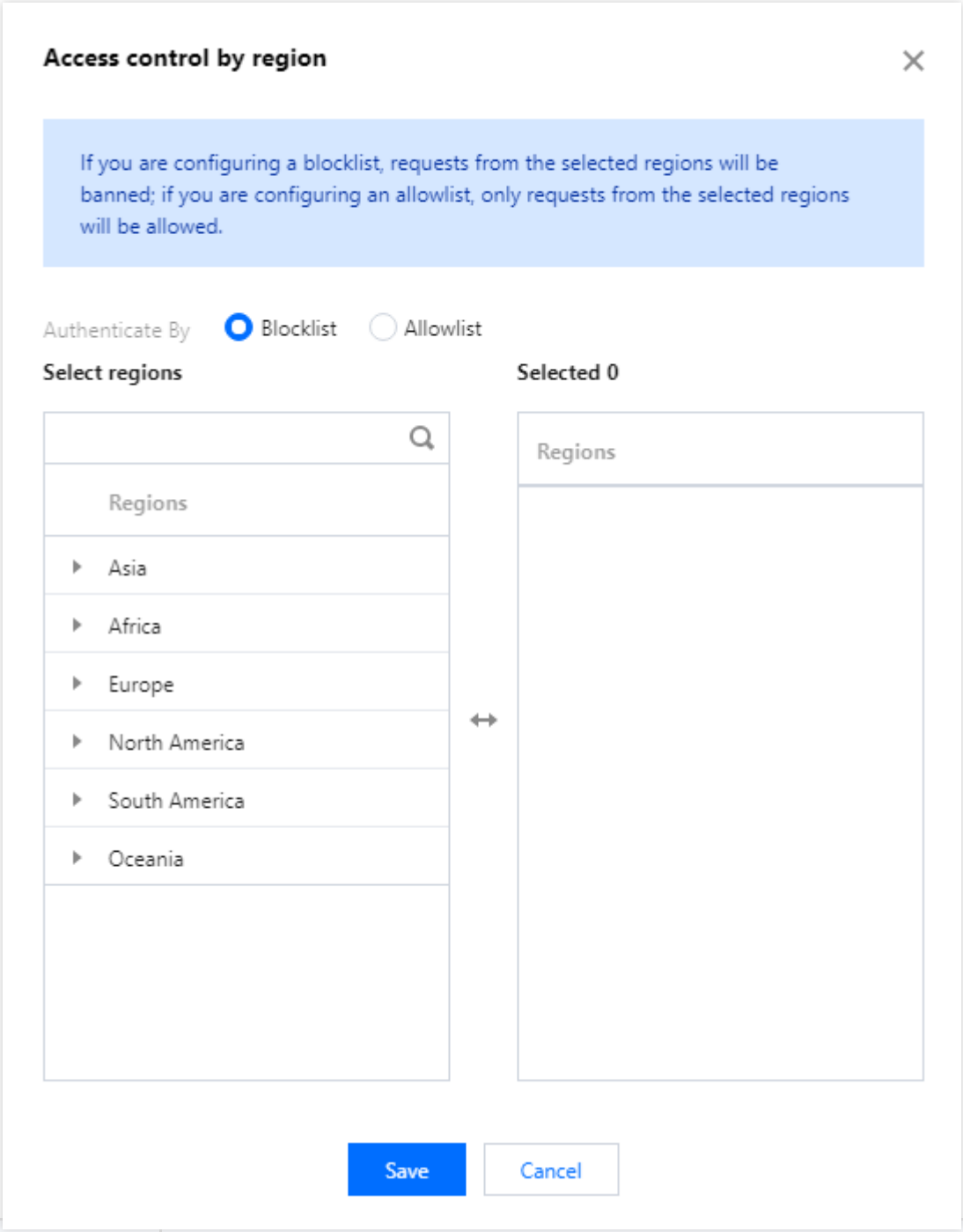
1. Select Domain Management on the left sidebar. Click the **playback domain** you want to configure region management for, or click **Manage** on the right side to enter the Domain Management page.



2. Under the **Access control** tab, find **Access control by region**.



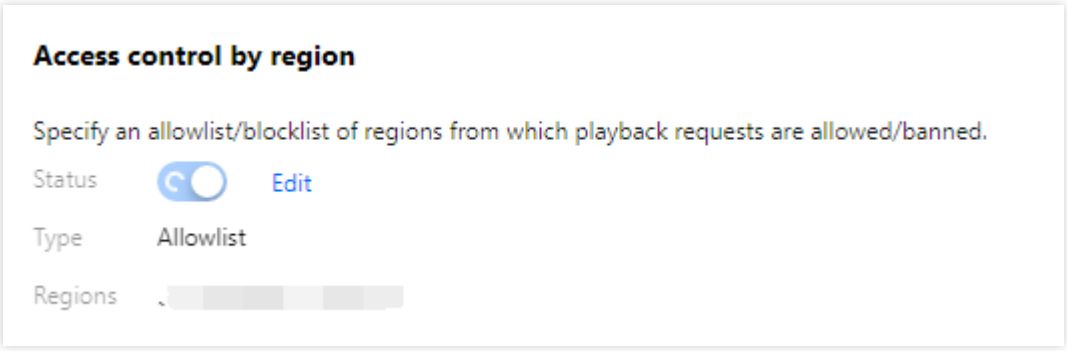
3. Click  to enable access control by region and complete the following settings:



Configuration Item	Description
Authenticate By	Choose whether to configure an **Allowlist** or **Blocklist**. An allowlist and blocklist cannot be effective at the same time. If you configure an **allowlist**, access to live stream content will be allowed only for the regions added to the allowlist. Access will be denied for regions that are not added to the allowlist. If you configure a **blocklist**, access to live stream content will be denied for the regions added to the blocklist. Access will be allowed for all regions that are not added to the blocklist.

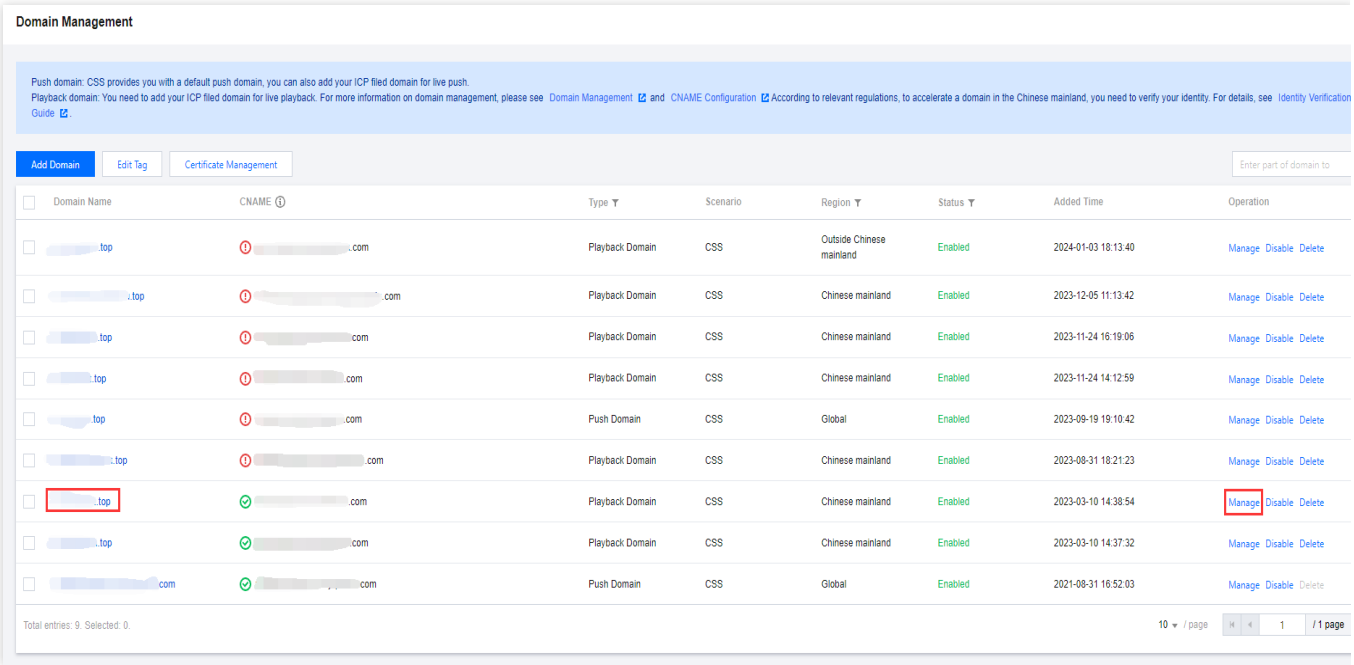
Configuring Regions	You can view and expand regions under **Asia**, **Africa**, **Europe**, **North America**, **South America**, and **Oceania** and them to the list of selected regions. You can also search for regions to find them more quickly.

4. Click **Save** to save the configuration (it takes a while for the configuration to take effect).

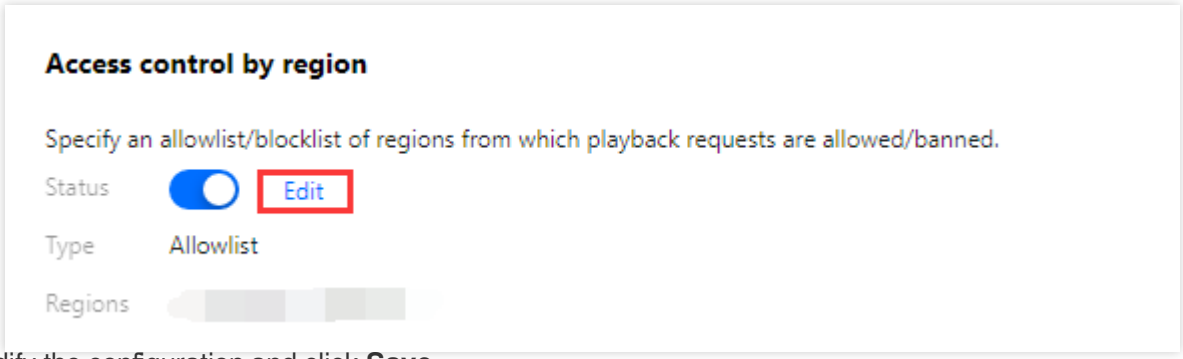


Modifying Access Control by Region

1. Select Domain Management on the left sidebar. Click the **playback domain** you want to modify the region management settings for, or click **Manage** on the right side to enter the Domain Management page.



2. Under the **Access control** tab, find **Access control by region** and click **Edit**.

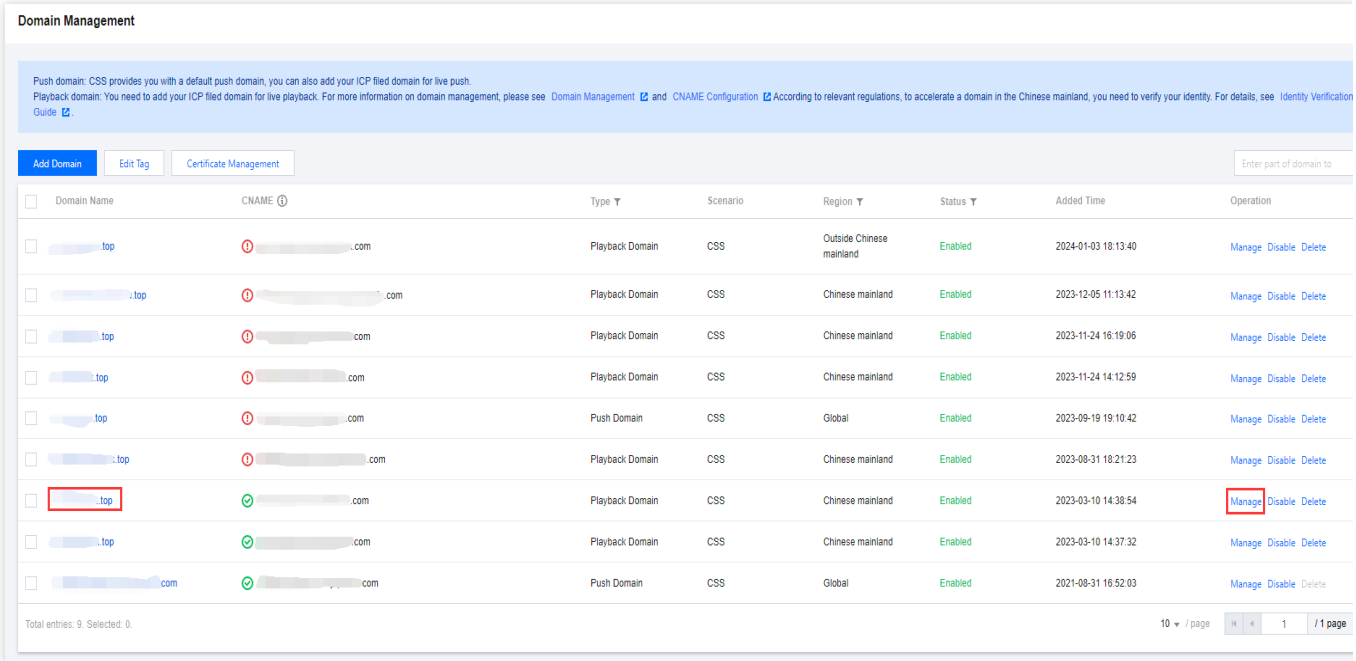


3. Modify the configuration and click **Save**.

Disabling Access Control by Region

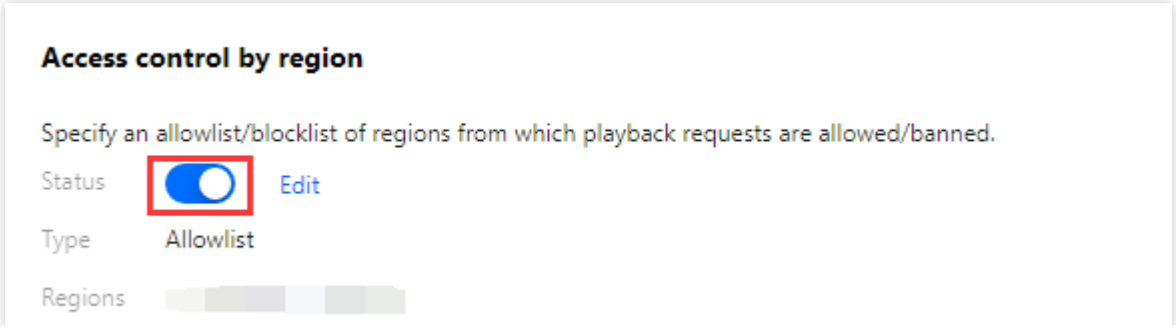
Follow the steps below to disable access control by region:

1. SelectDomain Management on the left sidebar. Click the **Playback Domain** you want to disable access control by region for, or click **Manage** on the right side to enter the Domain Management page.



2. Under the **Access control** tab, find **Access control by region**. Click

to disable access control by region.


Access control by region
Specify an allowlist/blocklist of regions from which playback requests are allowed/banned.
Status
Edit
Type
Allowlist
Regions

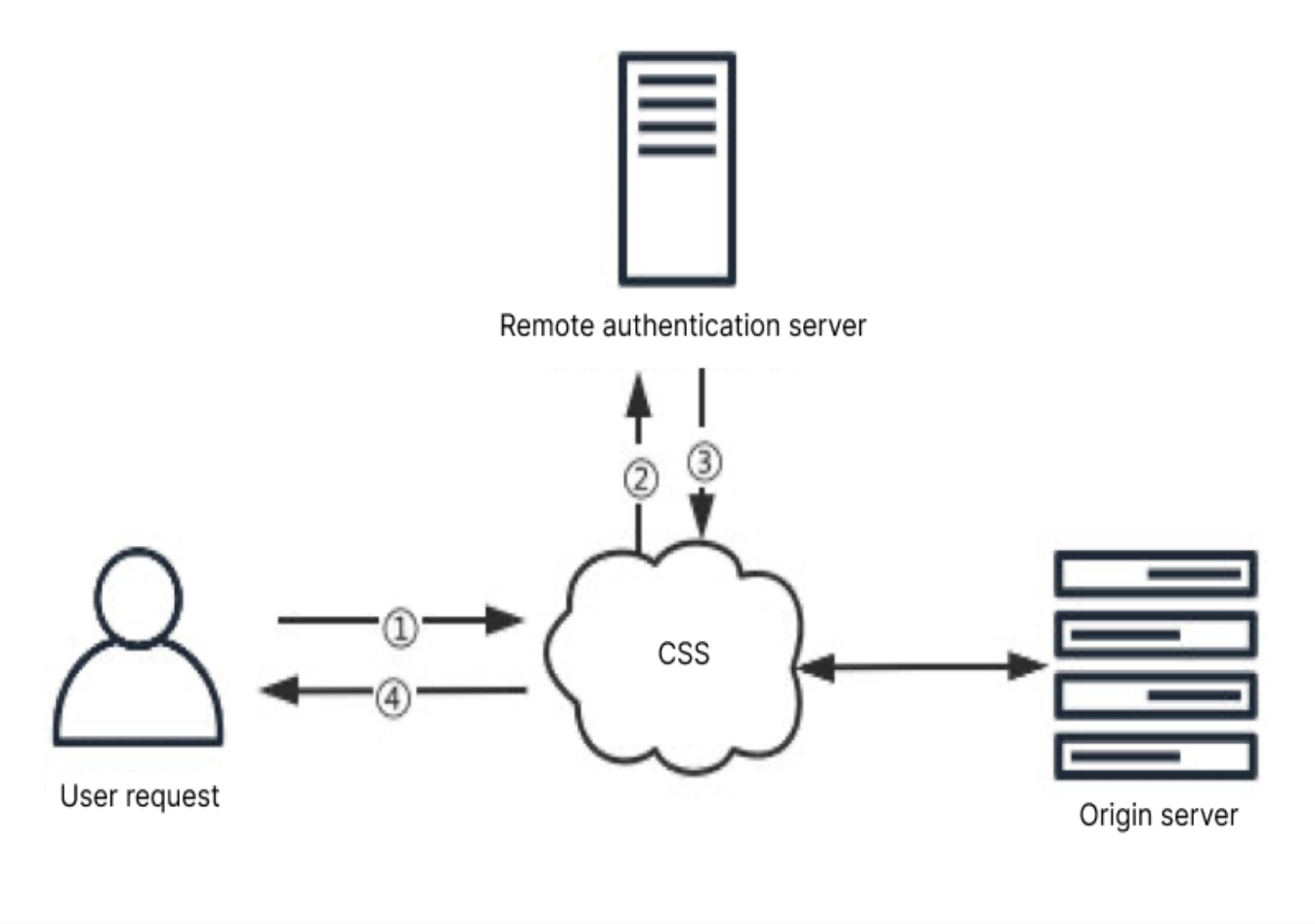
Remote Authentication Configuration

Last updated：2024-06-17 17:00:55

With remote authentication, after authenticating a push/playback request for hotlink protection, CSS will call your server API to send the request to your server so that you can determine whether the request is legitimate. Based on the result your server returns, CSS will approve or reject the push/playback request. This ensures more precise authentication and improves security. However, you need to develop your own authentication server.

Workflow

Remote authentication works as follows:



No	Description
1	A request is sent to CSS.
2	If remote authentication is enabled for the domain, CSS will process the request as specified and then

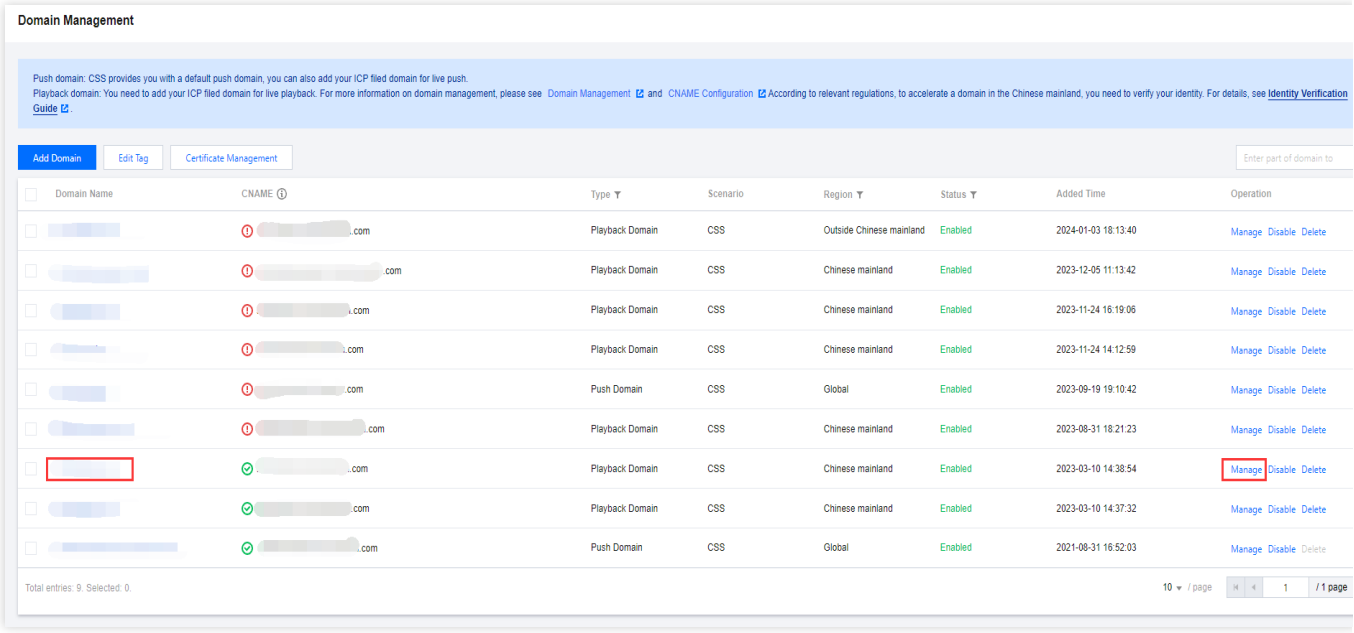
	send it to your authentication server.
3	Your authentication server returns the result. The HTTP status code 200 indicates that the request should be approved, while the code 403 indicates that the request should be rejected.
4	CSS approves or rejects the request based on the result.

Prerequisites

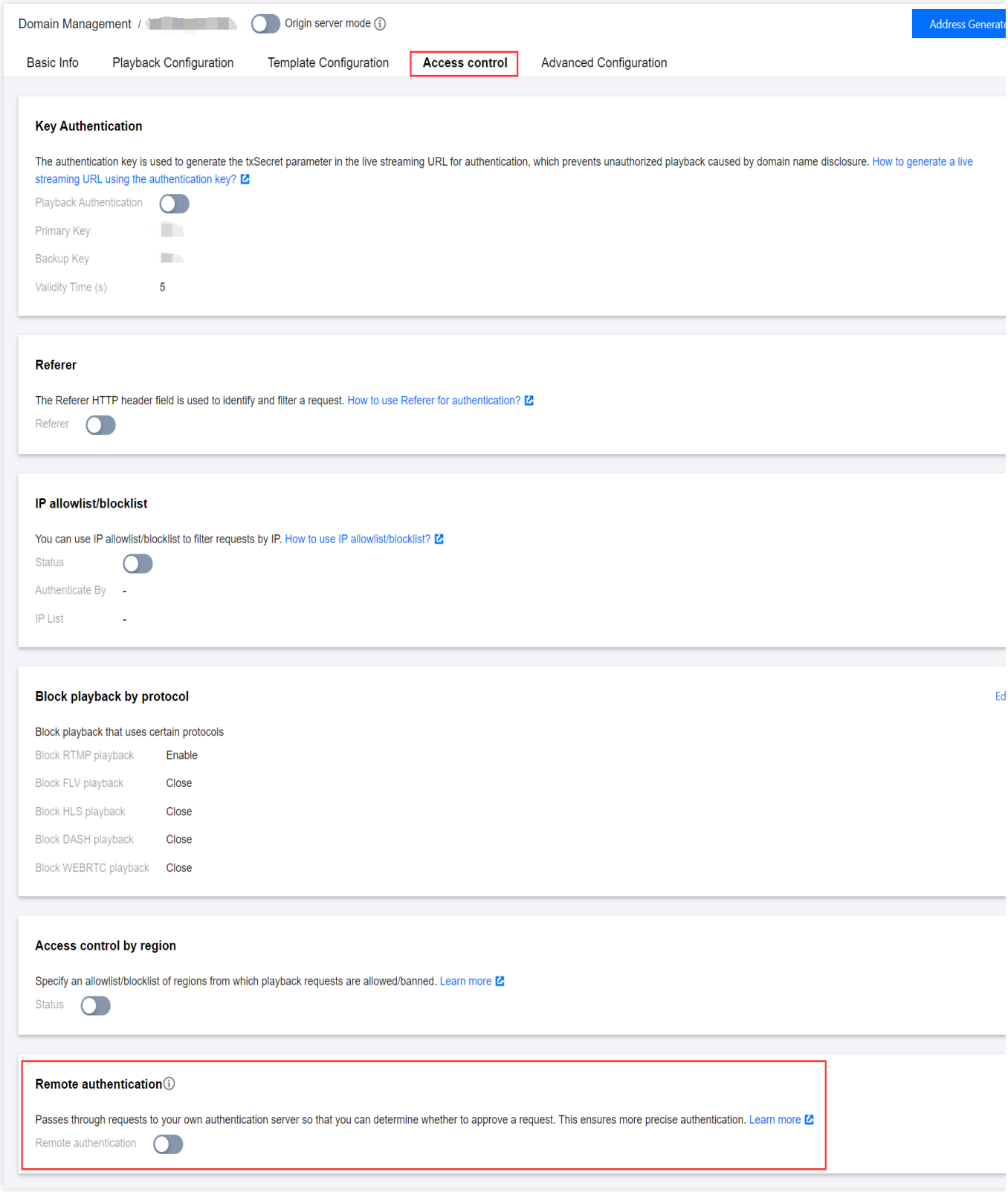
You have activated CSS and logged in to the CSS console.
You have added a playback domain name.

Configuring Remote Authentication

1. Select Domain Management on the left sidebar. Click the name of the target playback domain or click **Manage** on the right to enter the domain management page.



2. Under the **Access Control** tab, find **Remote authentication**.



3. Click

to enable remote authentication and complete the following settings:

Remote authentication

Authentication server address *: https://www.example.com:8080/Api/RemoteAuthenticationInterface

Example: https://www.example.com:8080/Api/RemoteAuthenticationInterface

Request method: POST

URL authentication

Parameters to keep *: Keep all / Remove all / Keep specified parameters

Custom parameters to add

Type	Field	Value	Operation
Select	host	$host	Delete

Add

Request header authentication

Request header to keep *: Keep all / Remove all / Keep specified parameters: value1|value2

Custom parameters to add

Type	Field	Value	Operation
Select	User-Agent	$User-Agent	Delete

Add

Timeout period (ms) per try *: 3000

Max retries *: 1

Behavior upon timeout: Approve / Reject

Asynchronous Authentication

Save Cancel

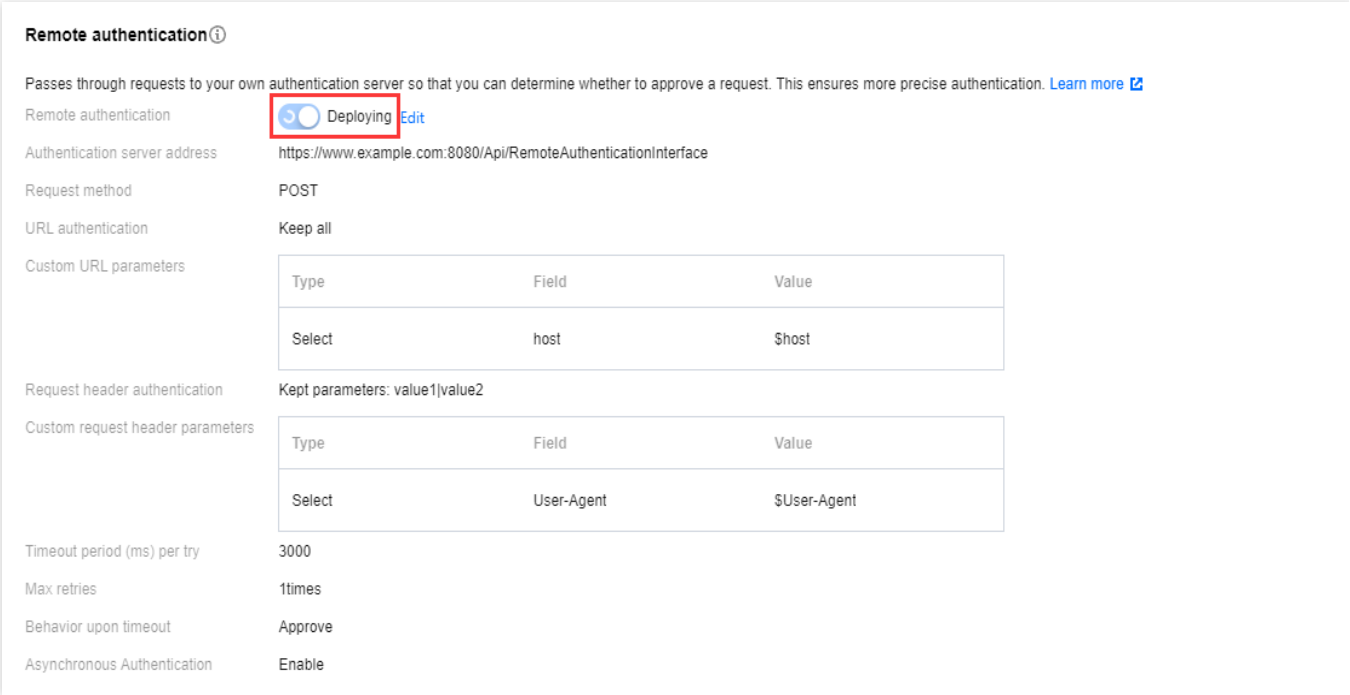
Configuration Item		Description
Authentication server address		The address of your authentication server (required). Format: http(s)://+Domain or IP address+Port+Path.
Request method		POST is selected by default. You can also use HEAD or GET.
URL authentication	Parameters to keep	All URL parameters are kept by default. You can also specify parameters to keep or remove all parameters. If you select "Keep specified parameter", fill in the box the parameters you want to keep. Separate them with |, as in value1|value2. The parameters are case-sensitive (“key” and “KEY” are different parameters).
	Custom parameters to add	Click "Add" to add authentication parameters (max 50). You can either select a parameter to add or add a custom parameter. The parameters you can select include "host", "uri", "client_ip", and "cdn_ip", which represent the playback domain, the original request URL, the client IP address, and the CDN IP address respectively. If you select "Custom", "Parameter" and "Value" are required. The names and values are case-sensitive ("key" and "KEY" are different parameters). Chinese characters are not allowed.
Request header authentication	Request header to keep	All URL parameters are kept by default. You can also specify parameters to keep or remove all parameters. If you select "Keep specified parameter", fill in the box the parameters you want to keep. Separate them with |, as in value1|value2. If you select "Keep all", the CDN node will delete the host header. If you want to keep it, select "Keep specified parameter" or add a custom parameter. The parameters are case-insensitive.
	Custom parameters to add	Click "Add" to add authentication parameters (max 50). You can either select a parameter to add or add a custom parameter. The parameters you can select include "User-Agent", "Referer", and "X-Forwarded-For", which represent the system and browser information of the user, the referer of the URL, and the URL disguise. If you select "Custom", "Parameter" and "Value" are required. The names and values are case-insensitive. Chinese characters not allowed.
Timeout period (ms) per try		This is required. Enter a value between 500 and 3000. The default is 3000.
Max retries		Enter a value between 0 and 3. The default is 1.

Behavior upon timeout	The default is "Approve". You can also set it to "Reject". Whether to approve or reject a request if the system does not receive a response (HTTP status code 200 or 403) after the total timeout period elapses (Total timeout period = Timeout period per try x (Max retries + 1)).
Asynchronous Authentication	Asynchronous authentication is disabled by default. You may enable this feature manually based on your specific business requirements. Once enabled, playback will commence without waiting for the remote authentication result, allowing for immediate content viewing. If the remote authentication subsequently fail, the playback will be disconnected. This approach avoids the issue of increased initial screen load time due to the latency of remote authentication. In the asynchronous authentication mode, the authentication for ts and m3u8 files in the HLS protocol will not be effective, and synchronous authentication will continue to be maintained.

4. Click **Save**.

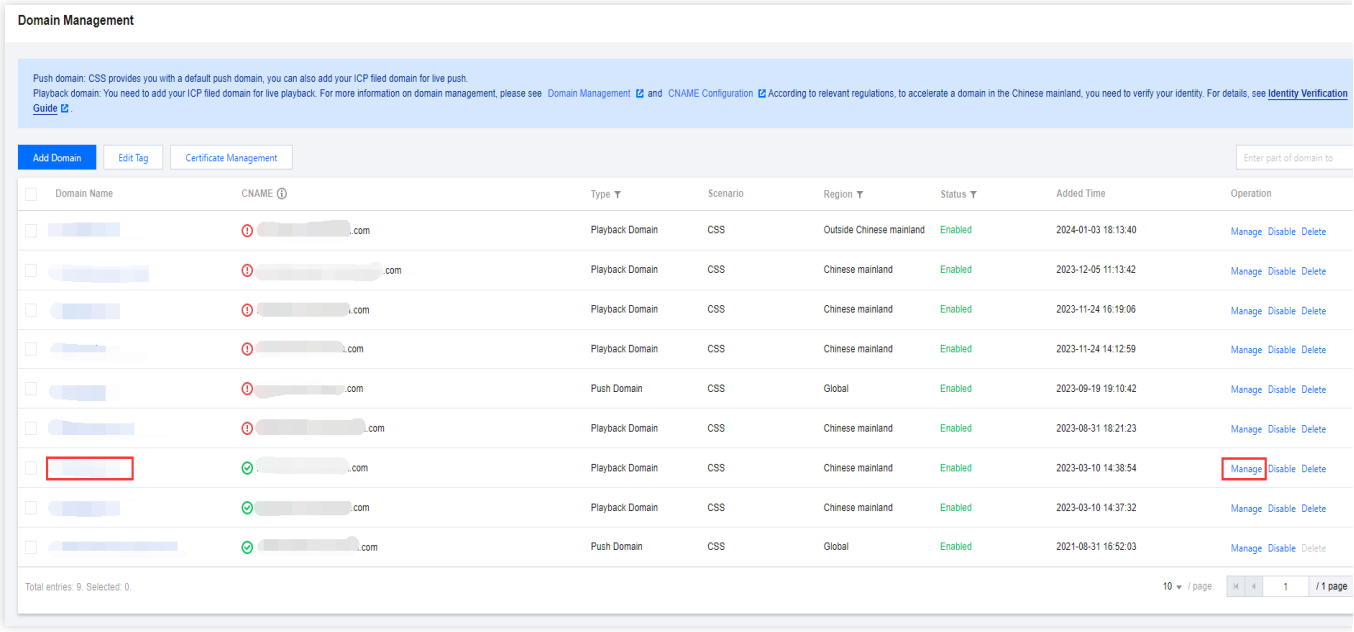
Note:

After configuring the remote authentication feature, it will take approximately 10 minutes to become effective. We appreciate your patience during this time.

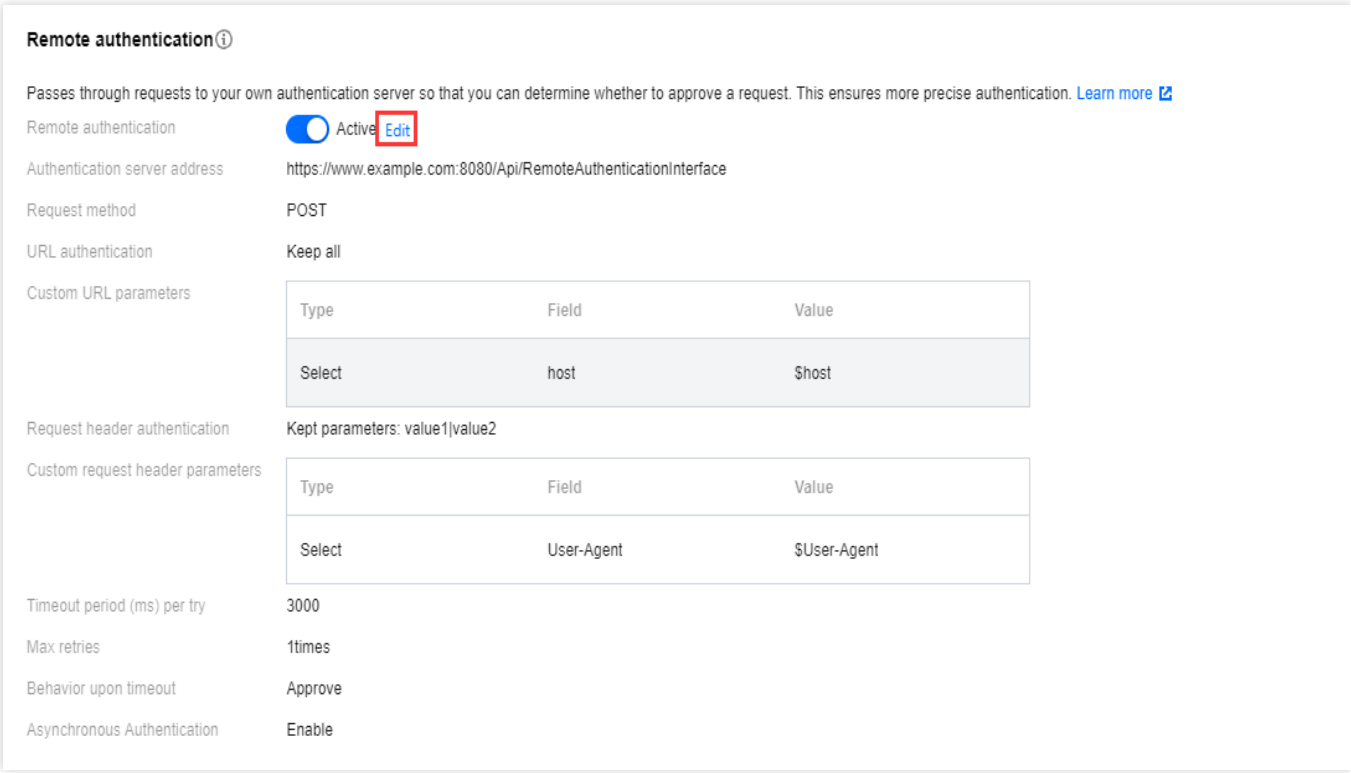


Modifying Remote Authentication Settings

1. Select Domain Management on the left sidebar. Click the name of the target playback domain or click **Manage** on the right to enter the domain management page.

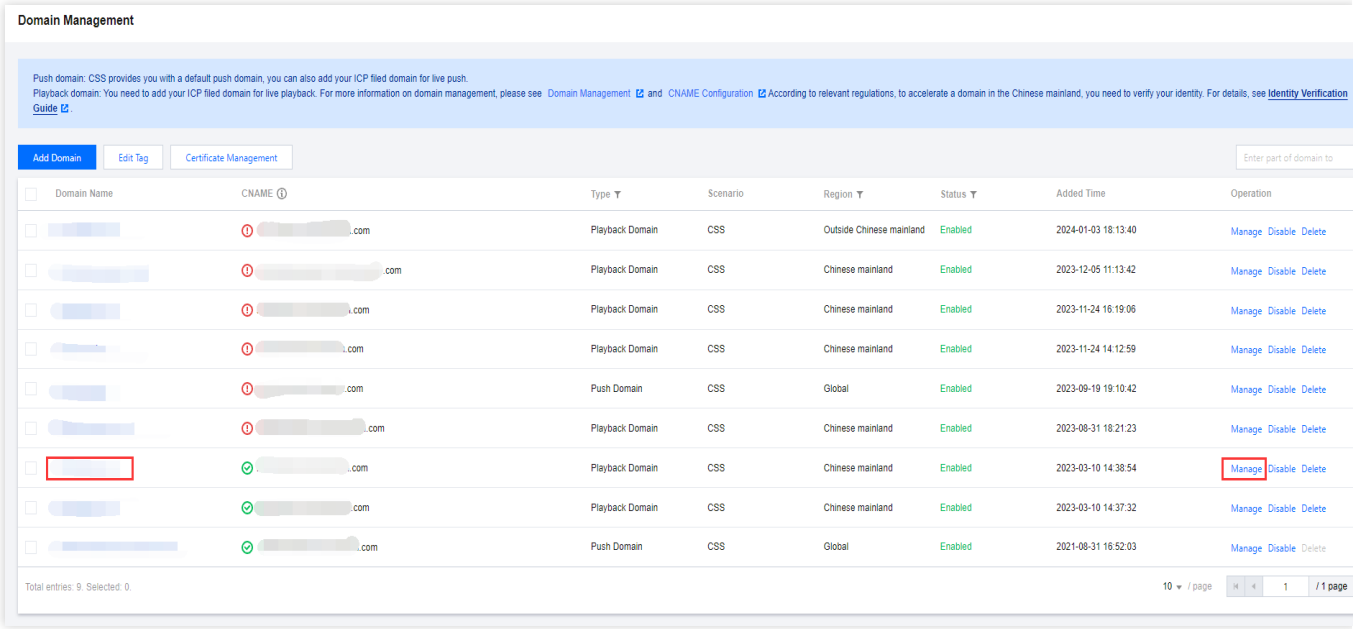


2. Under the **Access Control** tab, find **Remote authentication** and click **Edit**.
3. Modify the settings and click **Save**.



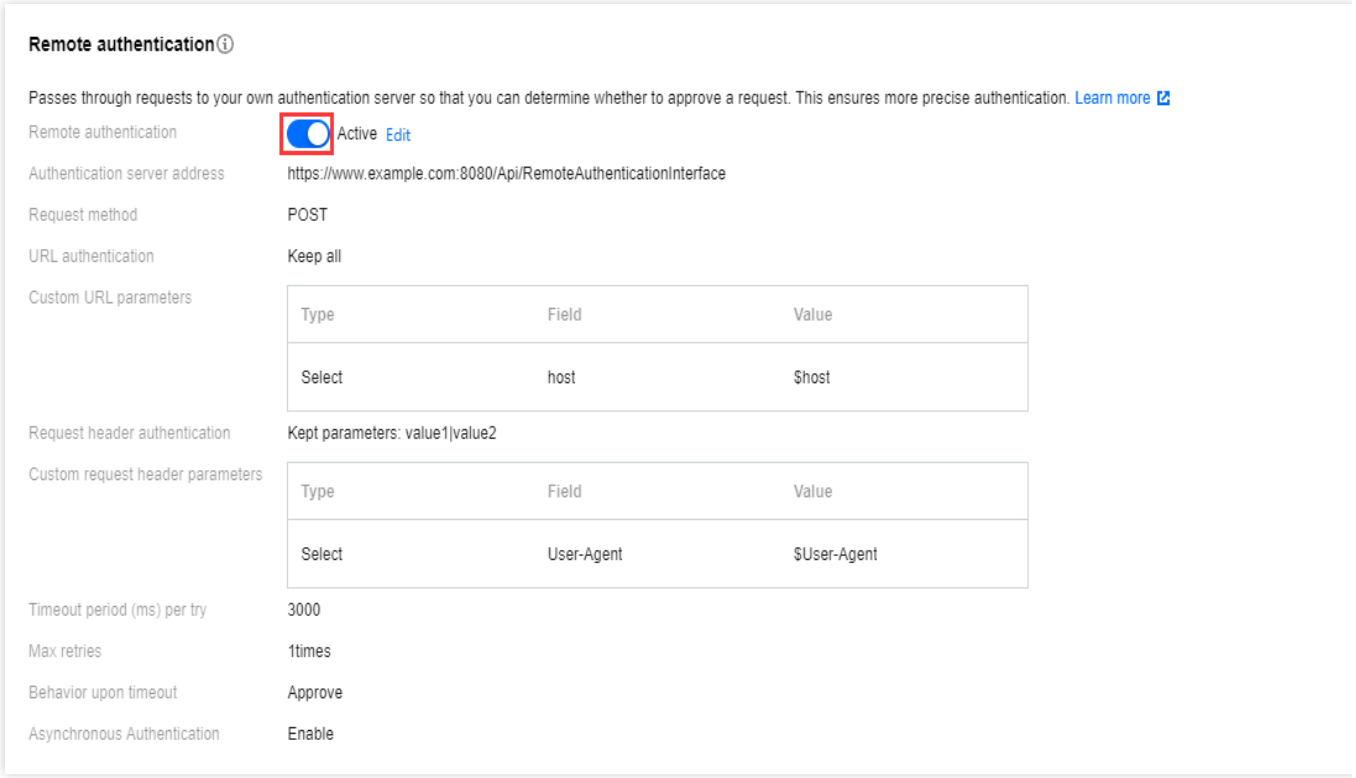
Disabling Remote Authentication

1. Select Domain Management on the left sidebar. Click the name of the target playback domain or click **Manage** on the right to enter the domain management page.

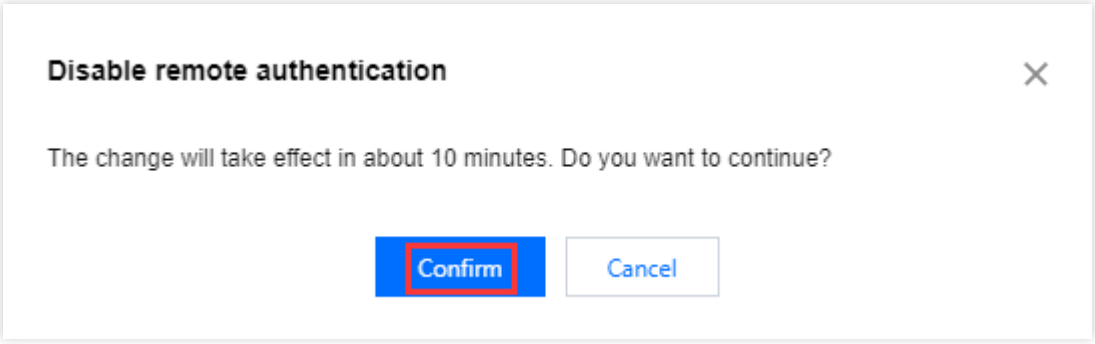


2. Under the **Access Control** tab, find **Remote authentication**, and click

to disable remote authentication.



3. To disable the remote authentication configuration, it is expected to take effect in about 10 minutes. Click **Confirm**.


Disable remote authentication
The change will take effect in about 10 minutes. Do you want to continue?
Confirm
Cancel

UA Blocklist/Allowlist Configuration

Last updated：2025-05-16 11:31:10

Cloud Streaming Services (CSS) supports access control by configuring User-Agent blacklist and whitelist rules. This method makes rule judgment based on the User-Agent information in the user's HTTP request header to allow or deny user access as needed.

How It Works

Configure **UA allowlist**: Only the configured UA content can access the current live broadcast content.
Configure **UA blocklist:** Only the configured UA content cannot access the current live broadcast content.

Must-Knows

Turn on/off UA Blocklist/Allowlist, it is expected to take effect in 15-20 minutes.
If UA authentication and other authentication methods are configured at the same time, the priority order is: Protocol > IP > Region > UA. The system will first authenticate according to the protocol, then IP, region, and finally UA.

Prerequisites

You have activated CSS and logged in to the CSS console.
You have added a playback domain.

Enabling UA Blocklist/Allowlist

1. Select Domain Management, click the **Playback Domain** that requires UA Blocklist/Allowlist configuration or the **Manage** on the right, and enter the Domain Management page.

2. Within the **Access Control** > **UA Blocklist/Allowlist**, click on

to enable the UA Blocklist/Allowlist.

3. After enabling the **UA blocklist/allowlist**, enter the **UA blocklist/allowlist**, configuration page and perform the following configuration:

Blocklist

Allowlist

Configuration Item	Description
Authenticate By	Allowlist or blocklist: You cannot select both.
Empty UA	The empty User-Agent function is turned off by default and can be turned on manually. After empty User-Agent is enabled: In the blocklist scenario, requests are allowed if the UA value is empty or the UA field does not exist. In the allowlist scenario, requests are rejected if the UA value is empty, and requests are allowed if the UA field does not exist.
Authentication Content	Wildcards * and multiple values are supported, with one value per line. For multiple values, fill in each value on a separate line. English semicolons (;) are not supported. For example: curl* *IE* *Chrome* *Firefox* It is case-sensitive, supporting up to 100 characters.

4. Click **Confirm** to save the configuration.

Note:

The UA blocklist/allowlist will take effect in about 10 minutes after configuration. Please wait.

Modifying an UA Blocklist/Allowlist

1. Select Domain Management on the left sidebar, and click the target **playback domain** or click **Manage** on the right to enter the domain management page.

2. Click Access Control and, in the **UA Blocklist/Allowlist** area, click **Edit.**

3. Modify the configuration and click **Confirm**.

Disabling UA Blocklist/Allowlist

Follow the steps below to disable UA Blocklist/Allowlist:
1. Select Domain Management on the left sidebar, and click the target **playback domain** or click **Manage** on the right to enter the domain management page.

2. Select the **Access Control** tab. In the **UA Blocklist/Allowlist** area, click

to disable UA Blocklist/Allowlist.

3. When closing UA Blocklist/Allowlist, the system will pop up a confirmation window. Click **Confirm** to turn off the feature. Please note that it is expected to take 15-20 minutes after shutdown to take effect.

Certificate Management

Last updated：2025-04-29 14:26:19

Normally, live streaming domain names use the Hypertext Transfer Protocol (HTTP). HTTP can be converted to Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) using SSL/TLS protocol for encrypted data transmission. You can go to **Certificate Management** to query and configure SSL certificates for domain names.

How to Configure

The purpose of configuring an SSL certificate for a domain name is to encrypt key user data for secure transmission. A Secure Sockets Layer (SSL) certificate allows a site to switch from HTTP (HyperText Transfer Protocol) to its SSL-based encrypted version HTTPS (HyperText Transfer Protocol over Secure Socket Layer). Currently, only the playback domain name supports the configuration of SSL certificates.

Configuring Certificate

1. Go to Domain Management in the CSS console, and click **Certificate Management** to go to the certificate management page.

2. Click **Configure Certificate** to add a certificate configuration.

3. In the certificate configuration pop-up window, select a certificate source:
Self-owned certificate: enter remarks, content, and key of this certificate. After the configuration is saved, the certificate info will be synced to Certificate Management in the SSL Certificate Service console. For details about how to set the certificate content and key, please see HTTPS Configuration.

Tencent Cloud-hosted certificate: select a certificate you purchased in the SSL Certificate Service console.

4. After the certificate is confirmed to be available, click **Next** to enter the domain name configuration page.
5. In **Bind Domain Names**, select one or more playback domain names which match the certificate. If a selected domain name is already bound to a certificate, the new certificate will apply.
6. In **Selected**, you can view selected domain names and whether their HTTPS configuration is enabled.

7. Choose whether to enable HTTPS Configuration for selected domain names:

Note:

Toggling **Enable HTTPS Configuration** on will enable HTTPS configuration for the domain names.

Enable HTTPS Configuration is enabled by default. If you toggle this button off, the HTTPS configuration status of the domain names will not change after binding, with only their certificate updated.

8. Click **Confirm**.

Viewing Certificate Configuration

After you configure a certificate, you can go to Certificate Management to view its configuration, including the domain name, remarks, source, HTTPS configuration, and expiration time.

Updating Certificate Configuration

1. Go to Certificate Management, find the target certificate configuration in the list, and click **Update** on its right.

2. On the certificate configuration page, configure the certificate again.
3. Click **Confirm**.

Deleting Certificate Configuration

1. Go to Certificate Management, find the target certificate configuration in the list, and click **Delete** on its right.

2. In the confirmation pop-up window, click **Confirm**.

Note:

After you unbind the certificate, the domain names cannot use HTTPS configuration.

Stream Management

Last updated：2024-07-16 09:36:23

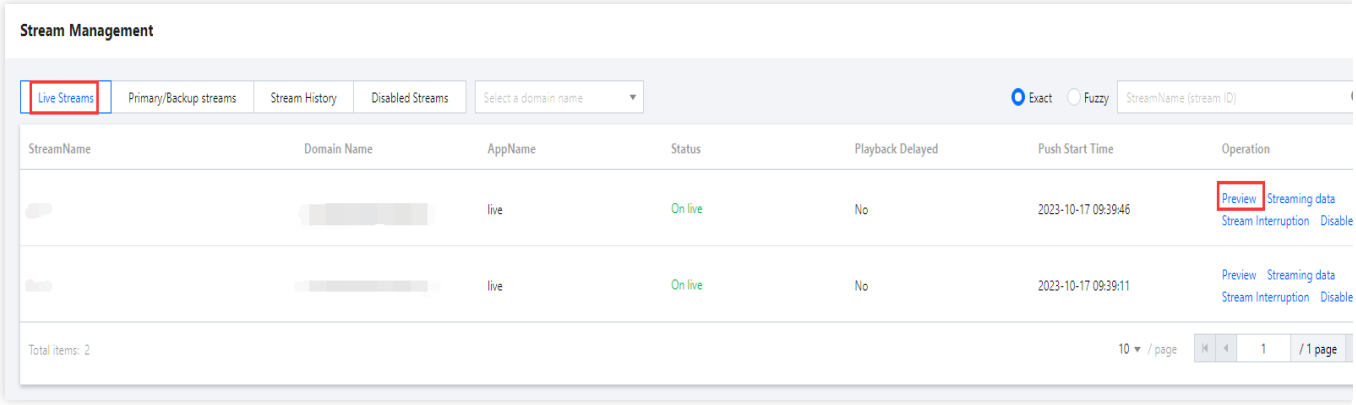
Log in to the CSS console and enter Stream Management. Stream Management includes interrupting live streams and disabling live streams, as well as viewing **Live Streams**, **Primary/Backup Streams**, **Stream History**, **Disabled Streams**, and their detailed information. Here is a brief introduction and usage of these features:

Live Streams Management

Log in to the CSS console, then navigate to Stream Management > **Live Streams**, and perform operations according to your actual business needs.

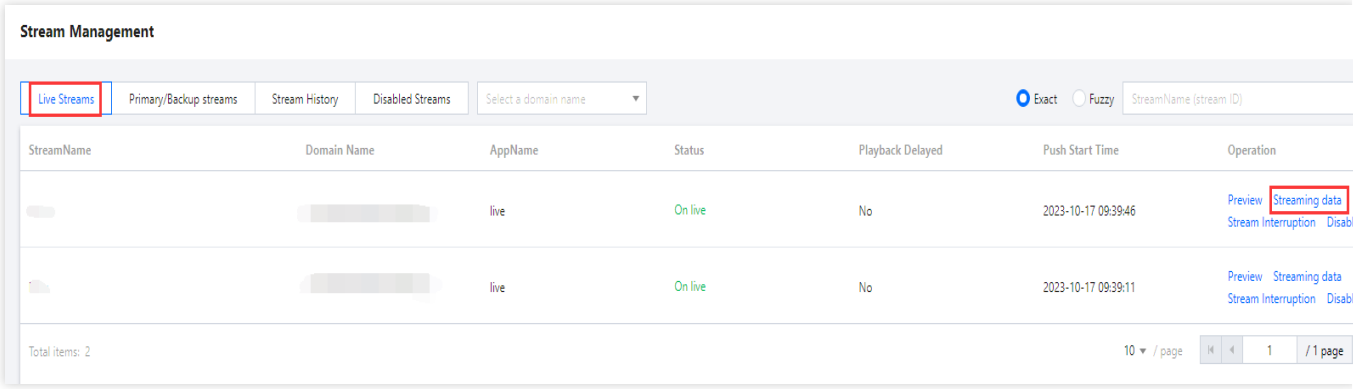
Preview live stream

In the Live Streams list, you can select the domain and corresponding online stream you want to query. Click "Preview" on the right to view the real-time live streaming image.



View stream data

Click on the **stream data** on the right side to view detailed information of the online live stream, such as traffic, bandwidth, frame rate, bitrate, etc.

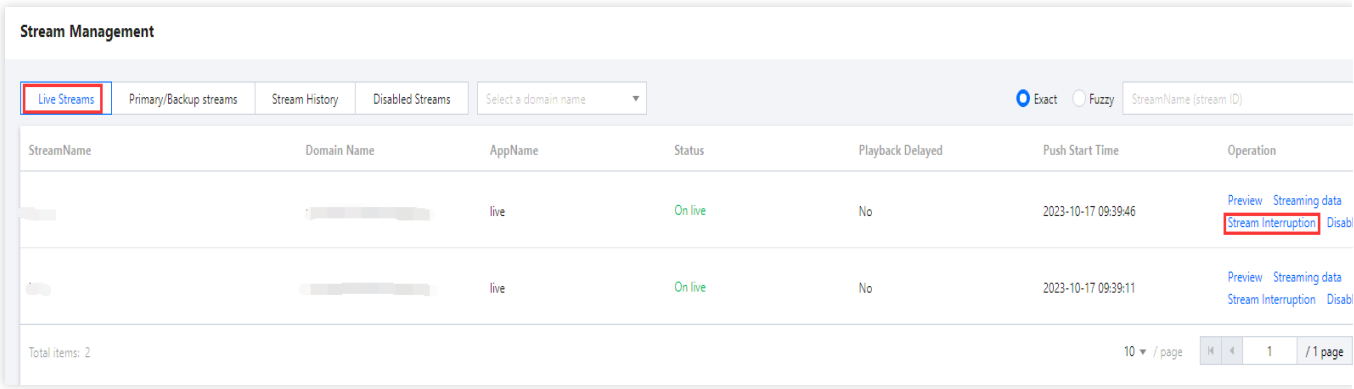


Interrupt live stream

Click **Stream Interruption** on the right to interrupt the current live stream publishing.

Note:

After the interruption, the current live stream will stop publishing. You can resume the live stream by republishing with the same Stream Name.

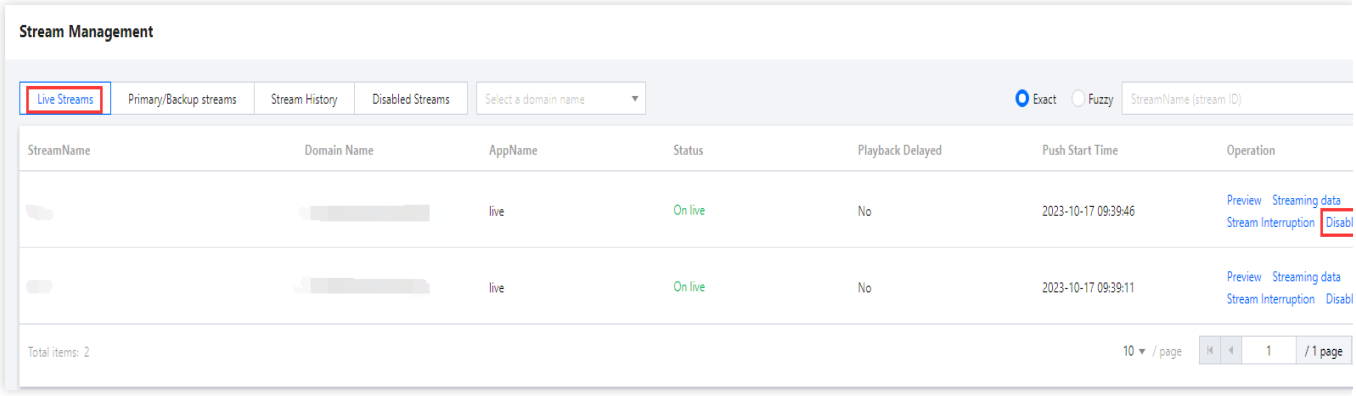


Disable live stream

Click **Disable** to disable the live stream.

Note:

After disabling, the current live stream will stop publishing (republishing is not possible for the current Stream Name until it is re-enabled). You can manually resume it or it will be automatically enabled after 7 days by default.



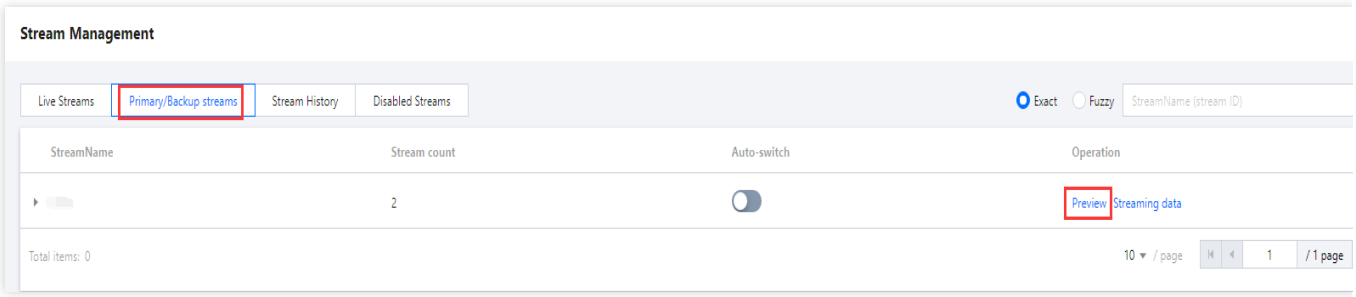
Primary and backup stream management

The primary and backup stream feature refers to the system's ability to automatically merge and output two live streams with the same **Stream ID**. The primary stream's content is prioritized for playback. If there are issues with the primary stream's content, you can **automatically** or **manually** switch to the backup stream content to ensure the stability of the live image. The primary and backup streams can be enabled or disabled for optimal scheduling. When optimal scheduling is enabled, the system will dynamically evaluate the quality of each stream and select the highest-quality stream as the primary stream.

Log in to the CSS console, then navigate to Stream Management > **Primary/Backup streams**, and perform operations according to your actual business needs.

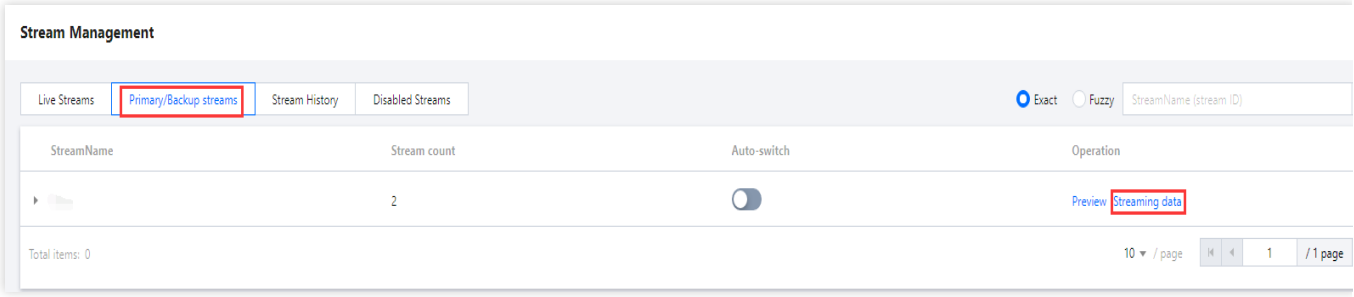
Preview live stream

Click **Preview** on the right to view the real-time live streaming image.



View stream data

Click on the **stream data** on the right side to view detailed information of the online live stream, such as traffic, bandwidth, frame rate, bitrate, etc.

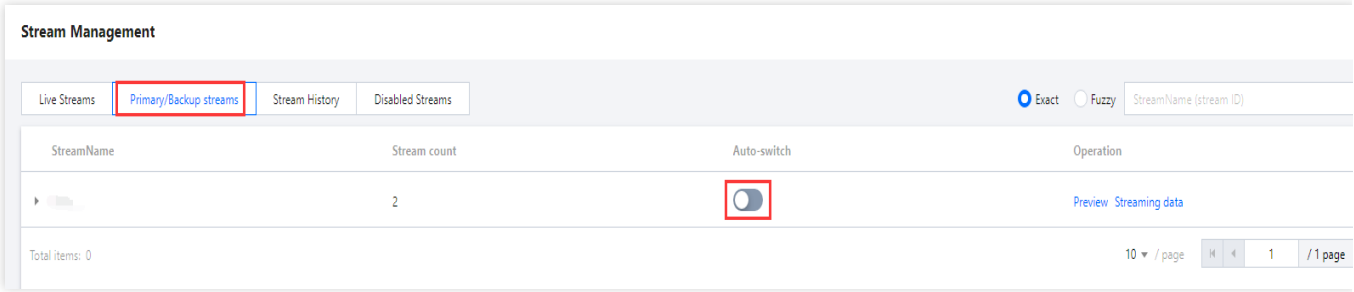


Optimal Scheduling Management

Enable optimal scheduling

Click

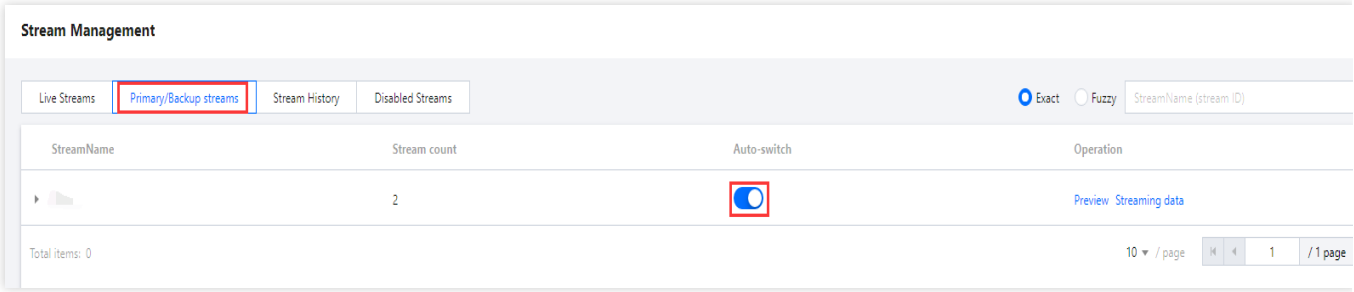
, to enable optimal scheduling. When optimal scheduling is enabled, the system will dynamically evaluate the quality of each stream and select the highest-quality stream as the primary stream.



Disable Optimal Scheduling

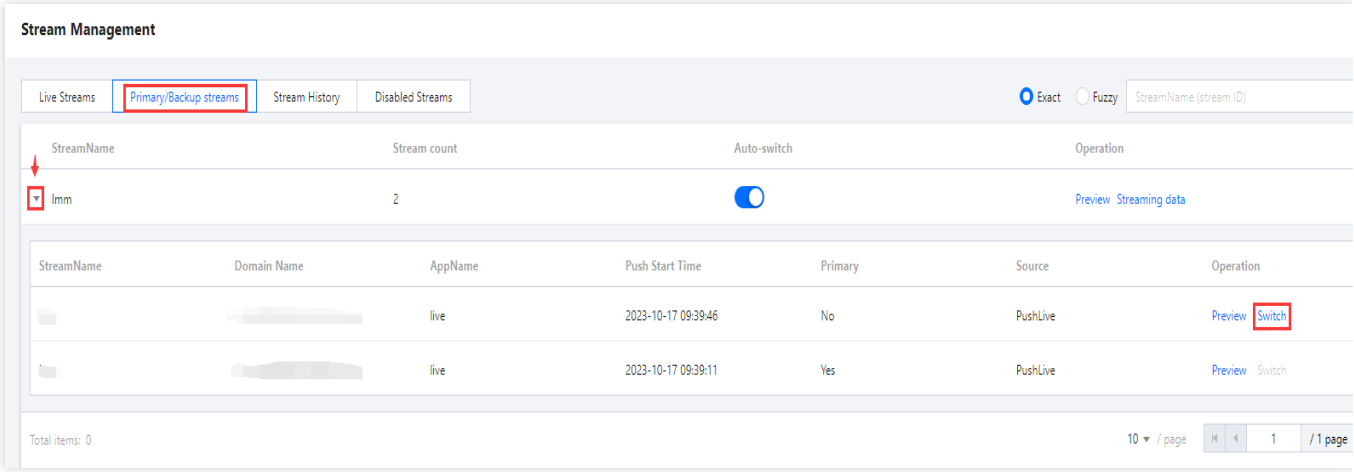
Click

, to disable optimal scheduling.



Primary and Backup Stream Switching

Click on the left-pointing triangle to expand the manual switch to the standby option.
Click the **Switch** on the right side to switch between the main and backup streams. By manually switching the main and backup streams, you can flexibly deal with issues that may arise during the live broadcast.



Stream History Management

Log in to the CSS console, then navigate to Stream Management > **Stream History**, You can query historical live stream data and perform operations according to your actual business needs.

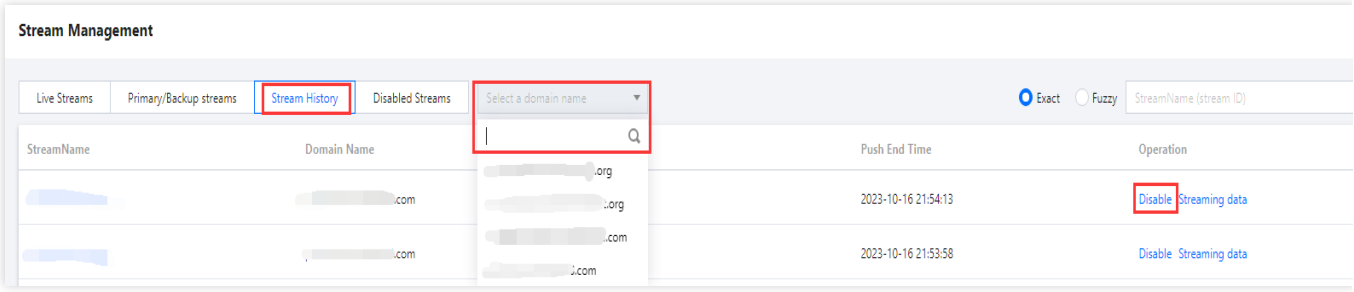
Disable Historical Live Stream

In the historical stream list, you can select the domain name to be queried and the corresponding historical live stream. Click **Disable** to disable the historical live stream.

Note:

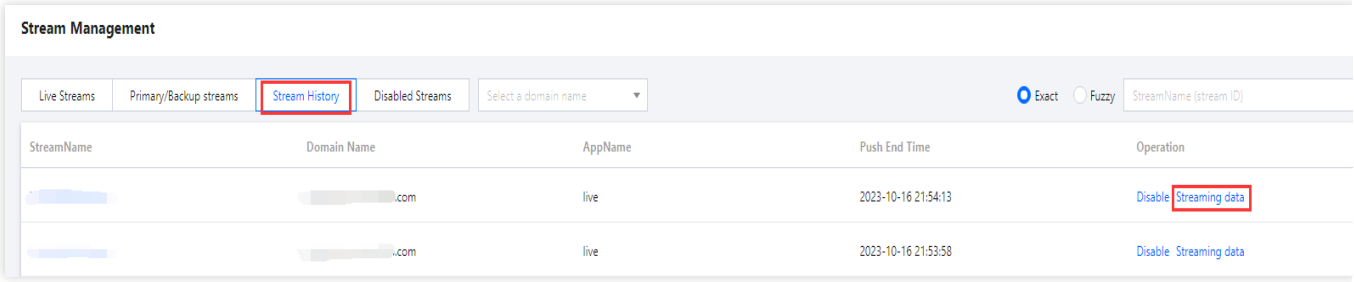
After being disabled, the current live broadcast will stop pushing (streaming cannot be re-pushed until the current StreamName is restored). It can be manually restored or automatically enabled after 7 days by default.

You can view stream history in the past 7 days under the **Stream History** tab or query records in the past month in Stream Interruption Records.



View stream data

Click on the **stream data** on the right side to view detailed information of the online live stream, such as traffic, bandwidth, frame rate, bitrate, etc.

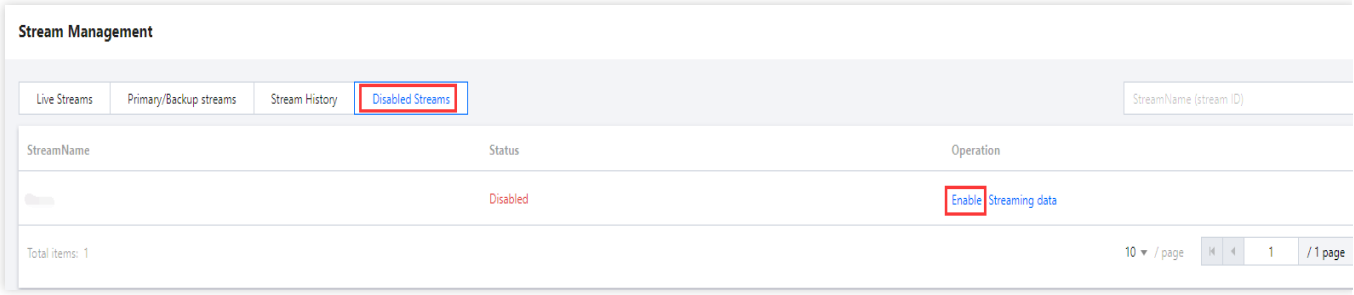


Disabled Streams Management

Log in to the CSS console, then navigate to Stream Management >**Disabled Streams**, and perform operations according to your actual business needs.

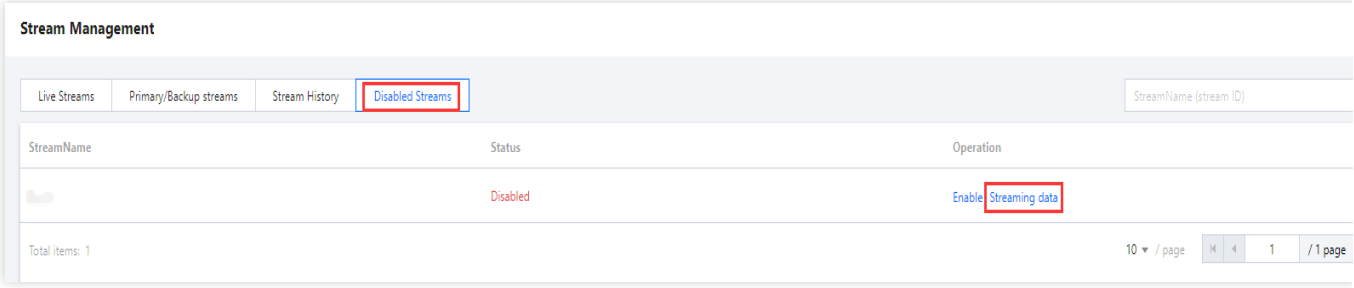
Enable live streaming

In the Disabled Streams list, select the corresponding disabled live stream and click **Enable** to resume the live stream publishing.



View stream data

Click on the **stream data** on the right side to view detailed information of the online live stream, such as traffic, bandwidth, frame rate, bitrate, etc.



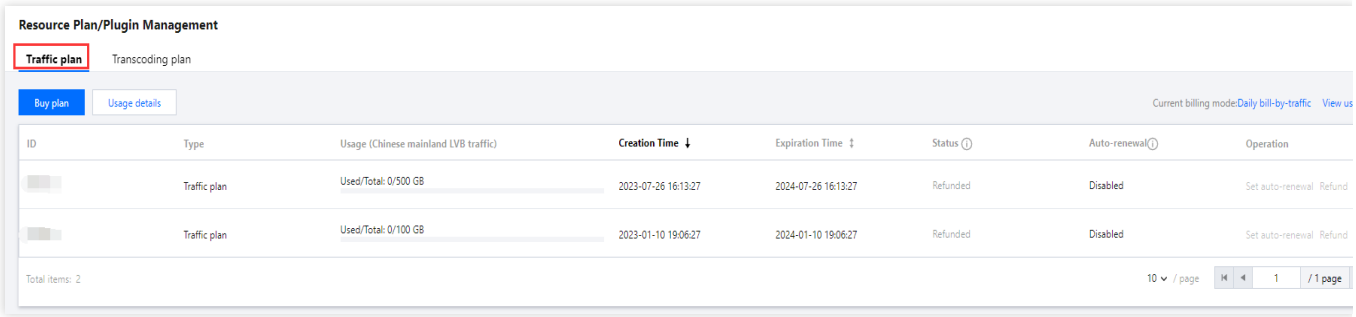
Package Management

Last updated：2024-08-27 10:51:52

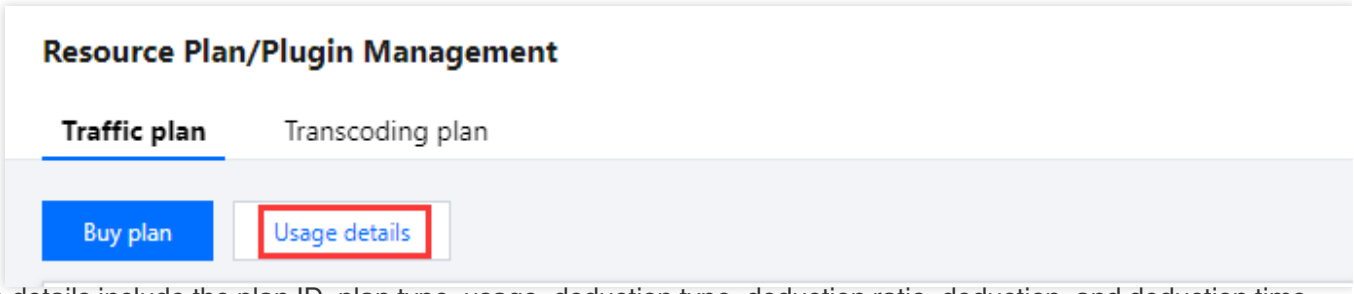
You can view the usage of your traffic and transcoding plan in the CSS console.

Traffic plan

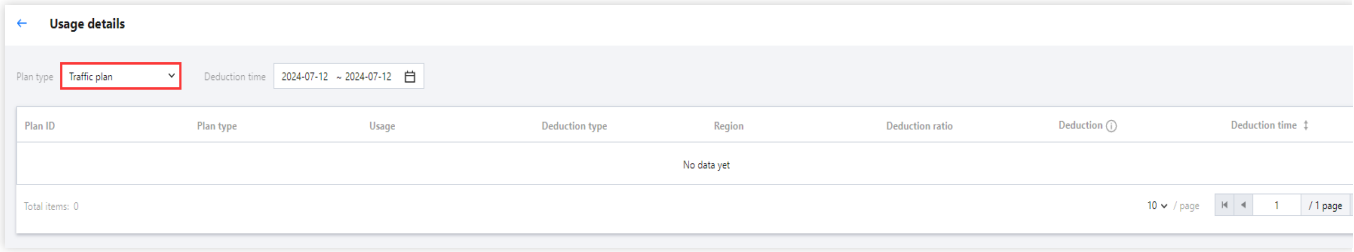
Select plan on the left sidebar. You can do the following under the **Traffic plan** tab:
Supports viewing the usage, purchase time, expiration time, and status of the **traffic plan** purchased.
The plan status includes unused, in use, used up, expired, and frozen. Auto-renewal status includes disabled, renewal succeeded, renewal failed, auto-renewal enabled, and unsupported. If the renewal fails, the system will prompt the reason for the failure, such as "insufficient account balance".



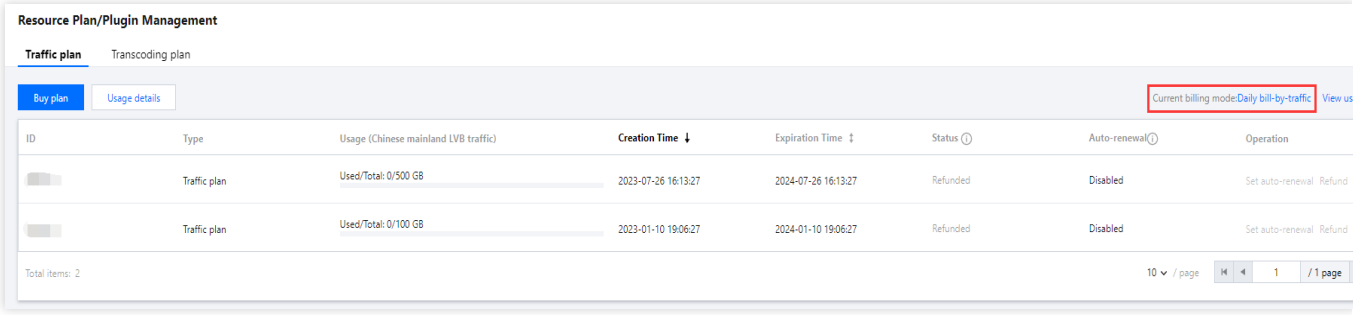
Click **Usage details** to view the deduction details for the usage of the **traffic plan** purchased.



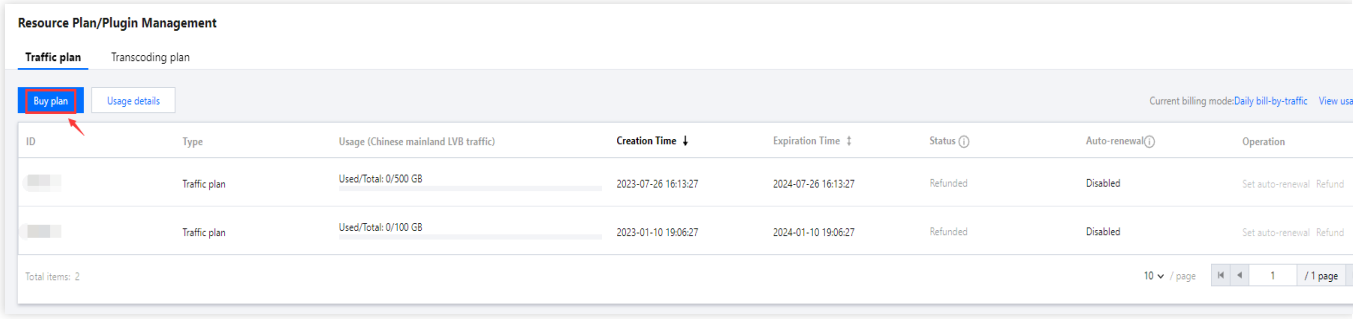
Usage details include the plan ID, plan type, usage, deduction type, deduction ratio, deduction, and deduction time.
The usage of the traffic plan will be updated when the bill is generated the next day (the exact billing time may vary).
For the deduction rules of the traffic plan, see the Prepaid plan.



View your **current billing mode** in the top right corner. Traffic plan can be used for deduction only in **daily bill-by-traffic** mode. If you use other modes, your plan will be frozen and their validity will not be extended.



Click **Buy plan** to go to the purchase page to buy traffic plan.



Note:

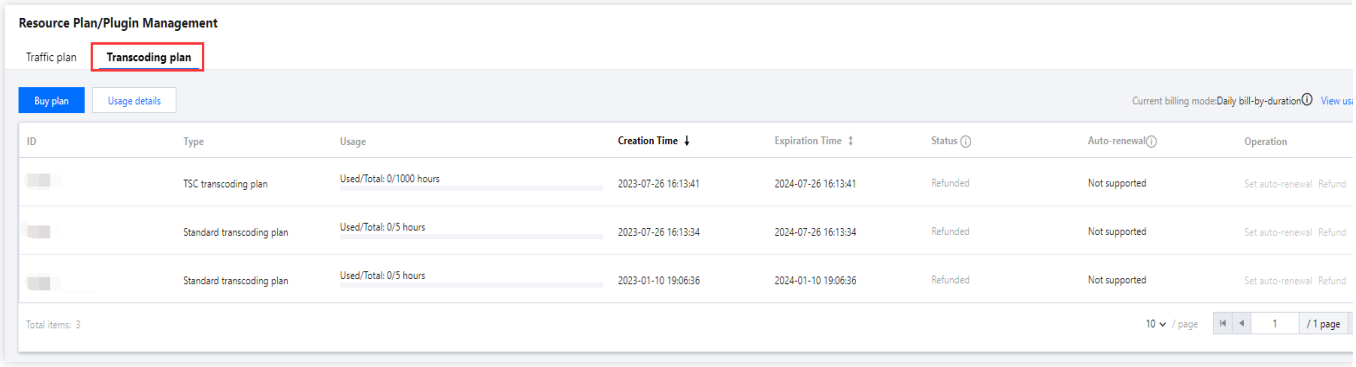
Before you buy a plan, please read Traffic plan to learn about the **billing details** and **limits**.

You can refund a plan in the console if it meets the requirements of our refund policy.

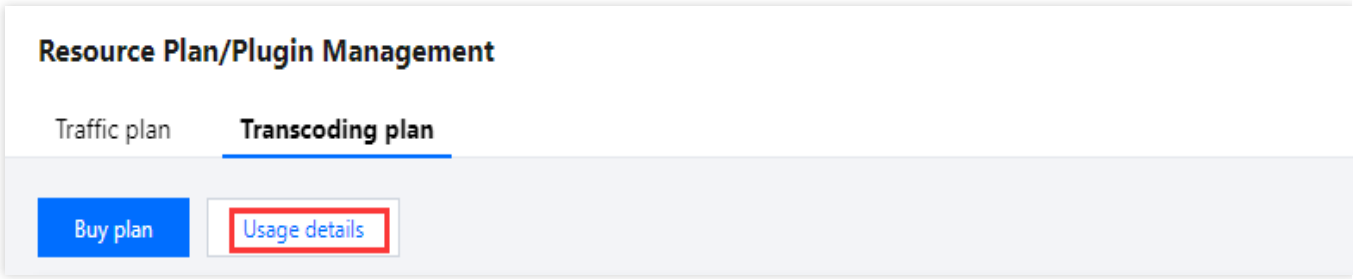
Transcoding plan

Select plan on the left sidebar. You can do the following under the **Transcoding plan** tab:

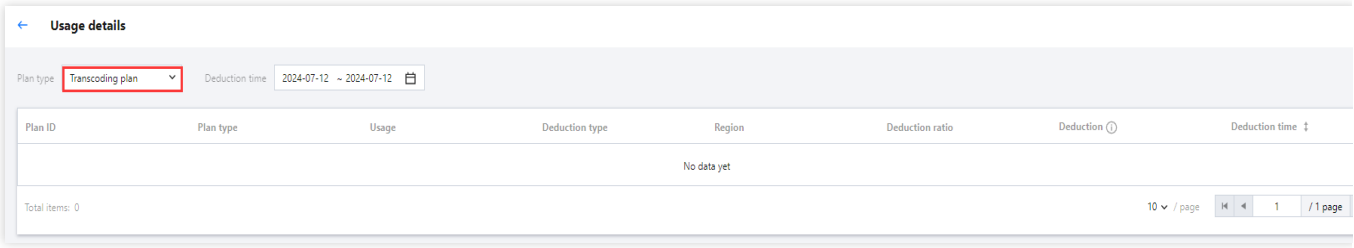
View the usage, purchase time, expiration time, and status of **standard transcoding plan** and **TSC transcoding plan**.



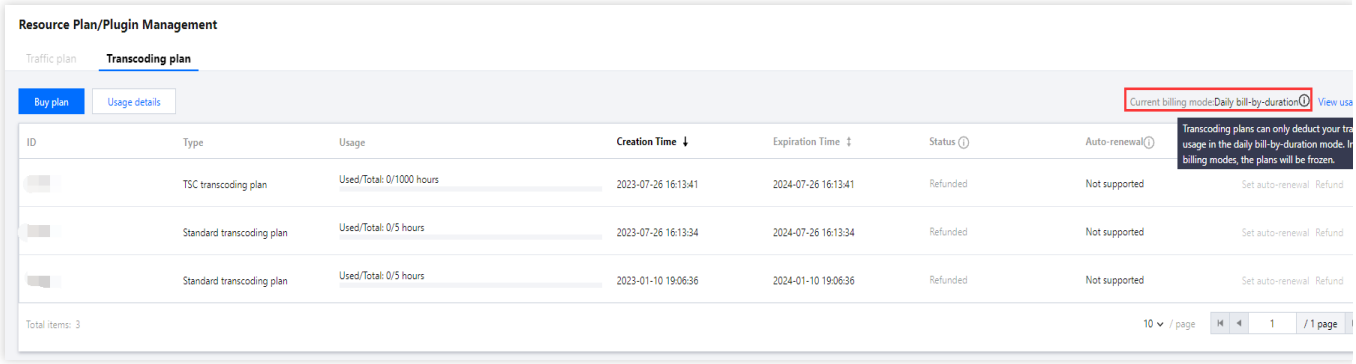
Click **Usage details** to view the deduction details for the usage of the **standard transcoding plan** and the **TSC transcoding plan** purchased.



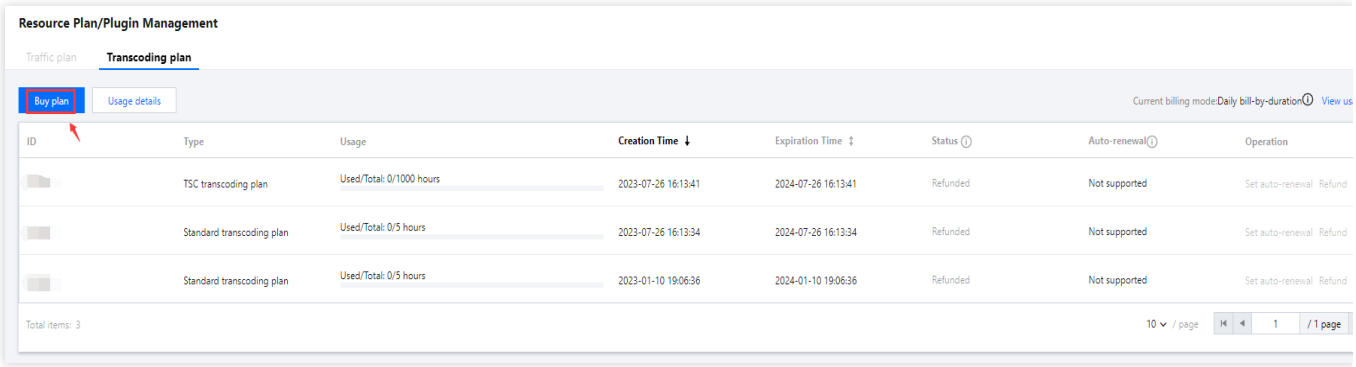
Usage details include the plan ID, plan type, usage, deduction type, deduction ratio, deduction, and deduction time. **The usage of the transcoding plan will be updated when the bill is generated the next day (the exact billing time may vary).**



View your **current billing mode** in the top right corner. Transcoding plan can be used for deduction only in **daily bill-by-traffic** mode. If you use other modes, your plan will be frozen and their validity will not be extended.



Click **Buy plan** to go to the purchase page to buy transcoding plan.



Note:

Before you buy a plan, please read Standard Transcoding plan and TSC Transcoding plan to learn about the **billing details** and **limits**.

Feature Configuration
Live Watermarking

Last updated：2024-08-27 10:51:52

CSS supports the watermark feature. It adds watermarks to the live streaming screen to protect video content from theft. This document describes how to create, modify, bind, unbind, and delete a watermark template in the console.
You can create a watermark template in the following ways:
Create a watermark template in the CSS console. For more information, please see Creating Watermark Template.
Create a watermark template by calling an API. For more information, please see AddLiveWatermark.

Notes

After creating a template, you can bind it to a push domain name. The binding will take effect in 5–10 minutes.
The watermark templates are managed at the domain name level in the console, and rules created by APIs cannot be canceled there for the time being. If you bound the watermark configuration to a specified stream through the watermark management API and want to unbind them, you need to call the DeleteLiveWatermark API.
Binding, unbinding, and modifying a template affect only new live streams after the update but not ongoing ones. To make the new rule take effect for ongoing live streams, you need to interrupt them and push them again.

Prerequisites

You have activated the CSS service and added a push domain name.

Creating Watermark Template

1. Log in to the CSS console and select **Feature Configuration** > **Live Watermarking**.
2. Click **Create Watermark** to enter the watermark template creation page.
3. Enter a watermark name, which can contain up to 30 letters, digits, underscores (_), and hyphens (-).
4. Click **Select Image** to upload a watermark image. The size of the watermark image supports stretching to full window dimensions.

Note:

For the best visual effect, the watermark should be a transparent image in PNG format; the image size should be smaller than 2MB; the uploaded image file name should only support: English, numbers, and symbols - ! _ . *.

5. Set the watermark image preview window size:

Default width and height values: Width 1920px, Height 1080px.

Width and height value range: 360px - 4096px.

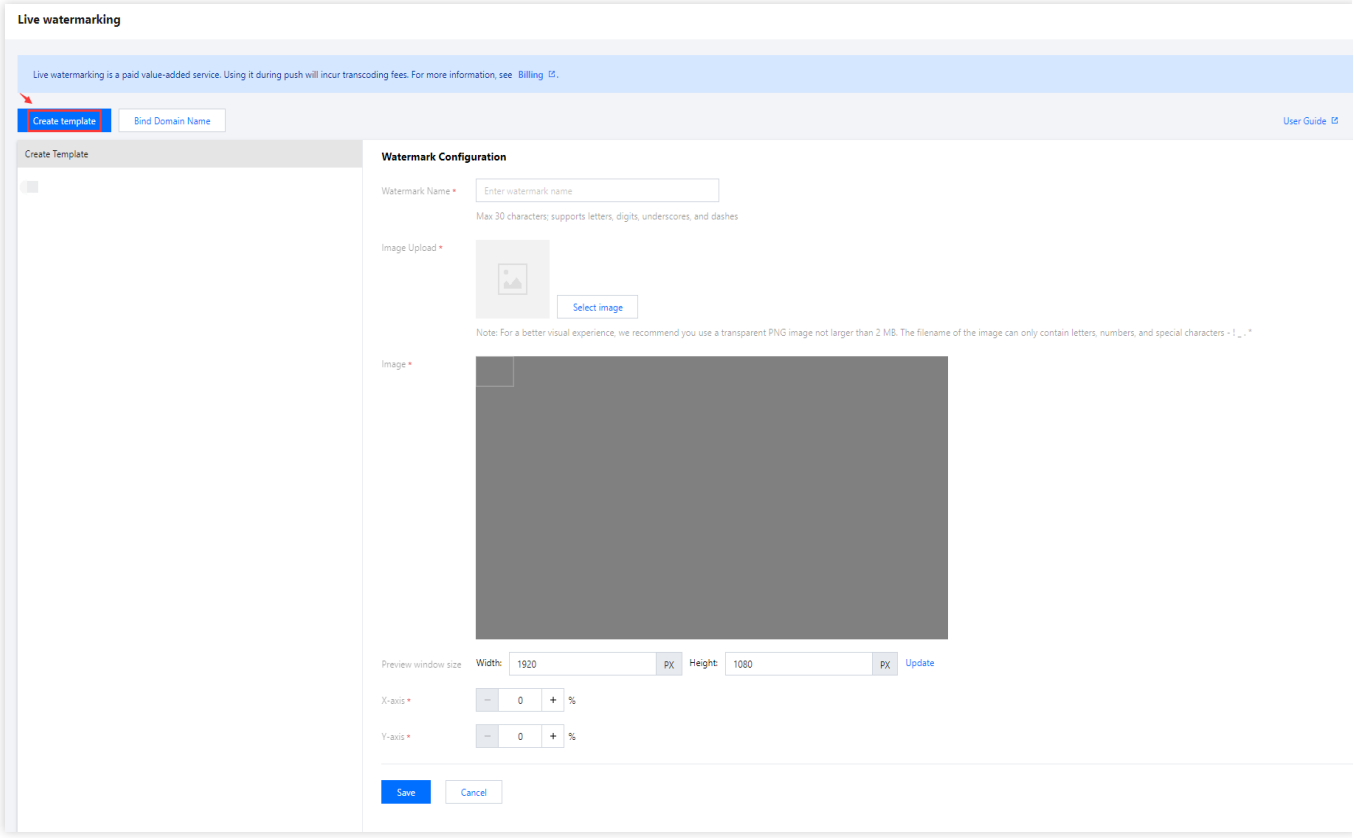
Clicking **Update** the right side will automatically validate and synchronize the update of the watermark image preview window.

6. Specify the watermark location in the following ways:

Drag the watermark image in the configuration pane.

Adjust the coordinates of the X axis and Y axis.

7. Click **Save**.

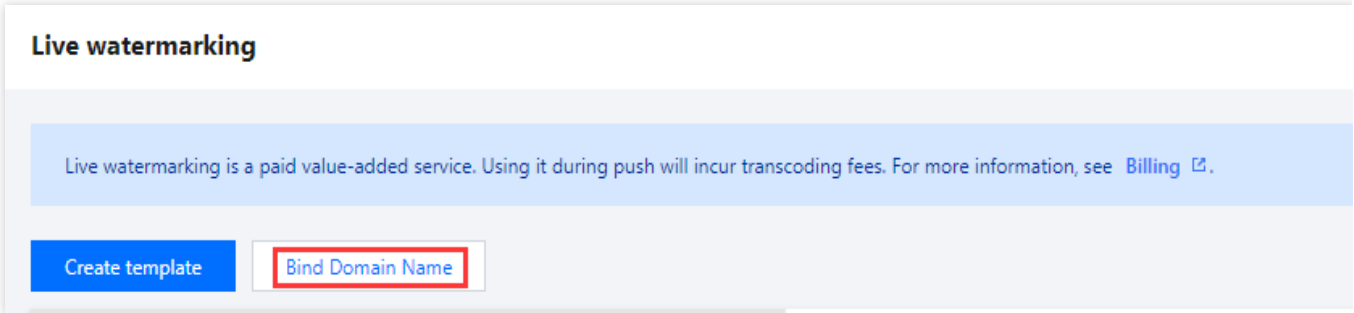


Binding Domain Name

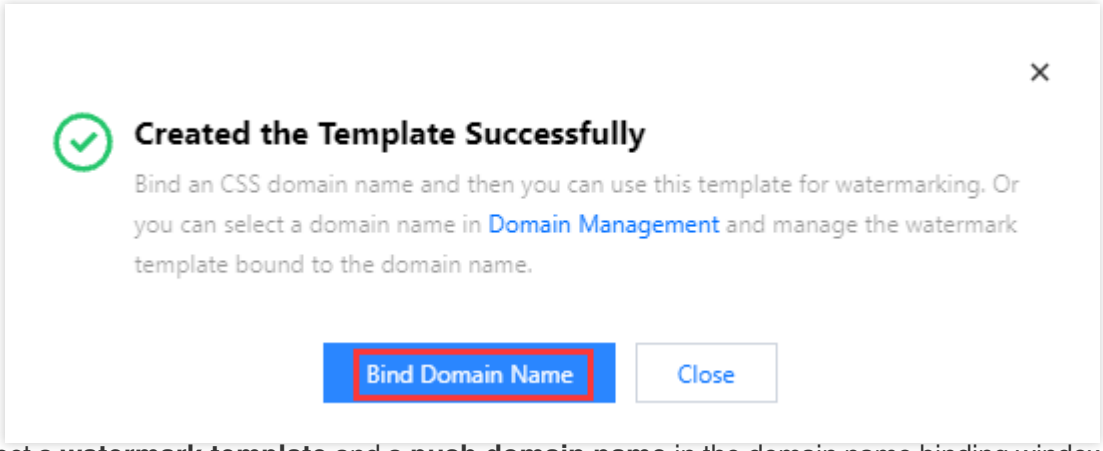
1. Log in to the CSS console and select **Feature Configuration** > Live Watermarking.

2. Enter the domain name binding page in either of the following ways:

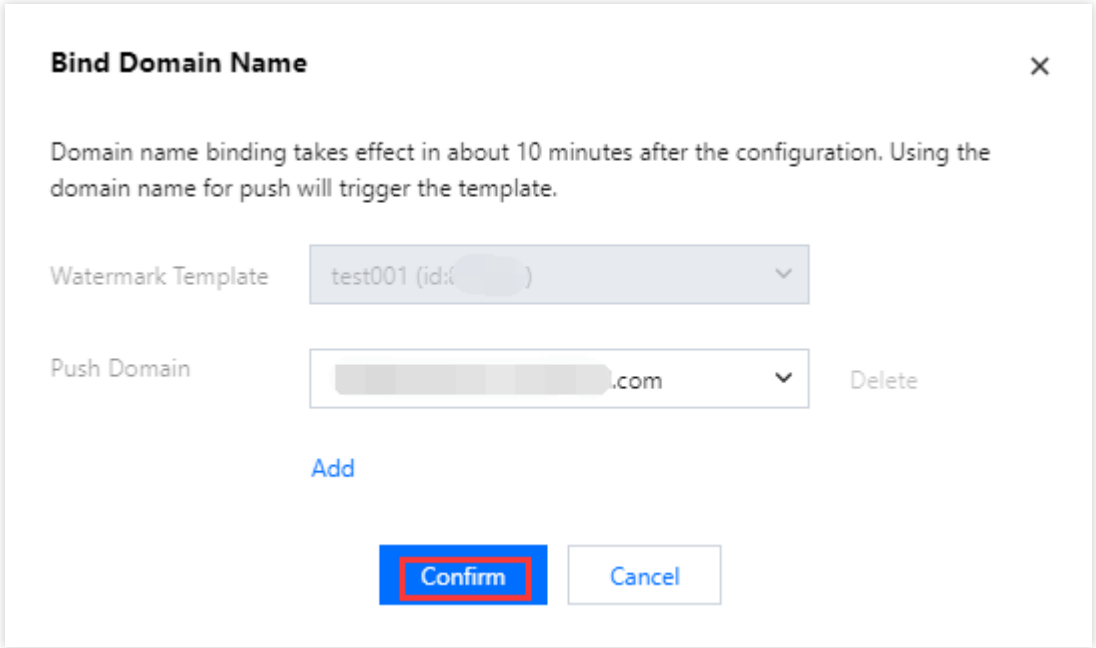
Directly bind a domain name: click **Bind Domain Name** in the top-left corner.



Bind a domain name after creating the watermark template: after the watermark template is created, click **Bind Domain Name** in the pop-up window.



3. Select a **watermark template** and a **push domain name** in the domain name binding window and then click **Confirm**.

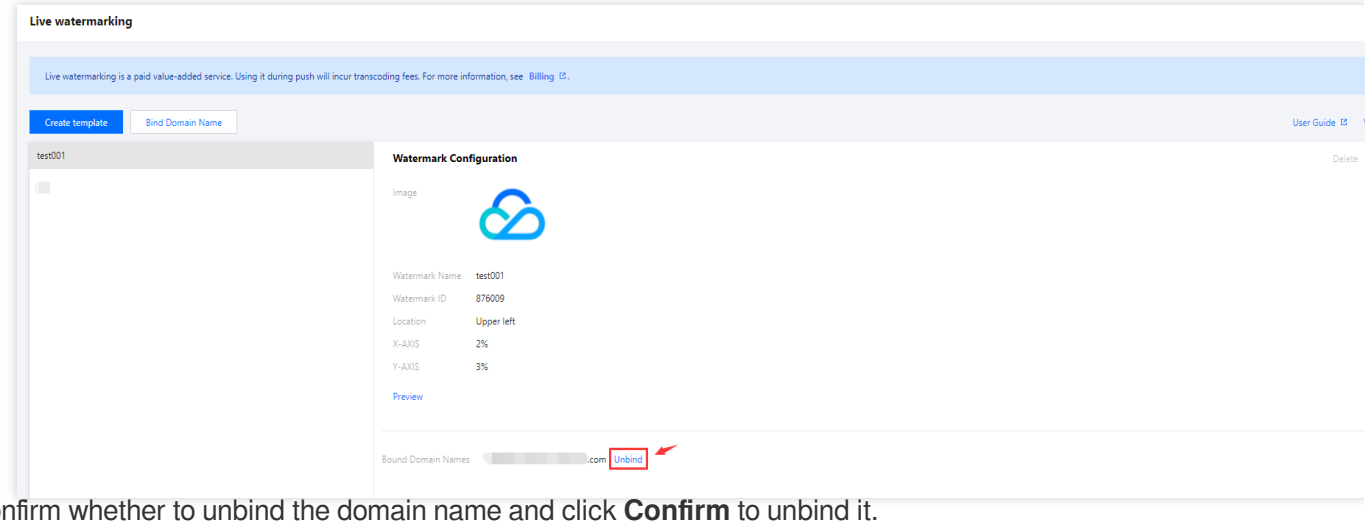


Note：

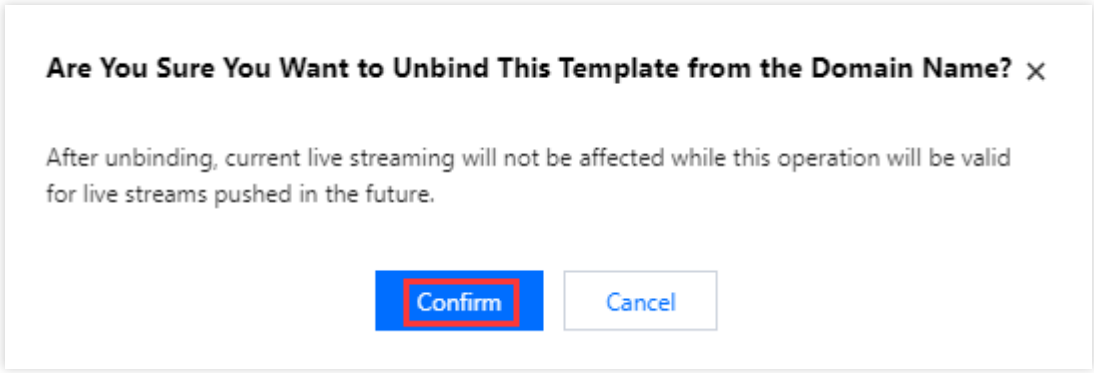
You can click **Add** to bind multiple push domain names to this template.

Unbinding

1. Log in to the CSS console and select **Feature Configuration** > Live Watermarking.
2. Select domain names bound to the watermark template and click **Unbind**.

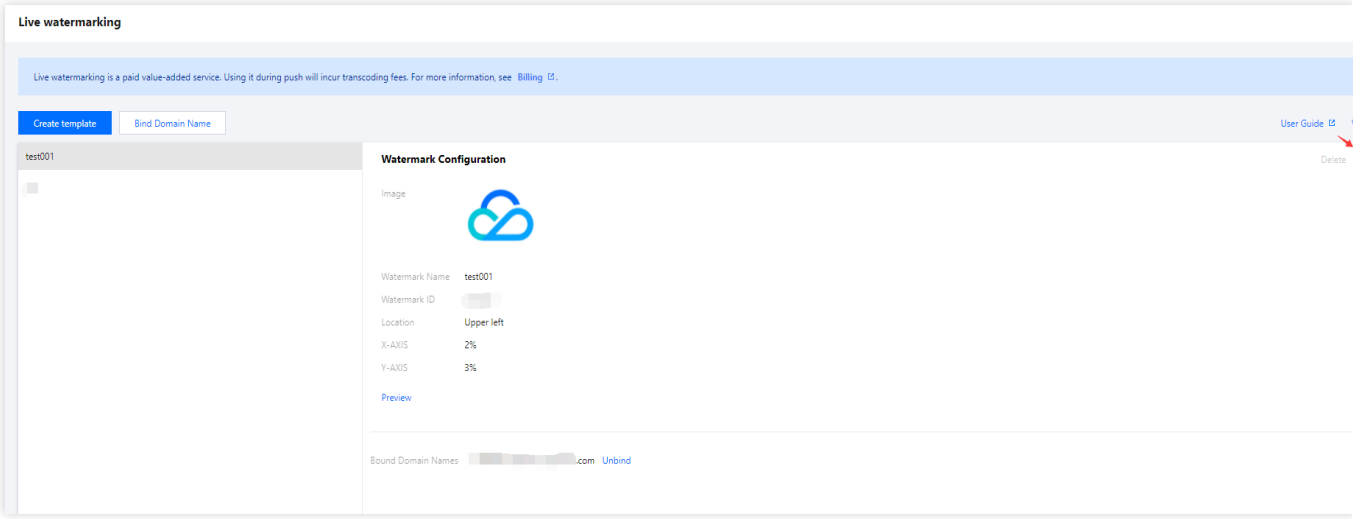


3. Confirm whether to unbind the domain name and click **Confirm** to unbind it.



Modifying Template

1. Go to **Feature Configuration** > **Live Watermarking**.
2. Select the target watermark template and click **Edit** on the right to modify the template information.
3. Click **Save**.



Note:

You can click **Preview** to view how the watermark will be displayed on the screen.

Deleting Template

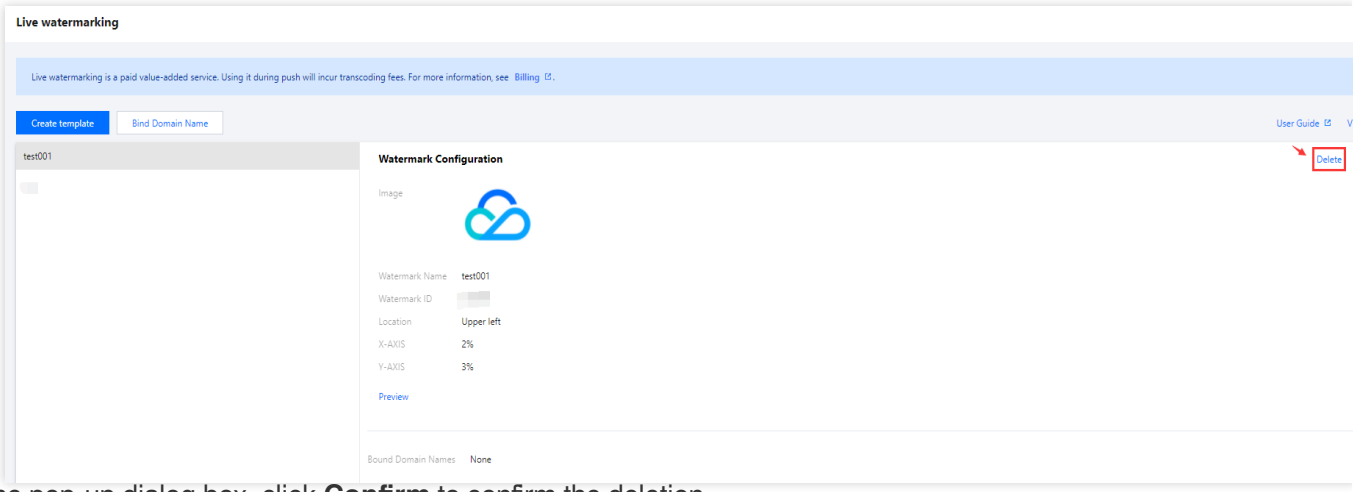
Note:

If the template is already associated, you need to Unbind it first before you can perform the delete operation.

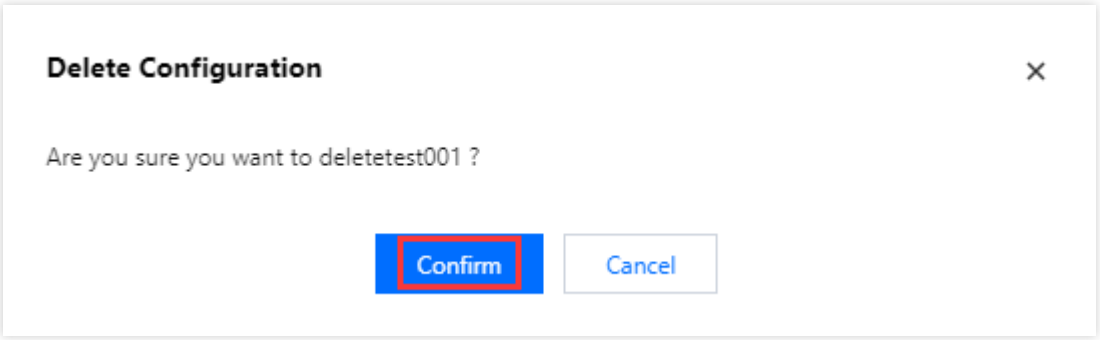
Once the template is deleted, it cannot be recovered. Please proceed with caution.

If a template has been bound to a domain name, you need to unbind the template before deleting it. For detailed directions, please see Unbinding.

1. Go to **Feature Configuration** > Live Watermarking.
2. Select the watermark template you have successfully created, and click **Delete** in the upper right corner.



3. In the pop-up dialog box, click **Confirm** to confirm the deletion.



Relevant Operations

For more information on how to **bind**/**unbind** a **domain name** to/from a watermark template, please see Watermark Configuration.

Live Transcoding

Last updated：2025-04-29 14:26:20

Live transcoding (including video transcoding and audio transcoding) refers to the process where the original stream pushed from the live streaming site is converted into streams of different codecs, resolutions, and bitrates in the cloud before being pushed to viewers. This meets playback needs in varying network environments on different devices.
This document describes how to create, bind, unbind, modify, and delete a transcoding template via the CSS console.
You can create a transcoding template in two ways:
Create a transcoding template in the CSS console. For detailed directions, see Creating a standard transcoding template, Creating a TSC transcoding template, and Creating an audio-only transcoding template.
Create a transcoding template for live streams using an API. For the API parameters and examples, see CreateLiveTranscodeTemplate.

Must-Knows

CSS supports standard transcoding, Top Speed Codec (TSC) transcoding, and audio-only transcoding. Please read the billing documents before using the services.
Standard transcoding: Standard Transcoding Packages, Standard Transcoding (pay-as-you-go)
TSC transcoding: TSC Transcoding Packages, TSC Transcoding (pay-as-you-go)
Compared with **standard transcoding**, **TSC transcoding** provides higher video quality at lower bitrate. Leveraging technologies including intelligent scene recognition, dynamic encoding, and CTU/line/frame-level bitrate control, TSC transcoding allows you to provide higher-definition streaming services at lower bitrates (50% lower on average). It is widely used for game streaming, showroom streaming, and event streaming.
After creating a template, you can bind it with a playback domain name. The binding takes effect in 5-10 minutes.
After binding a template, you can add the template name (`_template name`) after `StreamName` in the original URL to generate a URL for the transcoding output. Note that the **template name** and **stream name** cannot have the same suffix. For example, if the template name is `hd` , and `StreamName` is `test_a1_hd` , the system will use `test_a1` as the stream name and `hd` as the transcoding template, and playback will fail.
If you have specified the height and width or short and long sides of the transcoding output, to prevent image distortion, keep the resolution of published streams as close to the values set as possible.
On the **Live Transcoding** page of the console, you can view the domain a template is bound to, as well as finer-granularity bindings performed via APIs. You can also unbind a template here.
You can bind one playback domain name with **multiple transcoding templates**, or bind one transcoding template with **multiple playback domain names**.
You can create up to **50** transcoding templates.

The transcoding configuration template for live streaming supports the configuration of a **face blurring** feature, which can achieve the blurring of faces and specific objects. To utilize this feature, you need to submit a ticket to request support. Enabling this service will incur live transcoding fees and Media Processing Service (MPS) intelligent recognition fees.

Creating a Transcoding Template

Creating a standard transcoding template

1. Log in to the CSS console and select **Feature Configuration** > **Live Transcoding**.

2. Click **Create Template**, select **Standard Transcoding** for transcoding type, and complete the following configuration:
Basic configuration: Template name, video bitrate, video resolution and more. For details, see Basic Configuration for Standard Transcoding.
Advanced configuration (optional): Click **Advanced Configuration** to show advanced settings. For details, see Advanced Configuration for Standard Transcoding.
3. Click **Save**.

Basic Configuration for Standard Transcoding

Basic Configuration for Standard Transcoding	Required	Description
Transcoding type	Yes	The optional transcoding types, include standard transcoding, TSC transcoding, or audio-only transcoding.
Template name	Yes	Please enter 1 to 10 characters. The live transcoding template name. It only supports letters and alphanumeric combinations and does not support pure digits. The template name must not duplicate existing transcoding template names, adaptive bitrate template names, or sub-stream names.
Template description	No	The live transcoding template description. It can only contain Chinese characters, letters, digits, spaces, underscores (_), and hyphens (-).
Video quality	No	You can choose Smooth, SD, HD or FHD. After you select a value, the system will automatically enter the recommended video bitrate and height, which can be modified.

Video bitrate(in Kbps)	Yes	You can choose to keep the original bitrate, set the video bitrate, or use the default transcoding bitrate. Set the transcoding code rate, value range: 101Kbps - 8000Kbps. If you enter a value not larger than 1,000, it must be a multiple of 100. If you enter a value larger than 1,000, it must be a multiple of 500.
Video resolution (px)	Yes	Choose to keep the original resolution, set by width and height, or set by length. The default is set by long and short sides. The input value is the short side value, which can be switched to width and height settings, and the input value is the height value. Value range: 0-3000. The value must be a multiple of 2. The other side will be auto-scaled.
DRM encryption	No	It is disabled by default and can be enabled manually. To enable DRM encryption, you need to first obtain the key information in DRM Management. DRM encryption of Widevine, FairPlay, and NormalAES are supported for HLS. For FairPlay encryption, you need to upload the certificate you obtain from Apple to your player. Encryption types: default Widevine, optional Fairplay, and NormalAES.

Advanced Configuration for Standard Transcoding

Advanced Configuration for Standard Transcoding	Required	Description
Video Encoding	No	The original codec is used by default. You can choose H.264, H.265, H.266, or AV1.
Face blurring	No	If necessary, you can submit a ticket to enable this feature and activate Media Processing Service (MPS). The feature is disabled by default and can be manually enabled. The feature can be used to blur faces and specific objects, with the following effect: Enabling this service will incur live transcoding fees and MPS intelligent recognition fees.

Video frame rate (fps)	No	You can choose to keep the original frame rate, set the video frame rate, and keep the original frame rate by default. **Set the video frame rate range**: 1fps - 60fps.
GOP(seconds)	No	The GOP setting range is between 1 to 6 seconds. The larger the GOP, the higher the latency; a smaller GOP may potentially lead to stuttering. If not configured, the system default value will be adopted.
Live subtitles	No	The subtitle feature is deactivated by default, but can be manually activated. To activate this feature, it is necessary to bind a subtitle template. Choose a subtitle template to bind based on your business requirements. Preview and observe the effects of the subtitle template. You can adjust the subtitle template according to business needs at any time.
Parameter limit	No	Parameter limits are disabled by default. After a limit is enabled, if you enter a value higher than the original, the original will be used. This can avoid video quality issues caused by using high video quality settings to transcode videos of low quality.

Creating a TSC transcoding template

1. Log in to the CSS console and select **Feature Configuration** > Live Transcoding.
2. Click **Create Template**, select **Top Speed Codec Transcoding** for transcoding type, and complete the following configuration:

Basic configuration: Template name, video bitrate, video resolution, etc. For details, see Basic Configuration for TSC Transcoding.

Advanced configuration (optional): Click **Advanced Configuration** to show advanced settings. For details, see Advanced Configuration for Top Speed Codec Transcoding.

3. Click **Save**.

Basic Configuration for TSC Transcoding

Basic Configuration for TSC Transcoding	Required	Description
Transcoding Type	Yes	The optional transcoding types, include standard transcoding, TSC transcoding, or audio-only transcoding.

Template name	Yes	Please enter 2 to 10 characters. The live transcoding template name. It only supports letters and alphanumeric combinations and does not support pure digits. The template name must not duplicate existing transcoding template names, adaptive bitrate template names, or sub-stream names.
Template description	No	The live transcoding template description. It can only contain Chinese characters, letters, digits, spaces, underscores (_), and hyphens (-).
Video quality	No	You can choose Smooth, SD, HD or FHD. After you select a value, the system will automatically enter the recommended video bitrate and height, which can be modified.
Video bitrate(in Kbps)	Yes	You can choose to keep the original bitrate, set the video bitrate, or use the default transcoding bitrate. Set the transcoding code rate, value range: 101Kbps - 8000Kbps. If you enter a value not larger than 1,000, it must be a multiple of 100. If you enter a value larger than 1,000, it must be a multiple of 500.
Video resolution (px)	Yes	Choose to keep the original resolution, set by width and height, or set by length. The default is set by long and short sides. The input value is the short side value, which can be switched to width and height settings, and the input value is the height value. Value range: 0-3000. The value must be a multiple of 2. The other side will be auto-scaled.
DRM encryption	No	It is disabled by default and can be enabled manually. To enable DRM encryption, you need to first obtain the key information in DRM Management. DRM encryption of Widevine, FairPlay, and NormalAES are supported for HLS. For FairPlay encryption, you need to upload the certificate you obtain from Apple to your player. Encryption types: default Widevine, optional Fairplay, and NormalAES.

Advanced Configuration for TSC Transcoding

Advanced Configuration for TSC Transcoding	Required	Description
Video Encoding	No	The original codec is used by default. You can choose H.264, H.265, H.266, or AV1.
Video frame rate (fps)	No	You can choose to keep the original frame rate, set the video frame rate, and keep the original frame rate by default. **Set the video frame rate range**: 1fps - 60fps.
GOP(seconds)	No	Value range: 1-6. The larger the GOP, the higher the delay. If this parameter is left empty, the default value will be used. The GOP setting range is between 1 to 6 seconds. The larger the GOP, the higher the latency; a smaller GOP may potentially lead to stuttering. If not configured, the system default value will be adopted.
Live subtitles	No	The subtitle feature is deactivated by default, but can be manually activated. To activate this feature, it is necessary to bind a subtitle template. Choose a subtitle template to bind based on your business requirements. Preview and observe the effects of the subtitle template. You can adjust the subtitle template according to business needs at any time.
Parameter limit	No	It is disabled by default and can be enabled manually. After a limit is enabled, the original value of the input stream will be used if you enter a value larger than the original. This can avoid video quality issues caused by using high video quality settings to transcode videos of low quality.

Creating an Audio-only transcoding template

1. Log in to the CSS console and select **Feature Configuration** > Live Transcoding.

2. Click **Create Template**, select **Audio-only Transcoding** for transcoding type, complete the configuration, and then click **Save**.

Basic Configuration for Audio-only Transcoding	Required	Description
Transcoding type	Yes	The optional transcoding types, include standard transcoding, TSC transcoding, or audio-only transcoding.

Template name	Yes	Please enter 1 to 10 characters. The live transcoding template name. It only supports letters and alphanumeric combinations and does not support pure digits. The template name must not duplicate existing transcoding template names, adaptive bitrate template names, or sub-stream names.
Template description	No	The live transcoding template description. It can only contain Chinese characters, letters, digits, spaces, underscores (_), and hyphens (-).
Audio bitrate (Kbps)	Yes	You can choose to keep the original bitrate or set the audio bitrate, with the default being to keep the original bitrate. To set the audio bitrate, the value range is 101kbps - 500kbps.
Live subtitles	No	The subtitle feature is deactivated by default, but can be manually activated. To activate this feature, it is necessary to bind a subtitle template. Choose a subtitle template to bind based on your business requirements. Preview and observe the effects of the subtitle template. You can adjust the subtitle template according to business needs at any time.
DRM encryption	No	It is disabled by default and can be enabled manually. To enable DRM encryption, you need to first obtain the key information in DRM Management. DRM encryption of Widevine, FairPlay, and NormalAES are supported for HLS. For FairPlay encryption, you need to upload the certificate you obtain from Apple to your player. Encryption types: default **Widevine**, optional Fairplay, and NormalAES.

Binding a Domain Name

1. Log in to the CSS console and select **Feature Configuration** > Live Transcoding.
2. Bind a domain name in either of two ways:

Bind a domain to an existing template: Click **Bind Domain Name** in the top left.

Bind a domain name after creating a transcoding template: After creating a template, click **Bind Domain Name** in the pop-up window.

3. Select a transcoding template and a playback domain in the domain binding window and then click **Confirm**.

Note:
You can click **Add** to bind a template to multiple playback domains.

Unbinding a Domain Name

1. Log in to the CSS console and select **Feature Configuration** > Live Transcoding.
2. Select the target template and click **Unbind**.

3. In the pop-up window, click **Confirm**.

Modifying a Template

1. Log in to the CSS console and select **Feature Configuration** > Live Transcoding.
2. Select the target transcoding template and click **Edit** on the right to modify it.

3. After modification, click **Save**.

Deleting a Template

Note:
If a template has been bound to domains, you need to unbind them before you can delete the template.
You cannot delete a transcoding template that has the Live subtitles feature enabled.
1. Log in to the CSS console and select **Feature Configuration** > Live Transcoding.
2. Select the target template (make sure it's not bound to a domain), and click **Delete**.

3. In the pop-up window, click **Confirm**.

More

You can also **unbind** and **bind** domains and transcoding templates on the **Domain Management** page. For details, see Template Configuration.

Adaptive Bitrate

Last updated：2025-04-29 14:26:20

With the adaptive bitrate feature, the playback bitrate of a live stream can change smoothly based on network conditions. This ensures a smooth playback experience under changing network conditions.

Notes

After creating a template, you can bind it with a playback domain name. The binding takes effect in 5-10 minutes.
A playback domain can be bound with **multiple adaptive bitrate templates**, and an adaptive bitrate template can be bound to **multiple playback domains**.
Each adaptive bitrate template can have up to 15 streams.
For the adaptive bitrate feature to work, the player needs to support adaptive bitrate.
The GOP for the streams of an adaptive bitrate template must be identical.
The codec for the streams of an adaptive bitrate template must be the same.
Adaptive bitrate playback addresses only support HLS and WebRTC playback protocols. For the address concatenation rules, please refer to the Address Generator.
The transcoding configuration template for adaptive bitrate streaming supports the configuration of a face blurring feature, which can achieve the blurring of faces and specific objects. To utilize this feature, you need to submit a ticket to request support. In the adaptive bitrate template, even if multiple sub-stream templates have the face blurring feature enabled, the fee will be charged only once. Enabling this service will incur live transcoding fees and Media Processing Service (MPS) intelligent recognition fees.

Creating an Adaptive Bitrate Template

1. Log in to the CSS console and select **Feature Configuration > Adaptive Bitrate** on the left sidebar.
2. Click **Create template** and complete the following settings:
Basic information: The template name and description. For details, see Basic Information.
Stream information: See Stream Information.
3. Click **Add stream** to add a new stream to the template. You can add up to 15 streams for a template.
4. Click **Save**.

Basic Information

Basic Information	Required	Description
Template name	Yes	Please enter 1 to 10 characters.

		The adaptive bitrate template name. It only supports letters and alphanumeric combinations and does not support pure digits. The template name must not duplicate existing transcoding template names, adaptive bitrate template names, or sub-stream names.
Template description	No	The adaptive bitrate template description. It can only contain Chinese characters, letters, digits, spaces, underscores (_), and hyphens (-).
Live subtitles	No	The subtitle feature is deactivated by default, but can be manually activated. To activate this feature, it is necessary to bind a subtitle template. Choose a subtitle template to bind based on your business requirements. Preview and observe the effects of the subtitle template. You can adjust the subtitle template according to business needs at any time.

Stream Information

Stream Information	Required	Description
Transcoding type	Yes	The optional transcoding types, include standard transcoding and TSC transcoding.
Stream name	Yes	Please enter 1 to 10 characters. Substream Template Name supports 1-10 characters, only allowing letters and alphanumeric combinations, and does not support pure digits. The substream name cannot be duplicated with existing transcoding template names, adaptive bitrate template names, and substream names.
Video quality	No	You can choose **Smooth**, **SD**, **HD** or **FHD**. After you select a value, the system will automatically enter the recommended video bitrate and height, which can be modified.
Video bitrate (Kbps)	Yes	The output video bitrate. Value range: 101-8000. If you enter a value not larger than 1,000, it must be a multiple of 100. If you enter a value larger than 1,000, it must be a multiple of 500.
Video resolution (px)	Yes	By default, you set the **height** of the output video. You can also **set the short side length**. The value must be in the range of 2-3000 and must be multiple of two. The other side will be scaled proportionally.
DRM encryption	Yes	Disabled by default and can be enabled manually. To enable DRM encryption, you need to first obtain the key information in DRM Management.

		DRM schemes including Widevine, FairPlay, and NormalAES are supported for HLS playback. For FairPlay encryption, you need to upload the certificate you obtain from Apple to your player. Encryption Types: Default **Widevine**, Optional Fairplay and NormalAES.
Video Encoding	No	The original codec is selected by default. You can change it to H.264, H.265, H.266, or AV1. The codec for all the streams in the same adaptive bitrate template must be the same.
Face Blurring	No	If necessary, you can submit a ticket to enable this feature and activate Media Processing Service (MPS). The feature is disabled by default and can be manually enabled. The feature can be used to blur faces and specific objects, with the following effect: Enabling the service will incur live transcoding fees and MPS intelligent recognition fees.
Video frame rate (fps)	No	You can choose to keep the original frame rate or set a video frame rate. By default, the original frame rate is maintained. The video frame rate setting value range: 1 fps - 60 fps.
GOP(seconds)	No	The GOP is not specified by default. Value range: 1-6. The higher the GOP, the higher the latency. A smaller GOP may potentially lead to stuttering. The GOP for all the streams in the same adaptive bitrate template must be the same.
Parameter limit	No	Parameter limits are disabled by default. After a limit is enabled, if you enter a value higher than the original, the original will be used. This can avoid video quality issues caused by using high video quality settings to transcode videos of low quality.

Binding a Domain Name

1. Log in to the CSS console. Select **Feature Configuration > Adaptive Bitrate** on the left sidebar.
2. Bind a domain name in either of two ways:

Bind a domain to an existing template: Click **Bind Domain Name** in the top left.

Bind a domain after creating a template: After creating an adaptive bitrate template, click **Bind Domain Name** in the pop-up window.

3. Select an **adaptive bitrate template** and a **playback domain** and then click **Confirm**.

Note:
You can click **Add** to bind a template to multiple playback domains.

Unbinding a Domain Name

1. Log in to the CSS console. Select **Feature Configuration > Adaptive Bitrate** on the left sidebar.
2. Select the target template and click **Unbind**.

3. In the pop-up window, click **Confirm**.

Modifying a Template

1. Log in to the CSS console. Select **Feature Configuration > Adaptive Bitrate** on the left sidebar.
2. Select the target template and click **Edit** on the right to modify it.

3. After modification, click **Save**.

Deleting a Template

Note:
If a template has been bound to domains, you need to unbind them before you can delete the template.
You cannot delete a transcoding template that has the Live subtitles feature enabled.
Once the template is deleted, it cannot be recovered. Please proceed with caution.
1. Log in to the CSS console. Select **Feature Configuration > Adaptive Bitrate** on the left sidebar.
2. Select the target template (make sure it's not bound to a domain), and click **Delete**.

3. In the pop-up window, click **Confirm**.

Audio and Video Enhancement

Last updated：2024-12-03 10:43:57

The audio and video enhancement feature leverages advanced AI algorithms for audio-visual quality restoration and enhancement, achieving a transformative improvement in visual quality and significantly enhancing the subjective quality of audio and video content. This document provides instructions on creating, modifying, and deleting audio and video enhancement templates.

Notes

To use the audio and video enhancement feature, it should be paired with the Top Speed Codec (TSC) transcoding. When pulling a stream, include the stream-pulling parameter `txFeature=` followed by the name of the audio and video enhancement template to apply the enhancement effect to the live stream. An example of a stream-pulling URL is as follows:

```
http://domain/AppName/StreamName_Top Speed Codec transcoding template name.flv?txSecret=Md5(key+StreamName_Top Speed Codec transcoding template name+hex(time))&txTime=hex(time)&txFeature=enhancementtest
```

Currently, audio and video enhancement only supports transcoding resolutions of ≤ 1080P by default. To enable support for other resolutions, you can submit a ticket for configuration.
Audio and video enhancement is a paid add-on service. Using this feature will incur both TSC transcoding fees and audio and video enhancement fees. For details on the billing rules, see billing documentation.

Prerequisites

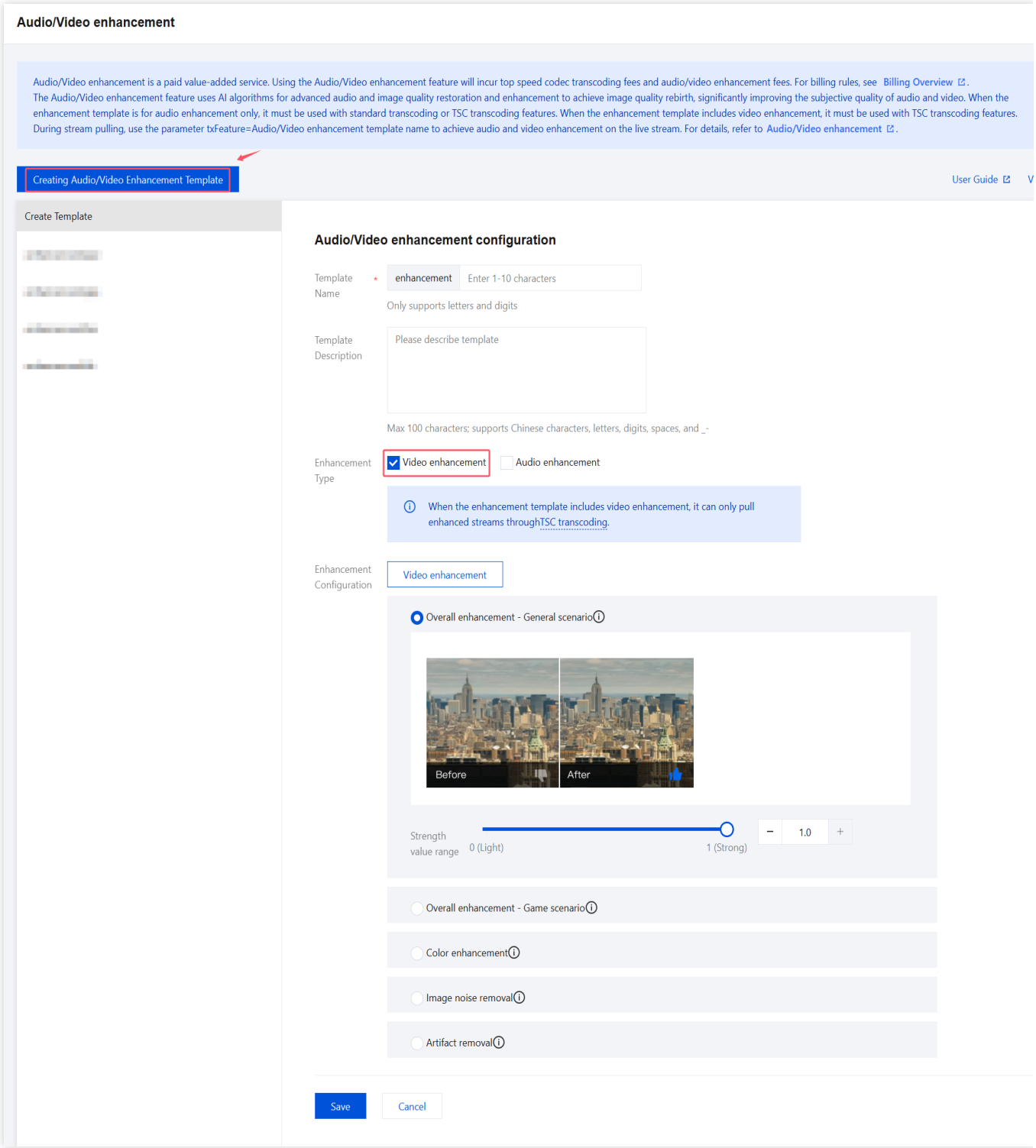
Tencent Cloud Streaming Services (CSS) has been activated, and a push domain name has been added.

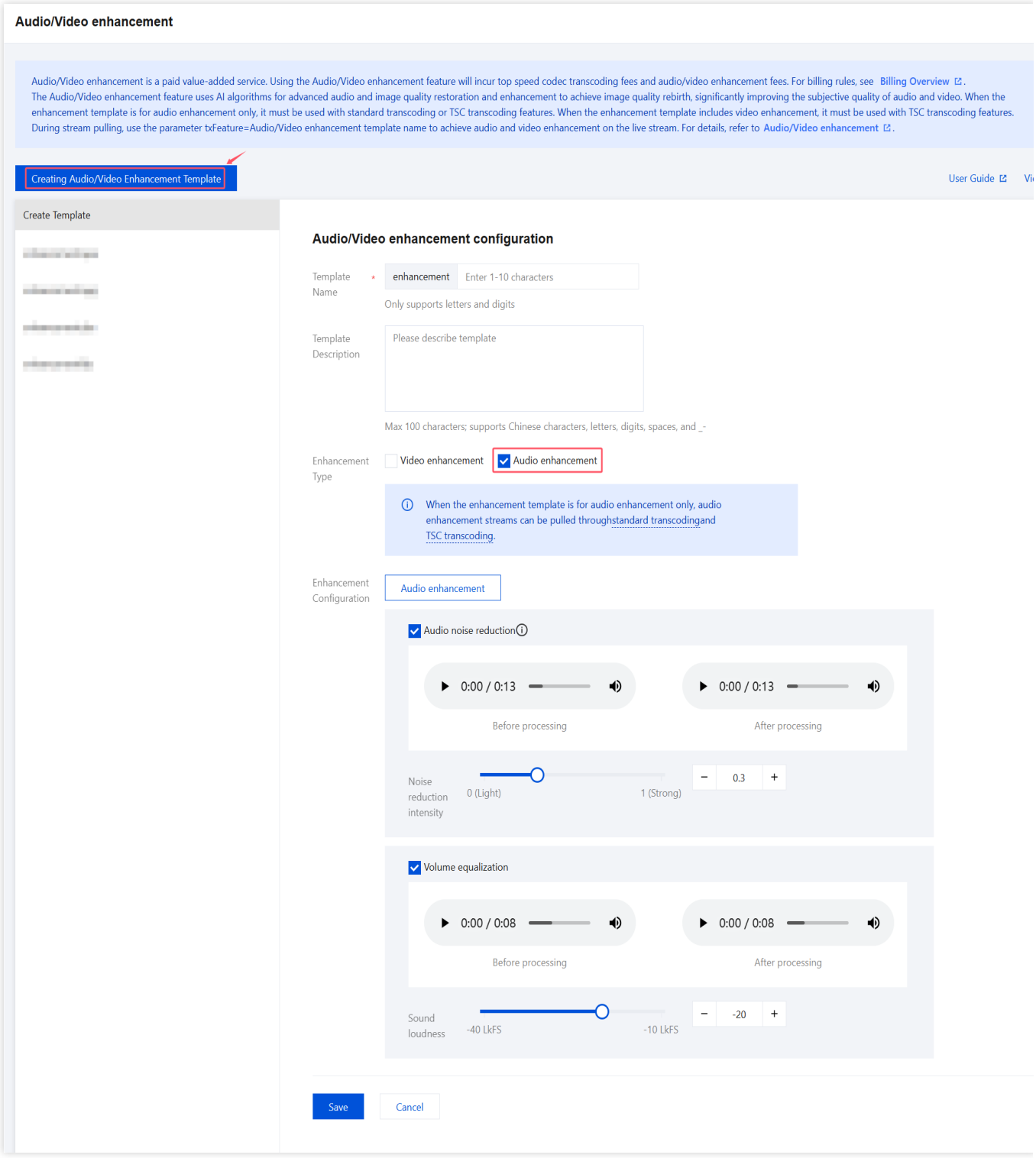
Creating an Audio and Video Enhancement Template

1. Log in to the CSS console and navigate to **Feature Configuration** > Audio/Video Enhancement.
2. Click **Create Audio/Video Enhancement Template** and configure the following settings:

Enhancement Type - Video Enhancement

Enhancement Type - Audio Enhancement


Audio/Video enhancement
Audio/Video enhancement is a paid value-added service. Using the Audio/Video enhancement feature will incur top speed codec transcoding fees and audio/video enhancement fees. For billing rules, see Billing Overview.
The Audio/Video enhancement feature uses AI algorithms for advanced audio and image quality restoration and enhancement to achieve image quality rebirth, significantly improving the subjective quality of audio and video. When the enhancement template is for audio enhancement only, it must be used with standard transcoding or TSC transcoding features. When the enhancement template includes video enhancement, it must be used with TSC transcoding features.
During stream pulling, use the parameter txFeature=Audio/Video enhancement template name to achieve audio and video enhancement on the live stream. For details, refer to Audio/Video enhancement.
Creating Audio/Video Enhancement Template
User Guide
Create Template
Audio/Video enhancement configuration
Template Name
enhancement
Enter 1-10 characters
Only supports letters and digits
Template Description
Please describe template
Max 100 characters; supports Chinese characters, letters, digits, spaces, and _-
Enhancement Type
Video enhancement
Audio enhancement
When the enhancement template includes video enhancement, it can only pull enhanced streams throughTSC transcoding.
Enhancement Configuration
Video enhancement
Overall enhancement - General scenario
Before
After
Strength value range
0 (Light)
1 (Strong)
1.0
Overall enhancement - Game scenario
Color enhancement
Image noise removal
Artifact removal
Save
Cancel



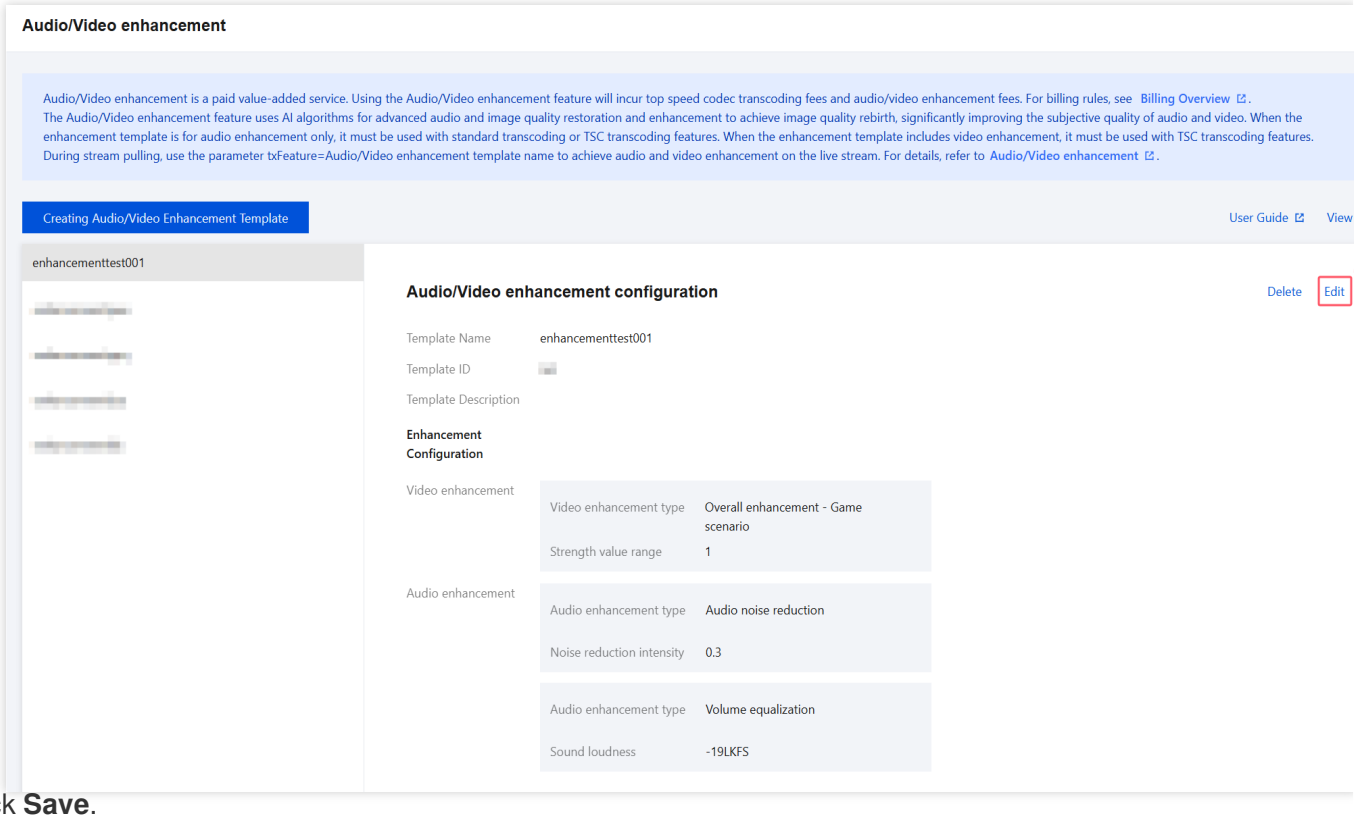
Configuration Item	Description
Template name	The prefix of the template name is fixed as enhancement. The name cannot exceed 10 characters and supports only English letters and numbers.
Template description	Supports Chinese, English, numbers, spaces, underscores (_), and hyphens (-), with a maximum of 100 characters.

Enhancement Type		When selecting the enhancement type, you can manually choose either **Video Enhancement**, **Audio Enhancement**, or both based on your actual business needs. If the enhancement template includes video enhancement, the enhanced stream can only be pulled using TSC transcoding. If the enhancement template includes only audio enhancement, the enhanced audio stream can be pulled using either standard transcoding or TSC transcoding.
	Video enhancement	**Enhancement Configuration** The default setting is overall enhancement - general scenario, which can be switched to overall enhancement - game scenario, color enhancement, image noise reduction, or artifact removal. The default intensity value is 1, with a configurable range from 0 to 1. When using the video enhancement feature, select the appropriate enhancement type based on your actual needs. Below is a description of the available video enhancement types. **Overall Enhancement - General Scenario**: Designed for common live streaming scenarios such as show streaming and e-commerce streaming, this enhancement leverages AI's comprehensive analysis capabilities to automatically balance texture content. It removes compression artifacts and glitches while enhancing critical details, significantly improving the overall subjective quality of the live stream. **Overall Enhancement - Game Scenario**: Tailored for game live streaming scenarios, this enhancement leverages AI's comprehensive analysis capabilities to automatically balance texture content. It removes compression artifacts and glitches while enhancing critical details, significantly improving the overall subjective quality of the live stream. **Color Enhancement**: Addressing color distortion or enhancement needs caused by issues with capture devices or video storage, this feature adjusts the colors to more closely match real-life tones while enhancing them to better suit human visual preferences. **Image Noise Reduction**: During live streaming, random noise may be introduced by cameras and environmental factors. This feature provides noise reduction while preserving details, eliminating random noise from the video. **Artifact Removal**: During transcoding or multiple rounds of transcoding, repeated compression can introduce block effects, ringing effects, chroma bleeding, and mosquito noise, causing visual distortions in the video. This feature effectively repairs compression-induced distortions, enhancing the visual quality of the video.
	Audio enhancement	**Enhancement Configuration** Audio noise reduction is selected by default. Based on your actual business needs, you can manually select Volume Equalization, or enable both features.

		Audio noise reduction The noise reduction intensity value controls the effect of audio noise reduction, with lower values indicating weaker noise reduction and higher values indicating stronger noise reduction. The default intensity value is 0.3, and the configurable range is 0 to 1. **Note:** It is recommended to enable noise reduction when there is no complex background noise and the focus is on highlighting vocals. For sources **without background music**, **it is recommended to set the intensity value below 0.6**. Higher values may degrade audio quality, leading to issues like muffled speech or excessive reverberation. For sources **with background music**, **it is not recommended to enable noise reduction. If it is necessary, set the intensity value below 0.3**. Higher values may suppress vocal volume and negatively impact audio quality. Volume equalization The sound loudness value measures the loudness level of an audio signal. It is recommended to adjust this parameter based on the actual playback environment: higher values for noisy environments and lower values for quiet environments. The default loudness value is -20, with a configurable range from -40 to -10.

Modifying a Template

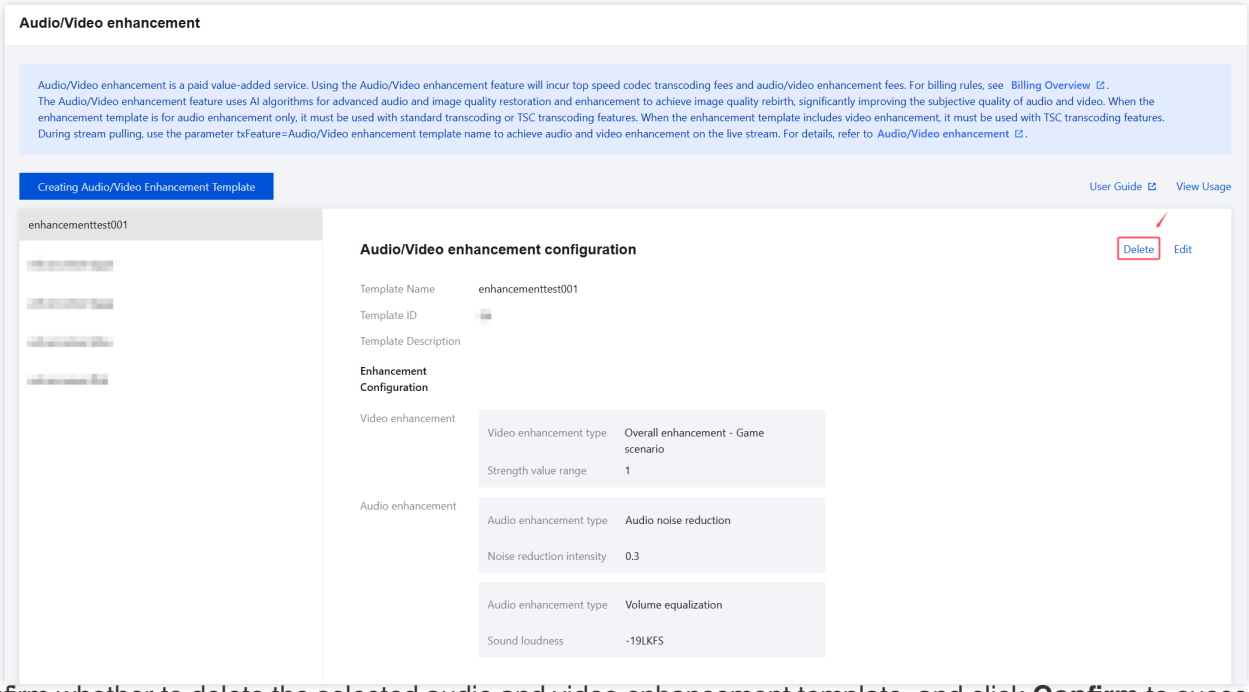
1. Navigate to **Feature Configuration** > Audio/Video enhancement.
2. Select the audio and video enhancement template you have created and click **Edit** on the right to modify the template information.



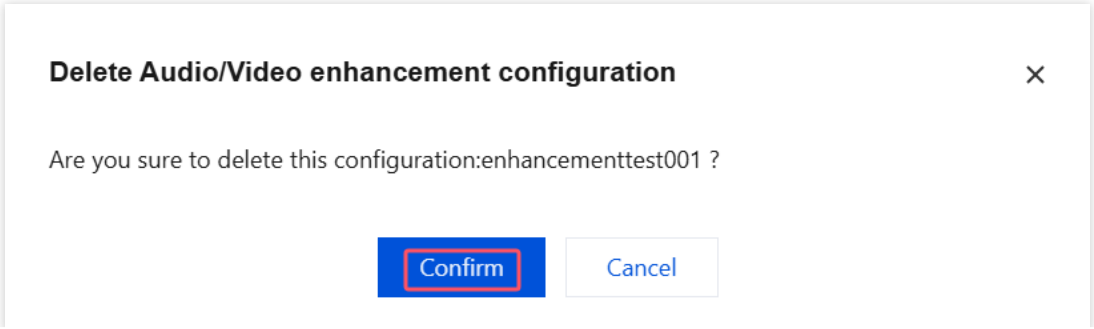
3. Click **Save**.

Deleting a Template

1. Navigate to **Feature Configuration** > Audio/Video enhancement.
2. Select the audio and video enhancement template you have created and click **Delete** at the top.



3. Confirm whether to delete the selected audio and video enhancement template, and click **Confirm** to successfully delete it.



AI Features
Live Subtitling
Subtitle Templates

Last updated：2025-05-23 14:35:30

The live subtitling feature can perform real-time Automatic Speech Recognition (ASR) in live streaming, convert the speech into subtitles, and support translation into the target language. Currently, the feature offers multilingual speech translation services. In practical applications, choose appropriate target language combinations based on your service needs and audiences.
This document describes how to create, modify, and delete subtitle templates through the console.

Points of Attention

A template takes effect about 5 to 10 minutes after successfully created.
To use the live subtitling function, after binding a subtitle template to a transcoding template, you should obtain the subtitle stream with the suffix of a playback address corresponding to the name of a transcoding template.
Live subtitling function is a **premium service**. Utilizing this function will incur live transcoding fees and ASR fees of MPS. Cross-language translation may generate voice translation fees of MPS. For the specific billing rules, please refer to billing document.

Prerequisites for Use

The CSS service has been activated.

Creating Subtitle Template

1. Log in to the CSS console. Choose **Feature Configuration> AI Features** > **Live Subtitles**.
Note:
Due to the use of the live subtitling function, creating a service role and authorizing the current account role to use MPS product services are required for the **first** creation of a subtitle template.
2. Click **Grant access** to enter the CAM role management page.

3. On the role management page, click **Grant**. After completing identity authentication to finish the MPS authorization, you can utilize the MPS service normally.

4. After successful authorization, select the service agreement and click **Start**. The system will automatically activate the MPS product and open the live subtitling management page.
5. Click **Create template** to enter the subtitle template creation page and configure the template as follows:

Note:
The font selection for subtitles will vary depending on the **Subtitle Translation** and **Subtitles** you have selected. Select the appropriate source language type, target language, and subtitles according to your actual needs.

Configuration Item	Description
Template Name	The prefix for the template name is fixed to "subtitle". The template name cannot exceed 30 characters and only supports English letters and digits.
Template Description	Subtitle template description. It contains up to 100 characters, only supporting letters, digits, underscores, and dashes.
Preset Styles	When preset styles are selected, the system will automatically adapt **Font Color**, **Subtitle Line Count**, **Characters per Line**, and **Margins and Line Spacing**. Currently, the following preset styles are supported: The default option is Small text without bar. You may select Small text without bar, Large text without bar, Small text with bar, or Large text with bar to configure the settings. After selection, the system will automatically set the corresponding subtitle style, which can be modified. Modifying configurations will clear the selected preset styles.
Dynamic/Steady State Effect	The default setting is **delayed steady-state sentence-by-sentence subtitles.** You can switch it to real-time dynamic subtitles or delayed steady-state word-by-word subtitles. When choosing the Delayed Steady State Subtitles mode, it's necessary to set the latency, with a default value of 10 seconds. Available latency options include 20 seconds, 30 seconds, and 60 seconds. **Note:** When you choose real-time dynamic subtitles, subtitles in live streaming will be dynamically corrected word by word based on changes in speech. When you choose delayed steady-state word-by-word subtitles, the system will delay the display of live streaming based on the set time, but the full-sentence subtitle mode provides a better viewing experience.
Subtitle Translation	The default source language is Chinese. English, Japanese, and Korean are also supported. It is set to "No Selection" by default. Switching to any of other unselected options in the source language is supported. For example, if "English" is selected as the source

	language, the available options for the target language include: No Selection, Chinese, Japanese, and Korean. Cross-language translation will incur voice translation fees of MPS. ASR fees will be generated without translation. For more details, please see Content II. If you need to translate it into other languages, please submit a ticket to contact us.
Subtitles	**Source** is supported by default. **Target** and **Bilingual Subtitle** are also supported. By selecting the three options of **Source language** , **Target language** , and **Subtitles** , you can achieve subtitle effects in different languages.
ASR Associating with Custom Hotwords	The Automatic Speech Recognition (ASR) with custom hotwords feature is disabled by default. Enabling custom hotwords can improve the recognition accuracy of ASR for proprietary words. After enabling the feature of custom hotword lexicons, you need to select the hotword lexicon you want to apply. If you have not created a hotword lexicon, you can click **Add** to jump to the Manage Lexicon page. For detailed steps, see Manage Lexicon.
Font Color	The font selection for subtitles will vary depending on the **Subtitle Translation** and **Subtitles** you have selected. You may choose a variety of fonts such as DIN Alternate Bold, Helvetica, or HelveticaInseratLTPro-Roman, or select a custom font according to your service needs. If you need a custom font, click **Custom** to upload the font. The system will display a confirmation box. Before uploading and using the font, check the notice, and then click **OK**. Note that only .ttf files are supported. Before using a custom font, make sure that you have obtained legal authorization, otherwise Tencent Cloud will not bear any legal responsibility arising from the use. The default font color is **white** , and you can customize the font color according to your preference. When "Subtitles" is set to "Bilingual Subtitle," it supports the configuration of distinct fonts and colors for each language individually.
Subtitle Background	You can select a preset style or upload a custom background according to your business needs. After selection, you can preview the effect. Custom upload instructions: Upload a file in PNG format, with a file size not exceeding 1MB.
Subtitle Line Count	Options are **1** or **2** . When lines exceed the displayed range, only the latest content will be displayed.
Characters per line	The value range is 1 - 200. When the Preset styles are set to "Small text without bar" or "Small text with bar," the default number of characters per line is 65. When the Preset styles are set to "Large text without bar" or "Large text with bar," the default number of characters per line is 25. One Chinese character counts as 1, while one English character or number counts as half. The fewer the characters per line are, the larger the font size is.

Real-Time Interpretation	The Real-Time Interpretation feature is disabled by default and is only displayed when the subtitle effect is set to Delayed steady-state sentence-by-sentence subtitles, and the Subtitles option is configured as either Target or Bilingual Subtitle. **Note:** Note: If this feature is enabled, the system will interpret the source audio to the target audio with the selected voice effect. This feature will incur recognition fees. For billing rules, seeBilling Documentation. This feature does not support Korean currently. By clicking and dragging the mouse over the relevant language play icon, you can audition the real-time voice translation effects. When the translation language is set to English, Real-Time Interpretation supports the following voice: WeRose. By clicking and dragging the mouse over the relevant language play icon, you can audition the real-time voice translation effects.
Preview	You can adjust the subtitle display effect by dragging and scaling the position and size of the subtitle content type and subtitle background. Uploading background images, selecting the preview window resolution, and entering the subtitle test content can help you preview subtitle styles. The subtitle effect is for reference only and the test content will not be translated.

6. Click **Save** to save the current template.

Binding Transcoding Template

1. Log in to the CSS console. Choose **Feature Configuration** > **AI Feature** > **Live Subtitles**.
2. The system allows subtitle templates to bind transcoding templates or adaptive bitrate templates. Both transcoding templates and adaptive bitrate templates have similar subsequent use procedures. A transcoding template serves as an example for description below:
2.1 Direct association with transcoding templates:
2.1.1 Associate a transcoding template after it is successfully created: After the successful creation of a transcoding template, click **Bind transcoding template** in the upper left corner.

2.1.2 Select **Transcoding template** or **Adaptive bitrate template** according to your actual business requirements, then click **Confirm**.

2.2 In order to bind a playback domain to the corresponding transcoding template, the subtitle effects will be output at the same time when the transcoding stream is obtained subsequently (add _ transcoding template name after the corresponding live stream StreamName to generate a transcoding stream address).
Note:

Once the transcoding template is bound, the subtitle function configured in the transcoding template will be synchronously activated.

Unbinding

1. Log in to the CSS console. Choose **Feature Configuration** > **AI Features** > **Live Subtitles**.
2. Select the transcoding template associated with a domain name and click **Unbind**.

3. Confirm whether to unbind the current associated domain. Click **Confirm** to unbind it.

Modifying a Template

1. Log in to the CSS console. Choose **Feature Configuration** > **Live Subtitles**.
2. Select the successfully created subtitle template and click **Edit** on the right to go to the template information modification page. Click **Save** to finish the modification.

Deleting a Template

Note:
If the template has already been associated, you must first unbind it before you proceed with the deletion process. Note that a template cannot be restored after deleted. Be careful when performing operations.
1. Log in to the CSS console. Choose **Feature Configuration** > **Live Subtitles**.
2. Select the successfully created subtitle template and click **Delete** above.

3. Confirm whether to delete the current subtitle template, then click **Confirm** to successfully delete it.

Manage Lexicon

Last updated：2025-05-23 14:35:30

Custom hotwords can significantly improve Automatic Speech Recognition (ASR) accuracy in recognizing particular words. If different words have the same pronunciation, the hotword with the highest weight will be used. Currently, hotwords are only supported for Mandarin Chinese and English. Hotwords take effect 10 minutes after successful configuration.

Creating a Library

1. Log in to the CSS console, and click **Feature Configuration > AI Features**, then click **Manage Lexicon**.

2. Click **Create library**. In the pop-up window, fill in the configuration information.

Configuration Item	Required	Description
Library	Yes	The prefix of the library name is always "hotword". It only supports English letters, digits, underscores (_), and hyphens (-), and contains up to 30 characters.
Direct Import	No	Toggle this on if you want to import hotwords from a file. Click **Select File**, and then select a file from your computer. Make sure that the file meets the following requirements: File format: TXT. File size: within 100 KB. File encoding: UTF-8 or GBK encoding.
Keywords	Yes	Add hotwords here. Only Chinese and English hotwords are supported. Each hotword can contain no more than 10 Chinese characters or 30 English characters. Punctuation marks and special characters are not allowed. Multiple hotwords should be separated by commas, and the number of hotwords cannot exceed 1,000. Hotwords and weights should be separated by "|". For example, "Tencent Cloud|10,speech recognition|5,ASR|10". The hotword weight ranges from 1 to 10. The greater the weight of a hotword, the greater the probability that the hotword can be recognized.

3. Click **Confirm**, and the hotwords are added.

Viewing a Library

On the Manage Lexicon page, click the name of the library you want to view on the left side, and view its detailed information in the pop-up window.

The information includes the library name, lexicon table ID, last updated time, number of hotwords, and list of hotwords and their weights.

Modifying a Library

1. On theManage Lexicon **page**, find the library you want to modify, click **Edit** on the right, and then modify the configuration information of the library in the pop-up window.

2. Click **Confirm** to save the current template and complete the modification of the custom library.

Deleting a Library

1. On theManage Lexicon **page**, find the library you want to delete, and then click **Delete** on the right.

2. A confirmation box will pop up. Click **OK** to delete the custom library.

Dynamic Overlays

Last updated：2025-06-03 15:15:02

The system supports overlaying dynamic overlays onto live streams, enabling effects such as adding advertisements, scoreboards, and character introductions to the live stream visuals.
This document will introduce how to create, modify, and delete dynamic overlay templates using the console.

Must-Knows

The template will take approximately 5 to 10 minutes to take effect after being successfully created.
The dynamic overlay feature is currently in the beta testing phase. At present, only transcoding fees are charged.
Starting in March 2025, additional fees for the dynamic overlay feature are expected to be implemented.
It is strictly prohibited to use images, videos, or text containing inappropriate content, such as pornography, illegal activities, or other violations, as dynamic overlay material.
The dynamic overlay effect on live streams can be achieved using the following two methods:
Configure the live stream and dynamic overlay input sources in the broadcast console.
Add the streaming parameter overlay_url (set to the dynamic overlay preview address) when pushing the stream. An example of a streaming address is as follows:

```
rtmp://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)&overlay_url=dynamic overlay preview address
```

Prerequisites

Tencent Cloud Streaming Services (CSS) has been enabled.

Dynamic Overlay Configuration Management (Administrative Side)

Adding Dynamic Overlays

1. Log in to the CSS console and navigate to **Feature Configuration > AI Features > Dynamic Overlays**.
2. Click **Add Dynamic Overlays** to open the addition window.

3. You can select **News**, **Event Scoreboard**, **General Images and Videos**, Or opt for all three options simultaneously.

Editing

1. Log in to the CSS console and navigate to **Feature Configuration > AI Features** > **Dynamic Overlays**.
2. In the overlay list, select the dynamic overlay you want to edit based on your business requirements, and click **Edit**.

3. After entering the Dynamic Overlay Configuration Management System page, you can customize styles, adjust the content, or copy the control address and preview address as needed. This allows live room managers to share and collaborate effectively.
4. Program Package, Event Scoreboard, and General Images and Videos are enabled by default, but you can manually disable it based on your business requirements. Additionally, you can independently customize program control, subtitle design, tag design, scrolling bar design, event control, event settings, scoreboard design,content control, image design,video design , and text design.

News

Event Scoreboard

General Images and Videos

You can customize the dynamic overlays for the news based on your business requirements.

Program Control

The content of tags, program names, and titles can be customized. Both Chinese and English characters, as well as special characters, are supported, with a maximum limit of 30 characters.

The content summary and scrolling bar content can be customized, supporting Chinese and English characters as well as special characters, with a maximum limit of 100 characters. The scrolling bar can display multiple items, with an adjustable order and the option to delete any item. The items will scroll and display sequentially.

Tags, program names, titles, dates and times, content summaries, and scrolling bars are enabled by default but can be manually disabled.

Subtitle Design

Default values can be used in the background color and font color of program names, titles, dates and times, and content summaries. You can also adjust the colors and transparency as needed.

Horizontal and vertical positions: The proportion of the screen's total width that the lower-left corner of the material is offset from the left side of the screen. The default value is 0, and the range for the horizontal position is 0 to 100. Improper settings may result in incomplete display of the scoreboard. Clicking Reset will reset both the horizontal and vertical positions to their default values.

The size, including width and height, should be set within the range of 0 to 100. Exceeding this range may result in abnormal display of the scoreboard. Clicking Reset will reset both height and width to their default values.

Tag Design

Default values can be used in the background color and font color of tags. You can also adjust the colors and transparency as needed.

Horizontal and vertical positions: The proportion of the screen's total width that the lower-left corner of the material is offset from the left side of the screen. The default value is 0, and the range for the horizontal position is 0 to 100. Improper settings may result in incomplete display of the scoreboard. Clicking Reset will reset both the horizontal and vertical positions to their default values.
The size, including width and height, should be set within the range of 0 to 100. Exceeding this range may result in abnormal display of the scoreboard. Clicking Reset will reset both height and width to their default values.

Scrolling Bar Design
Default values can be used in the background color and font color of the scrolling bar title and content. You can also adjust the colors and transparency as needed.
Horizontal and vertical positions: The proportion of the screen's total width that the lower-left corner of the material is offset from the left side of the screen. The default value is 0, and the range for the horizontal position is 0 to 100. Improper settings may result in incomplete display of the scoreboard. Clicking Reset will reset both the horizontal and vertical positions to their default values.
The size, including width and height, should be set within the range of 0 to 100. Exceeding this range may result in abnormal display of the scoreboard. Clicking Reset will reset both height and width to their default values.

You can customize the dynamic overlay for the event scoreboard based on your business requirements.
Event Control
The scores for the home team and the away team are integers, ranging from 0 to 100.
The minutes and seconds for event timing are integers. The range for seconds is 0 to 59.

Event Settings
The home team name, away team name, and event title support Chinese and English characters as well as special characters, with a maximum limit of 10 characters.
The home and away team logos support local file uploads.
The default timing method is clockwise, with an option to select counterclockwise.

Scoreboard Design
Default values can be used in the background color and font color of the home team, score, away team, timer/session, and event title. You can also adjust the colors and transparency as needed.
Horizontal and vertical positions: The proportion of the screen's total width that the lower-left corner of the material is offset from the left side of the screen. The default value is 0, and the range for the horizontal position is 0 to 100. Improper settings may result in incomplete display of the scoreboard. Clicking Reset will reset both the horizontal and vertical positions to their default values.
The size, including width and height, should be set within the range of 0 to 100. Exceeding this range may result in abnormal display of the scoreboard. Clicking Reset will reset both height and width to their default values.

You can customize dynamic stickers for general images and videos according to your specific business requirements.

Content Control

The content of images can be customized.

The text content supports both Chinese and English characters, as well as special symbols, with a maximum limit of 100 characters. Multiple text entries can be added.

The video content supports customization. You can choose whether to enable audio, which is disabled by default but can be manually activated. Once enabled, the audio from the video will also be integrated into the live stream.

Layer Order: Allows users to adjust the layering sequence of images, videos, and text by dragging elements within the console. By default, the order is set to images, videos, and text, with text positioned on the outermost layer.

Images, videos, and text content are enabled by default, though they can be manually disabled.

Image Design

Supports configuring position and size ratios.

The horizontal and vertical positions are adjustable. By clicking "**Reset**" , the horizontal and vertical positions will be restored to their default settings.

The size settings encompass both height and width. By clicking "**Reset**", the height and width will be restored to their default values.

Video Design

Supports configuring position and size ratios.

The horizontal and vertical positions are adjustable. By clicking "**Reset**", the horizontal and vertical positions will be restored to their default settings.

The size settings encompass both height and width. By clicking "**Reset**", the height and width will be restored to their default values.

Text Design

The background color and font color can be set to their default values. Alternatively, you may customize the colors and adjust their transparency as needed.

Supports the adjustment of text size, encompassing font size, positioning, and scaling proportions.

The horizontal and vertical positions are adjustable. By clicking "**Reset**", the horizontal and vertical positions will be restored to their default settings.

The size settings encompass both height and width. By clicking "**Reset**", the height and width will be restored to their default values.

5. Users can click the background option to select a local image or enter a pull stream address to preview the dynamic overlay effect.

News Effect Preview

Event Scoreboard Effect Preview
General Images and Videos preview

6. After completing the configuration, click **Share and collaborate** to copy the configuration output link and share it with the live room manager.
News
Event Scoreboard
General Images and Videos

Preview

1. Log in to the CSS console and navigate to **Feature Configuration > AI Features > Dynamic Overlays**.
2. In the overlay list, select the dynamic overlay you want to preview based on your business requirements and click **Preview** to open the real-time preview window.

Renaming

1. Log in to the CSS console and navigate to **Feature Configuration > AI Features** > **Dynamic Overlays**.
2. In the overlay list, select the corresponding dynamic overlay based on your business requirements and click **Rename**.

3. After renaming the dynamic overlay, click **Save**.

Deleting

1. Log in to the CSS console and navigate to **Feature Configuration > AI Features > Dynamic Overlays**.
2. In the overlay list, select the dynamic overlay you want to delete based on your business requirements and click **Delete**.

3. Operate with caution. Once deleted, the dynamic overlay cannot be recovered. If you are certain about the deletion, click **Delete** again to confirm.

Copying Address

1. Log in to the CSS console and navigate to **Feature Configuration > AI Features** > **Dynamic Overlays**.
2. In the overlay list, select the corresponding dynamic overlay based on your business requirements, click **More** to expand, and copy the control address and preview address.

Note:
Share the control address with the live room manager. After the control address is opened, the dynamic overlay effects can be customized, and content can be adjusted in real time according to the live room requirements. The adjusted effects will be synchronized in real time to the live stream with the overlay.
When you implement the dynamic overlay effect on live streams, the value used for the `overlay_url` parameter in the streaming address or the dynamic overlay input source added in the broadcast console corresponds to the **preview address**.

Live Room Manager

1. Open the control address shared by the administrative side to customize the dynamic overlay effects as needed and adjust the overlay content according to live stream requirements.
2. By using the preview address shared by the administrative side in the broadcast console or by including it as a streaming parameter in the streaming address, the live stream can be overlaid with dynamic overlays. This enables effects such as scoreboards, character introductions, advertisements, and announcements in the live stream.

ROI Intelligent Recognition

Last updated：2025-05-23 14:35:30

ROI (region of interest) recognition can identify the positions of important visual elements in a video in real time, such as faces, game characters, or steaming hosts, and send this information along with the video to the playback device. Using the ROI information, the player can do things like blur the background in a scene and prevent on-screen comments from covering important elements of the video. This document explains how to create, modify, and delete ROI recognition templates in the console.

Notes

A template takes effect about 5-10 minutes after it is created.
To use the ROI recognition feature, you need to add the parameter `roirecognition` = ROI configuration name to your streaming URL. This lets the player access and process ROI data from the live stream, which can enable features like background blur and preventing on-screen comments from covering important parts of the video. For detailed instructions, see ROI Intelligent Recognition Feature Practice. Example streaming URL:
`rtmp://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)&roirecognition=TemplateName`
The ROI recognition feature is a **paid value-added service**. Using this feature incurs live transcoding fees and Media Processing Service (MPS) intelligent content recognition fees. For specific billing rules, refer to the billing documentation.

Prerequisites

You have activated Tencent Cloud Streaming Services.

Creating an ROI Configuration Template

1. Log in to the CSS Console and navigate to **Feature Configuration > AI Features > ROI Intelligent Recognition.**

Note:

To use the ROI intelligent recognition feature in the Live Streaming Lab, **the first time** you create a template, you will also need to create a service role and authorize the current account to use MPS. Click **Authorize Now** to enter the CAM for authorization.
2. Click **Authorize Now** to enter the CAM role management page.

3. On the role management page, click **Grant** to complete the identity verification and finalize the Media Processing Service authorization, enabling normal use of the Media Processing Service.

4. After successful authorization, check the service agreement and click **Start**, and the system will automatically activate the MPS product and open the Intelligent Streaming Media Processing management page.
5. Enter the ROI Intelligent Recognition management page, and click **Create ROI template**.

6. Enter the ROI configuration page and proceed with the following configuration:

Configuration Item	Description
Name	The default prefix "roi" is added to the template name. The template name can be 1-10 characters long (only combinations of letters and digits are supported).
Description	Supports only Chinese, English, digits, spaces, underscores (_), hyphens (-) and can be up to 100 characters long.
Training Model	Default is **General**. Supported training models include: Honor of Kings, NBA2K Game, and Live Shows. General: Capable of recognizing common areas of human eye focus in different environments. Honor of Kings: Capable of recognizing hero roles and zones in different environments within the Honor of Kings game. NBA2K Game: Capable of recognizing players, basketballs, scoreboards, and other zones in different environments within the NBA2K game. Live Shows: Capable of recognizing the host's face. **Note:** The system can identify elements such as faces and game characters within the video. Selecting an appropriate training model for the scenario can greatly improve the accuracy of ROI intelligent recognition. If the models provided do not meet the needs of your specific scenario, you can submit a ticket to request a model.

7. After filling in the configuration items, click **Confirm** to complete.

Modifying a Template

1. Log in to the CSS Console and navigate to **Feature Configuration> AI Features > ROI Intelligent Recognition**.
2. Select your successfully created ROI configuration template, and click **Edit** on the right to modify the template information.

3. Click **Confirm** to complete.

Deleting a Template

1. Log in to the CSS Console and navigate to **Feature Configuration > AI Features > ROI Intelligent Recognition**.
2. Select your successfully created ROI configuration template, and click **Delete** to the right.

3. Click **OK** to confirm that you want to delete the template.

AI Cloud-based Effects

Last updated：2025-06-23 17:49:07

The AI Cloud-based Effects feature of Cloud Streaming Services (CSS) integrates with the AI text-to-video technology, allowing users to generate personalized videos with special effects in real time by inputting text descriptions (Prompts). Users can also manage the list of generated special effects via the console or API, as well as send videos with special effects to a specified live stream. This feature enhances the interactive experience of users, creating unique emotional expression methods for both anchors and audiences. Compared with traditional fixed gift special effects, it has increased interactivity.
This article will show you how to send effects through the console.

Must-Knows

Using the AI Cloud-based Effects feature of CSS will incur two charges: one for generating a video with special effects and another for sending it. The specific fees are incurred based on the actual usage. For relevant billing instructions, see Documentation.
Videos with special effects are generated by large models and have a certain degree of randomness. Video effects will gradually improve with technological evolution and version iterations.
The use of Prompts containing prohibited sensitive words (such as violence and illegal sensitive words) is strictly forbidden.

Prerequisites

You have activated Tencent Cloud Streaming Services.

Send Special Effect

1. Log in to the CSS Console and navigate to Feature Configuration > AI Features > Cloud AI Special Effects,Click **Send Special Effect**.

2. In the pop-up page, check Online Live Stream and click **Confirm** to Send Special Effect.

3. You can also click the **Send Special Effect and Preview** button to preview it.

4. Click **Cancel** to stop the Send Special Effect.

Live Recording
Recording to VOD

Last updated：2025-05-21 11:12:59

CSS supports recording live streams and storing recording files in VOD for download and preview. This document describes how to create, bind, unbind, modify, and delete recording templates.
You can create a recording template in two ways:
In the CSS console: For detailed directions, see Creating a Recording Template.
Using an API: For the API parameters and examples, see CreateLiveRecordTemplate.

Notes

Recording files are saved in VOD by default. Please activate VOD first. To avoid service suspension due to overdue payments, you can also buy VOD storage packages in advance. For more information, see Getting Started with VOD.
After enabling the recording feature, please make sure that your VOD service is in normal status. If it is not activated or is suspended due to overdue payments, live recording will fail. No recording files will be generated. Nor will fees be incurred.
A recording file is available in about five minutes after recording ends. For example, if you start recording a live stream at 12:00 and stop at 12:30, you can get the recording at around 12:35.
Limited by the support of audio and video file formats (FLV/MP4/HLS) for codec types, you can only use the H.264 and H.265 video codec and the AAC audio codec.
After creating a recording template, you can bind it with push domain names. For detailed directions, see Recording Configuration. The binding takes effect in about 5-10 minutes.
For the naming rules of generated recording files, see VodFileName.
Binding, unbinding, or modifying a template affects only new live streams and not ongoing ones. To make the change apply to ongoing live streams, you need to stop them and push them again.
Mixed-stream recording does not support mixing streams inside the Chinese mainland with those outside. It will cause an error and playback will fail.

Prerequisites

You have activated CSS and added a push domain.
You have activated the VOD service.

Creating a Recording Template

1. Log in to the CSS console and select **Feature Configuration** > Live Recording on the left sidebar.
2. In the live recording settings, choose **Save to VOD** .

3. Click **Create template** to set the template information and proceed with the following configurations:
Basic recording configuration: This includes the template name, recording content, recording format, and other configuration items. For details, see Basic Recording Configuration Instructions.
Basic recording format configuration: This includes HLS file segmentation, max recording time per file, resumption timeout, and other configuration items. For details, see Basic Recording Format Configuration Instructions.
(Optional) Advanced recording format configuration: By clicking **Advanced Configuration** , you can access and select additional configurations. For details, see Advanced Recording Format Configuration Instructions.
Upon completion, click **Save** .

Basic Recording Configuration Instructions

Note:
When recording the original stream via WebRTC streaming, both HLS and MP4 formats can record and play audio normally, but the FLV format will lose audio. It is recommended to select HLS or MP4 format.
When an audio-only transcoding template is selected during specified transcoded stream recording, the HLS/FLV/MP4 recording file will miss the initial 2 seconds of content due to format conversion. Please plan your push and recording schedule accordingly.
Initiating a transcoding task is required for recording transcoded streams, which will incur additional transcoding costs. However, if the same transcoding template is used for playback, charges will not be duplicated.

Basic Configuration Item		Description
Template Name		The template name, which can contain Chinese characters, letters, digits, underscores (_), and hyphens (-).
Template Description		The template description, which can contain Chinese characters, letters, digits, underscores (_), and hyphens (-).
Recording Content	Original stream	Record videos before transcoding, watermarking, and stream mixing.Videos will be recorded before transcoding, watermarking, and stream mixing. Please note that for WebRTC streams, recording the original stream may cause audio playback to fail, We recommend you select "Watermarked stream" or "Transcoded and watermarked stream".
	Watermarked stream	Videos will be recorded after they are watermarked according to the specified watermark template. If a watermark template is not specified, the

		original stream will be recorded.
	Transcoded and watermarked stream	Click **Transcoded and watermarked stream**. You can select an existing transcoding template or click the name of a template to modify its configuration. Videos will be recorded after they are transcoded according to the specified transcoding template. If the template is deleted, the settings for recording watermarked streams will apply.
Record Standby Stream Content		The "Record Standby Stream Content" toggle is displayed only when the Recording Content includes either a Watermarked stream or a Transcoded and watermarked stream. By default, this toggle is set to off. If it is enabled, the recording files will contain the standby stream content. For operations related to standby streams, see Standby streams. Only when you record the watermarked stream, and transcoded and watermarked stream can the recorded files contain standy stream content. If it is not enabled, the recording file will not include the standby stream content.For operations related to standby streams, see Standby streams. **Note:** When utilizing a watermarked stream, the Standby Stream Content may undergo segmented recording due to differences in resolution and encoding methods from the live stream. To circumvent this issue, it is advisable to designate a transcoded stream for recording. This ensures that the Standby Stream Content undergoes transcoding, effectively preventing segmentation and pixelation issues.
Time zone		You can select **UTC+8** or **UTC** . When UTC+8 is selected as the timezone, the naming of the recording files will use the UTC+8 time. When UTC is selected as the timezone, the naming of the recording files will use the UTC time.
Recording Format		Videos can be output in formats of HLS, MP4, FLV, and AAC (for audio-only recording).

Basic Recording Format Configuration Instructions

Note:

Since the recording file is uploaded as it is recorded, it is impossible to ascertain the end time before uploading, preventing the inclusion of the end time in the file name.

Enabling simultaneous recording and uploading ensures files are uploaded immediately after recording ends. A single recording file supports a duration of up to 12 hours and enhances FLV recording's disaster recovery capability.

Playback files may experience lag when being dragged for online playback, but this does not affect local playback.

1. Select the recording content and formats and complete the following settings:

Basic Recording Format Configuration Item	Description
HLS File Segmentation	The HLS file segmentation feature is disabled by default. If post-processing services are needed, it is recommended to enable HLS file segmentation and set the duration of individual HLS recording files. If HLS file segmentation is enabled, the duration of individual HLS recording files can be configured, allowing for the definition of the duration of files produced by post-recording processing. If HLS file segmentation is disabled, recording will continue uninterrupted until the live stream ends. If post-recording processing has been configured, it will be initiated after the recording is complete.
Max Recording Time Per File (min)	Audio/Video - HLS format There is no upper limit on the recording duration of a file in HLS format. If the waiting time for continuation of recording is exceeded, a new recording file will be generated to continue recording. When an HLS recording file is saved to VOD, the duration of a single TS file is set to 60 seconds by default. When HLS file segmentation is enabled, the duration of a single HLS recording file can range from 1 to 720 minutes. Audio/Video - FLV format The duration of a single file recorded in FLV format is limited to 1 to 720 minutes. Audio/Video - MP4 format The duration of a single file recorded in MP4 format is limited to 1 to 720 minutes. Audio-only - AAC Format The duration of a single file recorded in AAC format is limited to 1 to 120 minutes.
Resumption Timeout (sec)	The resumption timeout period directly affects the time it takes to generate a recording file. When the interval of stream interruption does not exceed the set resumption timeout period, a single live stream will generate only one file. However, the recording file will be received after the resumption timeout period has elapsed, and recording costs will be incurred during the resumption timeout period. Please set a reasonable resumption timeout period. **Only HLS format** supports resuming recording after stream interruptions, with the resumption timeout period being configurable from 1 to 1,800 seconds.
Storage Period (days)	You can select Permanent to save a recording file permanently or Custom to specify a storage period (up to 1,500 days). If you set the period to 0, recording files will be saved permanently.

	If a specified time is chosen, in accordance with national regulations, operators must record live video content and ensure storage backup. It is recommended to store recording files for 60 days to 3 years.
VOD Subapplication/Category	Recording to a specified VOD category in VOD application is supported. By default, the recording is stored in the main application of the account, and only applications with an open write status are supported.

2. Click **Save**.

Advanced Recording Format Configuration Instructions

1. You can switch between different tabs to view the configuration requirements for Audio/Video - HLS format, Audio/Video - FLV format, Audio/Video - MP4 format, and Audio-only - AAC format.

Audio/Video - HLS Format

Audio/Video - FLV Format

Audio/Video - MP4 Format

Audio-only - AAC Format

After you select this format, AAC files will be generated when audio-only or quasi-audio/video live streams are pushed.

Advanced Configuration Item	Description
Post-Recording Process Configuration	The post-recording processing feature is disabled by default. You can manually enable this feature based on your business needs. After enabling post-recording processing, no post-recording process content is selected by default. You need to manually select the corresponding process content. When HLS, FLV, MP4, and AAC audio and video formats are enabled with post-recording processing, the on-demand task flow cannot be empty. You can cancel or change the **VOD task flow** . You can click to select the bound task flow and choose a task flow already created under the VOD application, or click the task flow name on the current VOD task flow selection page to go to the VOD console to add/modify the task flow configuration. After the task flow is successfully bound, the VOD task flow template will be executed after the recording file is generated, incurring corresponding video on demand fees.
Upload while recording	The upload while recording feature is disabled by default. You can manually enable this feature based on your business needs.

	Currently, only the FLV format supports the upload while recording feature. Once enabled, it allows immediate upload of files after recording ends, supports a recording file duration of up to 12 hours, and enhances FLV recording's disaster recovery capability. Playback files may experience lag when being dragged for online playback, but this does not affect local playback.

Binding a Domain Name

1. Log in to the CSS console and select **Feature Configuration** > Live Recording on the left sidebar.
Bind a domain to an existing template: Click **Bind Domain Name** in the top left.

Bind a domain after creating a template: After creating a template, click **Bind Domain Name** in the dialog box that pops up.

2. In the pop-up window, select a **recording template** and a **push domain** and then click **Confirm**.

Note:
You can click **Add** to bind multiple push domains to a template.

Unbinding a Domain Name

1. Log in to the CSS console and select **Feature Configuration** > Live Recording on the left sidebar.
2. Select a recording template bound with domain names, find the target domain name, and click **Unbind**.

3. In the pop-up window, click **Confirm**.

Note:
Unbinding a recording template will not affect ongoing live streams.
To cancel recording for ongoing streams, stop the streams and push them again.

Modifying a Template

1. Go to **Feature Configuration** > Live Recording.
2. Select the target recording template, click **Edit** on the right, modify the settings, and click **Save**.

Deleting a Template

Note:

If domain names are bound to a template, you need to unbind them before you can delete the template.

Once a template is deleted, it cannot be restored. Please proceed with caution.

In the console, recording templates are managed at the domain level. To unbind recording rules bound to streams by APIs, call DeleteLiveRecordRule.

1. Log in to the CSS console and select **Feature Configuration** > Live Recording on the left sidebar.
2. Select the target recording template, and click **Delete** in the upper right.

3. In the pop-up window, click **Confirm**.

More

For more information about **binding** and **unbinding** a domain name, see Recording Configuration.

FAQs

How are recording files named?

If a recording template is created in the console, the names of recording files (the names returned by the recording callback) are in the following format:

```
{StreamID}*{StartYear}-{StartMonth}-{StartDay}-{StartHour}-{StartMinute}-{StartSecond}*{EndYear}-{EndMonth}-{EndDay}-{EndHour}-{EndMinute}-{EndSecond}
```

Fields:

Placeholder	Description
{StreamID}	The stream ID.
{StartYear}	The start time - year.
{StartMonth}	The start time - month.
{StartDay}	The start time - day.
{StartHour}	The start time - hours.
{StartMinute}	The start time - minutes.

{StartSecond}	The start time - seconds.
{EndYear}	The end time - year.
{EndMonth}	The end time - month.
{EndDay}	The end time - day.
{EndHour}	The end time - hours.
{EndMinute}	The end time - minutes.
{EndSecond}	The end time - seconds.

Recording to COS

Last updated：2025-05-21 11:12:59

With CSS, you can record a live stream and save the recording file to VOD or COS. This document shows you how to record to Cloud Object Storage (COS).

Notes

To record to COS, you need to activate COS first. We recommend you buy a storage package in advance to avoid service suspension caused by overdue payments. For details, see COS > Getting Started.
After enabling the recording feature, please make sure that your COS service is in normal status. If COS is not activated or is suspended due to overdue payments, live recording will fail. No recording files will be generated. Nor will fees be incurred.
A recording file is available about five minutes after recording ends. For example, if you start recording a live stream at 12:00 and stop at 12:30, you can get the recorded video at around 12:35.
After creating a recording template, you need to bind it to a push domain. For detailed directions, see "Recording Configuration". The template takes effect 5-10 minutes after binding.
Mixed-stream recording does not support mixing streams inside the Chinese mainland with streams outside. Doing so will cause an error and playback of the recording file will fail.
CSS needs permissions to store recording files in COS. Before you use the record-to-COS feature, make sure you have granted the necessary permission. If recording to COS fails due to insufficient permissions, the video cannot be recovered. For how to grant the permission, see "Authorizing CSS to Store Recording Files in COS".
Due to the default traffic and QPS limits of COS storage buckets, if your estimated concurrent push streams exceed 5000, please Submit a Ticket to adjust the QPS limit to avoid affecting the normal use of your business.
If you do not specify a recording template when initiating a recording task, the recording file will be saved to VOD.
When storing recorded content in COS and the storage folder includes the stream ID, please ensure the legality of the stream ID aligns with the naming conventions of COS folders/files to prevent file saving failures. For details on COS object naming conventions, refer to the Naming Conventions Document.

Prerequisites

You have activated CSS and added a push domain.
You have activated COS.

Creating a Recording Template

1. Log in to the CSS console and select **Feature Configuration** > Live Recording on the left sidebar.
2. Select **Save to COS**.

3. Click **Create template** to set the template information and proceed with the following configurations:
Basic recording configuration: This includes the template name, recording content, recording format, and other configuration items. For details, see Basic Recording Configuration Instructions.
Basic recording format configuration: This includes HLS file segmentation, max recording time per file, resumption timeout, and other configuration items. For details, see Basic Recording Format Configuration Instructions.
(Optional) Advanced recording format configuration: By clicking **Advanced Configuration** , you can access and select additional configurations. For details, see Advanced Recording Format Configuration Instructions.
4. Upon completion, click **Save** .

Basic Recording Configuration Instructions

Note:
When recording the original stream via WebRTC streaming, both HLS and MP4 formats can record and play audio normally, but the FLV format will lose audio. It is recommended to select HLS or MP4 format.
When an audio-only transcoding template is selected during specified transcoded stream recording, the HLS/FLV/MP4 recording file will miss the initial 2 seconds of content due to format conversion. Please plan your push and recording schedule accordingly.
Initiating a transcoding task is required for recording transcoded streams, which will incur additional transcoding costs. However, if the same transcoding template is used for playback, charges will not be duplicated.

Basic Configuration Item		Description
Template Name		The template name, which can contain letters, digits, underscores (_), and hyphens (-).
Template Description		The template description, which can be customized and can contain Chinese and English characters, digits, spaces, underscores (_), and hyphens (-).
Recording Content	Original stream	Record videos before transcoding, watermarking, and stream mixing. Please note that for WebRTC streams, recording the original stream may cause audio playback to fail, We recommend you select "Watermarked stream" or "Transcoded and watermarked stream".
	Watermarked stream	Videos will be recorded after they are watermarked according to the specified watermark template. If a watermark template is not specified, the

		original stream will be recorded.
	Transcoded and watermarked stream	Click **Transcoded and watermarked stream** .You can select an existing transcoding template or click the name of a template to modify its configuration. Videos will be recorded after they are transcoded according to the specified transcoding template. If the template is deleted, the settings for recording watermarked streams will apply.
Record Standby Stream Content		The "Record Standby Stream Content" toggle is displayed only when the Recording Content includes either a Watermarked stream or a Transcoded and watermarked stream. By default, this toggle is set to off. If it is enabled, the recording files will contain the standby stream content. For operations related to standby streams, see Standby streams. Only when you record the watermarked stream, and transcoded and watermarked stream can the recorded files contain standy stream content. If it is not enabled,the recording file will not include the standby stream content.For operations related to standby streams, see Standby streams. **Note:** When utilizing a watermarked stream, the Standby Stream Content may undergo segmented recording due to differences in resolution and encoding methods from the live stream. To circumvent this issue, it is advisable to designate a transcoded stream for recording. This ensures that the Standby Stream Content undergoes transcoding, effectively preventing segmentation and pixelation issues.
Time zone		You can select **UTC+8** or **UTC** . When UTC+8 is selected as the timezone, the naming of the recording files will use the UTC+8 time. When UTC is selected as the timezone, the naming of the recording files will use the UTC time.
Recording Format		Videos can be output in formats of HLS, MP4, FLV, and AAC (for audio-only recording).

Basic Recording Format Configuration Instructions

Note:

Since the recording file is uploaded as it is recorded, it is impossible to ascertain the end time before uploading, preventing the inclusion of the end time in the file name.

Enabling simultaneous recording and uploading ensures files are uploaded immediately after recording ends. A single recording file supports a duration of up to 12 hours and enhances FLV recording's disaster recovery capability.

Playback files may experience lag when being dragged for online playback, but this does not affect local playback.

1. Select the recording content and formats and complete the following settings:

Basic Recording Format Configuration Item	Description
HLS File Segmentation	The HLS file segmentation feature is disabled by default. If post-processing services are needed, it is recommended to enable HLS file segmentation and set the duration of individual HLS recording files. If HLS file segmentation is enabled, the duration of individual HLS recording files can be configured, allowing for the definition of the duration of files produced by post-recording processing. If HLS file segmentation is disabled, recording will continue uninterrupted until the live stream ends. If post-recording processing has been configured, it will be initiated after the recording is complete.
Max Recording Time Per File (min)	Audio/Video - HLS format There is no upper limit on the recording duration of a file in HLS format. If the waiting time for continuation of recording is exceeded, a new recording file will be generated to continue recording. When an HLS recording file is saved to COS, the duration of a single TS file is set to 10 seconds by default. When HLS file segmentation is enabled, the duration of a single HLS recording file can range from 1 to 720 minutes. Audio/Video - FLV format The duration of a single file recorded in FLV format is limited to 1 to 720 minutes. Audio/Video - MP4 format The duration of a single file recorded in MP4 format is limited to 1 to 720 minutes. Audio-only - AAC format The duration of a single file recorded in AAC format is limited to 1 to 120 minutes.
Resumption Timeout (sec)	The resumption timeout period directly affects the time it takes to generate a recording file. When the interval of stream interruption does not exceed the set resumption timeout period, a single live stream will generate only one file. However, the recording file will be received after the resumption timeout period has elapsed, and recording costs will be incurred during the resumption timeout period. Please set a reasonable resumption timeout period. **Only HLS format** supports resuming recording after stream interruptions, with the resumption timeout period being configurable from 1 to 1,800 seconds.
Storage path	You can select a COS bucket from buckets that you have created and completed authorization in **Cloud Object Storage** . The region is the region of the mentioned bucket, which cannot be modified.
Backup storage path	The backup storage path feature is disabled by default. You can manually enable this feature according to your business needs.

	When network jitter prevents the recording file from being stored in the primary storage path, the system will automatically store it in the backup storage path to prevent file loss. Once the primary storage path is restored, the recording file in the backup storage path will be automatically synchronized to the primary storage path. The primary and secondary regions cannot be the same.
Folder	The default storage folder is `{RecordSource}/{Domain}/{AppName}/{StreamID}/{RecordId}/{StartYear}-{StartMonth}-{StartDay}-{StartHour}-{StartMinute}-{StartSecond}.` `{RecordSource}` indicates the content type. If the original stream is recorded, this is "origin". If a transcoded stream is recorded, this is the transcoding template ID. `{StartYear}` indicates the starting year. `{StartMonth}` indicates the starting month. `{StartDay}` indicates the starting day. `{StartMinute}` indicates the starting minute. `{StartSecond}` indicates the starting second. `{Domain}` indicates the push domain. `{AppName}` indicates the push path. `{StreamID}` indicates the stream ID. `{RecordId}` indicates the recording task ID, which is returned by the CreateRecordTask API. (/) indicates folder levels. (-) is an ordinary character. `{RandomID}` ：random number

2. Click **Save**.

Advanced Recording Format Configuration Instructions

1. Log in to the CSS console and select **Feature Configuration** > **Live recording** > Save to COS > Create template > Recording Format > Advanced Configuration.

Note:

Prerequisite: Since this is the **first time activating the post-recording MPS feature** , the Cloud Streaming Services console needs to call the Media Processing Service (MPS), requiring you to create a service role and authorize the current account role to use the MPS product.

2. Click **authorize** to enter the CAM role management page.

3. On the role management page, click **Grant** to complete the identity verification and finalize the MPS authorization, enabling normal use of the MPS.

4. After successful authorization, the system will automatically activate the MPS product and display the Save to COS page.
5. Choose **Create template > Recording Format > Advanced Configuration** , and proceed with the following configuration:
5.1 You can switch between different tabs to view the configuration requirements for Audio/Video - HLS format, Audio/Video - FLV format, Audio/Video - MP4 format, and Audio-only - AAC format.
Audio/Video - HLS Format
Audio/Video - FLV Format
Audio/Video - MP4 Format
Audio-only - AAC Format

After you select this format, AAC files will be generated when audio-only or quasi-audio/video live streams are pushed.

Advanced Configuration Item	Description
Post-Recording Process Configuration	The post-recording MPS feature is disabled by default. You can manually enable this feature based on your business needs. After enabling the post-recording MPS, no post-recording process content is selected by default. You need to manually select the corresponding process content. When HLS, FLV, MP4, and AAC audio and video formats are enabled with post-recording processing, MPS orchestration cannot be empty. After enabling the post-recording MPS, you can use the MPS orchestration to transcode, repackage, and perform a series of other post-processing services on the original recording files. The storage setting for the processed files is determined by the MPS orchestration task settings, while the original recording files are still retained. You can cancel or change the **MPS orchestration** . You can **click to select the bound MPS orchestration** and choose an orchestration already created under the MPS orchestration application, or click the orchestration name on the current MPS orchestration selection page to go to the MPS console to add/modify the orchestration configuration. After the orchestration is successfully bound, the MPS template will be executed after the recording file is generated, incurring corresponding Media Processing fees.
Upload while recording	The upload while recording feature is disabled by default. You can manually enable this feature based on your business needs.

	Currently, only the FLV format supports the upload while recording feature . Once enabled, it allows immediate upload of files after recording ends, supports a recording file duration of up to 12 hours, and enhances FLV recording's disaster recovery capability. Playback files may experience lag when being dragged for online playback, but this does not affect local playback.

Binding a Domain Name

1. Log in to the CSS console, select **Feature Configuration** > **Live Recording** on the left sidebar, and click **Save to COS.**
Bind a domain to an existing template: Click **Bind Domain Name** in the top left.

Bind a domain after creating a template: After creating a template, click **Bind Domain Name** in the dialog box that pops up.

2. In the pop-up window, select a **Recording template** and a **Push domain** and then click **Confirm**.

Note:
You can click **Add** to bind multiple push domains to a template.

Unbinding a Domain Name

1. Log in to the CSS console, select **Feature Configuration** > **Live Recording** on the left sidebar, and click **Save to COS**.
2. Select a recording template bound with domain names, find the target domain name, and click **Unbind**.

3. In the pop-up window, click **Confirm**.

Note:
Unbinding the recording template will not affect ongoing live streams.
To cancel recording for ongoing streams, stop the streams and push them again.

Modifying a Template

1. Go to **Feature Configuration** > **Live Recording** and select **Save to COS.**
2. Select the target recording template and click **Edit** on the right to modify the template information.
3. Click **Save**.

Deleting a Template

Note:
If the template has been associated, you need to first unbind it before you can delete it.
Once a template is deleted, it cannot be restored. Please proceed with caution.
The management of recording templates in the console is at the domain name level, and currently, it is impossible to cancel the rules created by the associated interface. If you have associated a specific stream through the recording management interface, you will need to call Delete Recording Rule to unbind it.
1. Log in to the CSS console, select **Feature Configuration** >**Live Recording** on the left sidebar, and click **Save to COS.**
2. Select the target recording template, and click **Delete** in the upper right.

3. In the pop-up window, click **Confirm**.

More

You can also **unbind** and **bind** domains and recording templates on the **Domain Management** page. For details, see Recording Configuration.

Recording Storage to Third Party

Last updated：2025-05-21 11:12:59

Cloud Streaming Services (CSS) provides a feature to record live streams and store recording files to third-party platforms (Amazon S3 and Google Storage). This document describes how to store recording files to third-party platforms.

Notes

The live recording feature is a **paid value-added** service. Before using it, you need to activate the third-party object storage service. Using the live recording feature will incur fees for the peak number of recording channels, fees of recording delivery to third-party services, and fees of storage after recording. For billing rules, see the billing documentation.
During the live streaming process, you can obtain a corresponding file about 5 minutes after the recording ends. For example, if the recording of a live stream starts at 12:00 and ends at 12:30, you can obtain a corresponding clip from 12:00 to 12:30 around 12:35.
After a recording template is successfully created, it can be bound to a push domain name. For more information, see Recording Configuration. The template will take effect approximately 5-10 minutes after it is successfully bound.
If you do not specify a recording template when initiating a recording task, the recording file will be stored to Video on Demand (VOD) by default.

Prerequisites

You have activated CSS and added a push domain name.
You have activated the third-party object storage (Amazon S3 and Google Storage) service.

Creating a Recording Template

1. Log in to the CSS console and go to **Feature Configuration** > Live Recording.
2. In Live Recording, select **Recording Storage to Third Party**.

3. Click **Create Template** to set template information and proceed with the following configurations:
Basic Recording Configuration Instructions: including template name, recording content, recording format, and other configuration items.

Recording Format Configuration Instructions: including HLS file segmentation, max recording time per file, resumption timeout, and other configuration items.
4. Upon completion, click **Save**.

Basic Recording Configuration Instructions

Note:
When the original stream is pushed and recorded via WebRTC, audio can be recorded and played normally for the HLS and MP4 formats, while audio will be lost for the FLV format. It is recommended to choose the HLS or MP4 format.
When an audio-only transcoding template is selected during specified transcoded stream recording, the initial 2 seconds of the recording content in the HLS/FLV/MP4 format will be lost due to format conversion. Please plan your stream pushing and recording time reasonably.
Initiating a transcoding task is required for recording transcoded streams, which will incur additional transcoding costs. However, if the same transcoding template is used for playback, the costs will not be charged again.

Basic Configuration Item		Description
Template Name		Live recording template name, customizable (only Chinese characters, English letters, digits, underscores (_), and hyphens (-) are supported).
Template Description		Live recording template description, customizable (only Chinese characters, English letters, digits, spaces, underscores (_), and hyphens (-) are supported).
Storage Location		You can choose to store data in **Amazon S3** or **Google Storage**.
Recording Content	Original stream	Record videos before transcoding, watermarking, and stream mixing. Please note that for WebRTC streams, recording the original stream may cause audio playback to fail, We recommend you select "Watermarked stream" or "Transcoded and watermarked stream".
	Watermarked stream	Videos will be recorded after they are watermarked according to the specified watermark template. If a watermark template is not specified, the original stream will be recorded.
	Transcoded and watermarked stream	Click **Transcoded and watermarked stream** .You can select an existing transcoding template or click the name of a template to modify its configuration. Videos will be recorded after they are transcoded according to the specified transcoding template. If the template is deleted, the settings for recording watermarked streams will apply.
Record Standby Stream Content		The "Record Standby Stream Content" toggle is displayed only when the Recording Content includes either a Watermarked stream or a Transcoded

	and watermarked stream. By default, this toggle is set to off. If it is enabled, the recording files will contain the standby stream content. For operations related to standby streams, see Standby streams. Only when you record the watermarked stream, and transcoded and watermarked stream can the recorded files contain standy stream content. If it is not enabled,the recording file will not include the standby stream content.For operations related to standby streams, see Standby streams. **Note:** When utilizing a watermarked stream, the Standby Stream Content may undergo segmented recording due to differences in resolution and encoding methods from the live stream. To circumvent this issue, it is advisable to designate a transcoded stream for recording. This ensures that the Standby Stream Content undergoes transcoding, effectively preventing segmentation and pixelation issues.
Time zone	You can choose UTC+8 or UTC. When this parameter is set to UTC+8, the time in the filename will be in UTC+8. When this parameter is set to UTC, the time in the filename will be in UTC.
Recording Format	Videos can be output in the formats of HLS, FLV, MP4, and AAC (for audio-only recording).

Recording Format Configuration Instructions

Note:

Since the recording file is uploaded as it is recorded, it is impossible to obtain the end time before the upload, so that the end time cannot be added to the filename.

Enabling upload while recording ensures files are uploaded immediately after recording ends. A single recording file supports a duration of up to 12 hours and enhances FLV recording's disaster recovery capability. Playback files may experience stutter when being dragged for online playback, but this does not affect local playback.

1. After you check a desired recording format in Recording Content, a settings interface for the format will pop up. You can choose one or more recording formats to set up simultaneously. Complete the following settings:

You can switch between different tabs to view the configuration requirements for Audio/Video - HLS, Audio/Video - FLV, Audio/Video - MP4, and Audio-only - AAC.

Audio/Video - HLS

Audio/Video - FLV

Audio/Video - MP4

Audio-only - AAC

After you select this format, AAC files will be generated when audio-only or quasi-audio/video live streams are pushed.

Basic Recording Format Configuration Item	Description
HLS File Segmentation	The HLS file segmentation feature is disabled by default. If the post-processing service is needed, it is recommended to enable HLS file segmentation and set the duration of individual recording files in the HLS format. If HLS file segmentation is enabled, the duration of individual recording files in the HLS format can be set to define the duration of files generated by post-recording processing. If HLS file segmentation is disabled, recording in the HLS format will continue until the live streaming ends. If post-recording processing is set, it will also be initiated after the recording is complete.
Max Recording Time Per File (min)	Audio/Video - HLS There is no upper limit on the recording duration of a file in the HLS format. In case of exceeding the resumption timeout, a new recording file will be generated to continue recording. When a recording file in the HLS format is stored to COS, the duration of a single TS file is 10 seconds by default. When HLS file segmentation is enabled, the duration of a single recording file in the HLS format can range from 1 to 720 minutes. Audio/Video - FLV The duration of a single file recorded in FLV format is limited to 1 to 720 minutes.. Audio/Video - MP4 The duration of a single file recorded in MP4 format is limited to 1 to 720 minutes. Audio-only - AAC The duration of a single file recorded in AAC format is limited to 1 to 120 minutes.
Resumption Timeout (sec)	The resumption timeout directly affects the time it takes to generate a recording file. When the interval of stream interruption does not exceed the set resumption timeout, only one file will be generated from a single live stream. However, the recording file will be received only after the resumption timeout has elapsed, and recording costs will be incurred during the resumption timeout. Set the resumption timeout reasonably. **Only HLS format** supports resuming recording after stream interruptions, with the resumption timeout period being configurable from 1 to 1,800 seconds.
Sub-Account	You need to fill in **Access Key ID** so that the system can identify and verify the user's identity. You need to fill in **Access Key** to ensure the security of data transmission. Access Key ID and Access Key are crucial credentials for authentication and authorization with cloud service providers (Amazon S3 and Google Storage). They are typically provided by cloud

	service platforms and are used to securely access and manage cloud resources. If you lose or forget this information, follow cloud service providers' instructions to retrieve or reset it.
Storage Path	Enter your bucket information in the Bucket field. Note that it should not exceed 100 characters. Region refers to the geographic location of the said Bucket. Enter your Region information, such as: ap-southeast-1, and ensure it does not exceed 100 characters.
Folder	The default recording storage folder is `{RecordSource}/{Domain}/{AppName}/{StreamID}/{RecordId}/{StartYear}-{StartMonth}-{StartDay}-{StartHour}-{StartMinute}-{StartSecond}`. Its variables are as follows: `{RecordSource}`: recording content, which is origin for the original stream and transcoding template ID for the transcoded stream. `{StartYear}`: start time - year `{StartMonth}`: start time - month `{StartDay}`: start time - day `{StartMinute}`: start time - minute `{StartSecond}`: start time - second `{Domain}`: push domain name `{AppName}`: push path `{StreamID}`: stream ID `{RecordId}`: recording ID, which distinguishes recording rules/recording tasks. In case of a recording task, it shows the task ID (that is, the ID is returned by CreateRecord). (/) indicates a hierarchical relationship and (-) is an ordinary character. `{RandomID}`: random number
Upload while recording	The upload while recording feature is disabled by default. You can manually enable this feature based on your business needs. **Currently, only the FLV format supports the upload while recording feature**. Once enabled, it allows immediate upload of files after recording ends, supports a recording file duration of up to 12 hours, and enhances FLV recording's disaster recovery capability. Playback files may experience stutter when being dragged for online playback, but this does not affect local playback.

2. Just click **Save**.

Binding a Domain Name

1. Log in to the CSS console and go to **Feature Configuration** > Live Recording > Recording Storage to Third Party.

Directly binding a domain name: Click **Bind Domain Name** on the top left.

Binding a domain name after creating a recording template: After successfully creating a recording template, click **Bind Domain Name** in the reminder box.

2. In the domain name binding window, select the **Recording Template** and **Push Domain Name** you need to bind and click **Confirm** to complete successful binding.

Note:
You can click **Add** to bind multiple push domain names to a template.

Unbinding a Domain Name

1. Log in to the CSS console and go to **Feature Configuration** > Live Recording > Recording Storage to Third Party.
2. Select a recording template bound with domain names, select a domain name to unbind, and click **Unbind** on the right.

3. Confirm whether you want to unbind the current bound domain name. Click **Confirm** to unbind it.

Note:
Unbinding the recording template will not affect ongoing live streams.
To make the unbinding take effect, you need to stop live streams and push them again, and no recording file will be generated from new live streams.

Modifying a Template

1. Go to **Feature Configuration** > Live Recording > Recording Storage to Third Party.
2. Select a recording template you have successfully created and click **Edit** on the right to modify template information.

3. Just click **Save**.

Deleting a Template

Note:
If a template has been bound with a domain name, you need to unbind it before deleting it.
Once a template is deleted, it cannot be restored. Please proceed with caution.

The management of recording templates in the console is at the domain name level. Currently, it is impossible to cancel rules created by bound APIs. If you have bound a specific stream through a recording management API, you need to call DeleteLiveRecordRule to unbind it.

1. Log in to the CSS console and go to **Feature Configuration** > Live Recording > Recording Storage to Third Party.
2. Select a recording template you have successfully created and click **Delete** on the top right.

3. Confirm whether you want to delete the current recording template. Click **Confirm** to delete it.

More

You can also **unbind** and **bind** domain names and recording templates. For details, see Recording Configuration.

Time Shifting Template

Last updated：2024-12-31 15:34:25

Time shifting is powered by the recording capability of CSS. It allows users to rewind and play earlier parts of a live stream. This is commonly used to play back highlights of live streamed sports events.

Notes

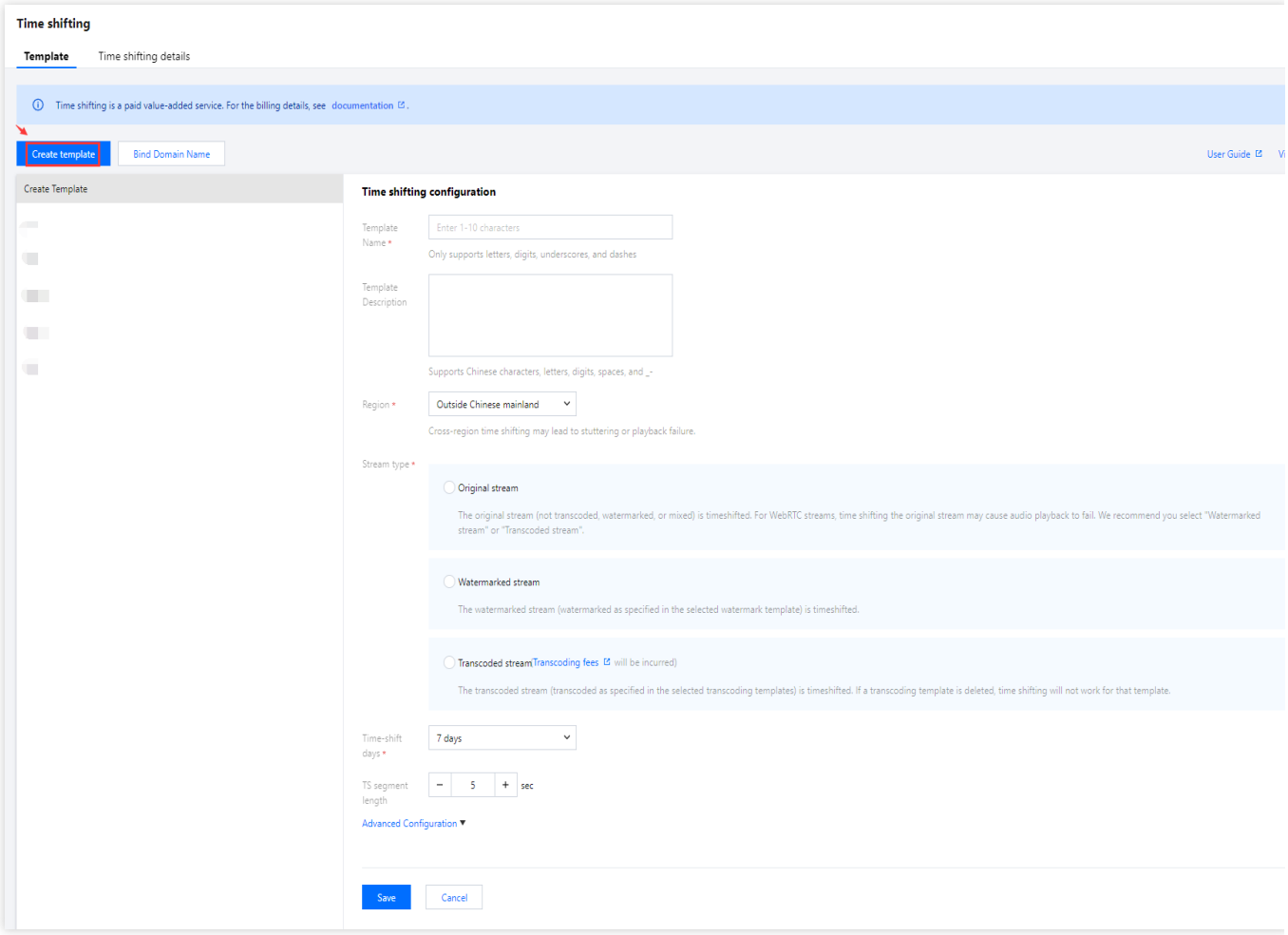
After creating a time shifting template, you need to bind it to a push domain. The configuration takes effect 5-10 minutes after binding.
When enabling the new live time-shifting feature, billing will be based on the Time-shift Data Write Volume. Using the new live time-shifting feature will also generate Live Streaming Traffic Bandwidth Fees and Live Transcoding Fees.
To timeshift a transcoded live stream, you need to configure a transcoding task for the stream in advance. This will incur transcoding fees. Please make sure the transcoding template used is not deleted.
When writing time-shift transcoded stream data, transcoding will be initiated first, generating Live Transcoding Fees. Please make sure that the selected transcoding template has not been accidentally deleted, otherwise, the accidentally deleted time-shift transcoded stream will not be playable. No transcoding fees will be generated when playing the time-shift transcoded stream.

Prerequisites

You have activated CSS and added a push domain name.

Creating a Time Shifting Template

1. Log in to the CSS console and select **Feature Configuration** > Time Shifting on the left sidebar.
2. Click **Create template** to set the template information and configure the following settings:



Item		Description
Template Name		The time shifting template name, which can be 1-10 characters long and can contain Chinese characters, letters, numbers, and _-
Template Description		The introduction and description of the live broadcast time shift template can be customized (only Chinese, English, numbers, spaces, _, - are supported).
Region		By default, outside Chinese mainland, Hong Kong, Macao, and Taiwan regions are supported, with the option to select Chinese mainland. Please bind the correct time-shift playback acceleration region, as cross-regional time-shift playback may result in lagging or inability to pull the stream.
Stream type	Original stream	If you choose this configuration, the time-shift content will not have transcoding, watermark, or mixed-stream effects. For time-shift content with WebRTC push, the audio may not be compatible with some players. It is recommended to choose "Watermarked Stream" or "Transcoded Stream".
	Watermarked stream	The watermarked stream (watermarked as specified in the selected watermark template) is timeshifted.

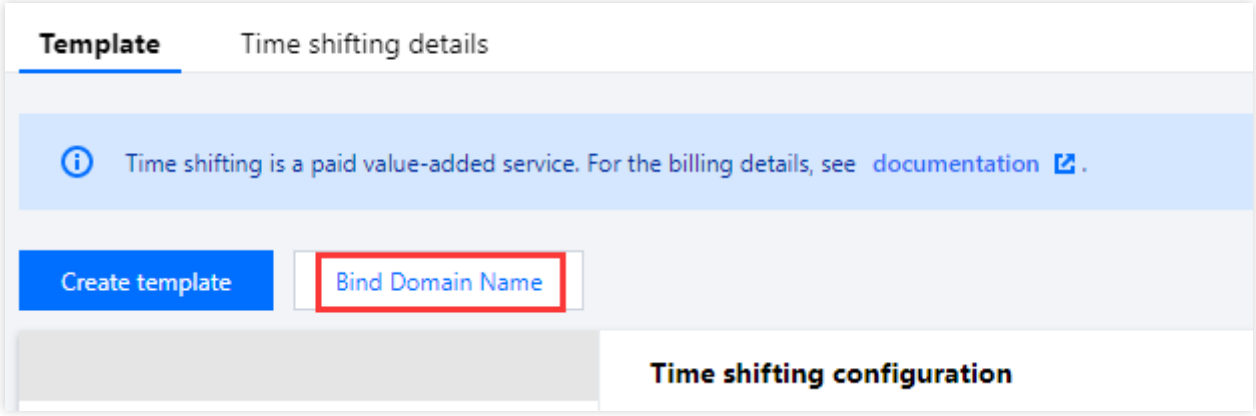
	Transcoded stream	When selecting this configuration, the time-shift video content will be the content after transcoding according to the transcoding template ID. If the transcoding template is deleted, the time-shift playback content will become invalid. Transcoded streams will generate Transcoding Fees.
Time-shift days		The default is 7 days, with options to choose 1 day, 3 days, 15 days, and 30 days.
TS segment length		The default length is five seconds. You can set it to a value between 3 and 10.

3. After completing the input, click **Save** to confirm.

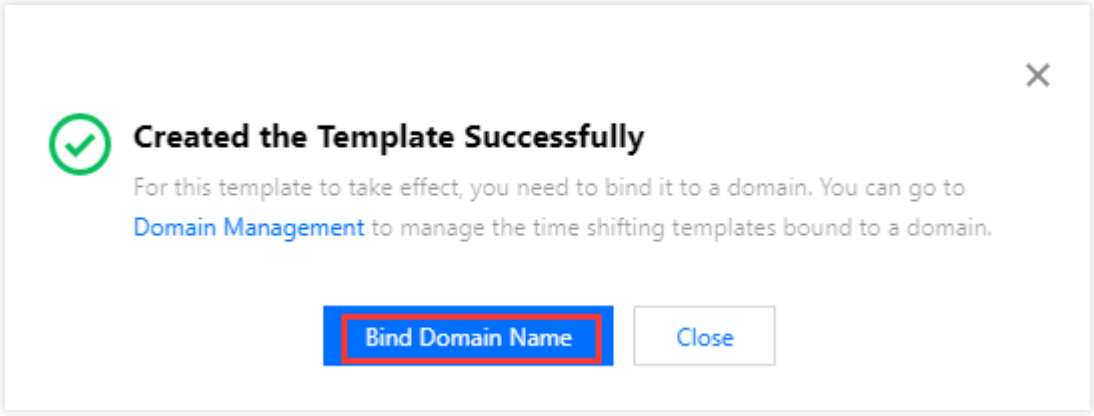
Binding a Domain Name

1. Log in to the CSS console, and select **Feature Configuration** > Time Shifting on the left sidebar.

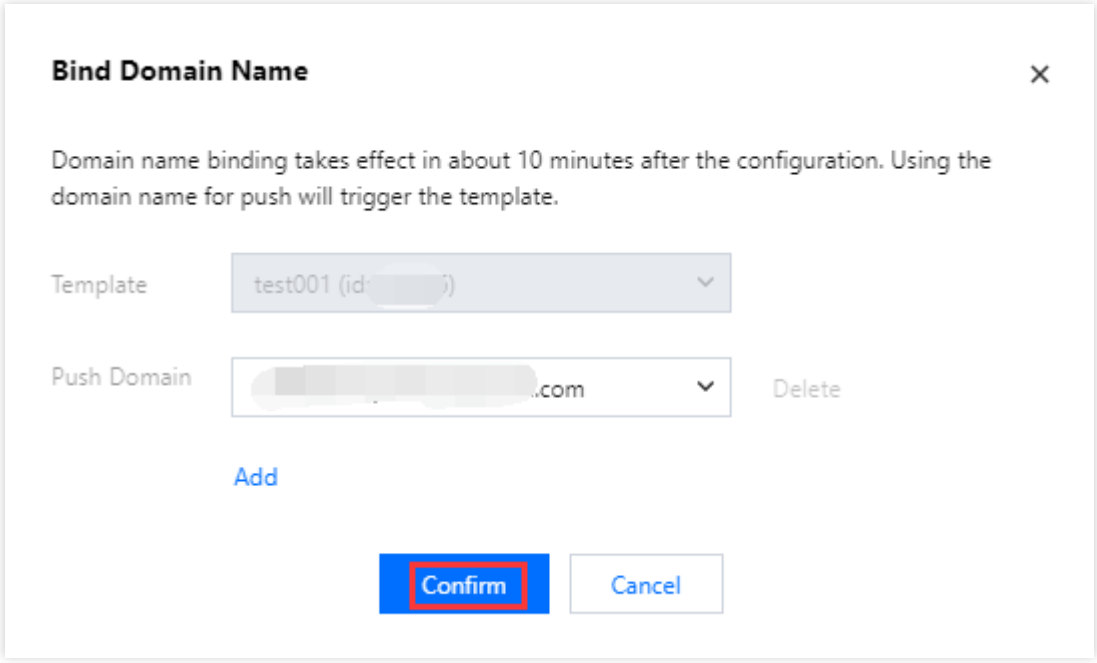
Bind a domain to an existing template: Click **Bind Domain Name** in the top left.



Bind a domain after creating a template: After creating a template, click **Bind Domain Name** in the dialog box that pops up.



2. In the pop-up window, select a **time shifting template** and a **push domain** and then click **Confirm**.

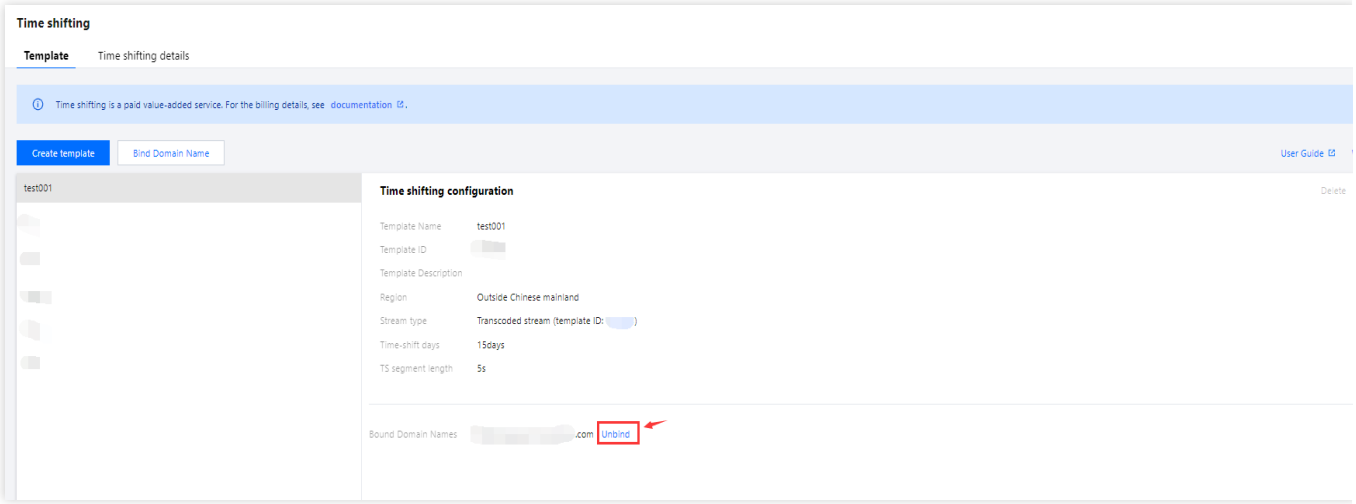


Note：

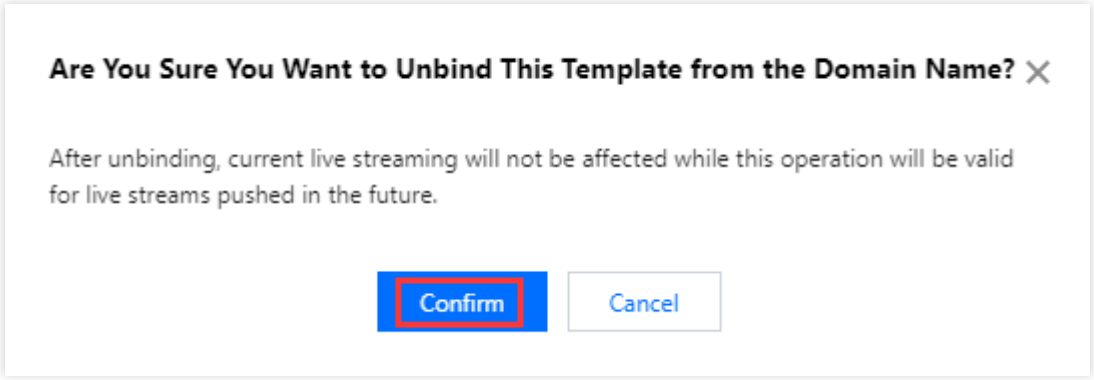
You can click **Add** to bind multiple push domains to a template.

Unbinding a Domain Name

1. Log in to the CSS console, and select **Feature Configuration** > Time Shifting on the left sidebar.
2. Select a time shifting template bound with domain names, find the target domain name, and click **Unbind**.



3. In the pop-up window, click **Confirm**.

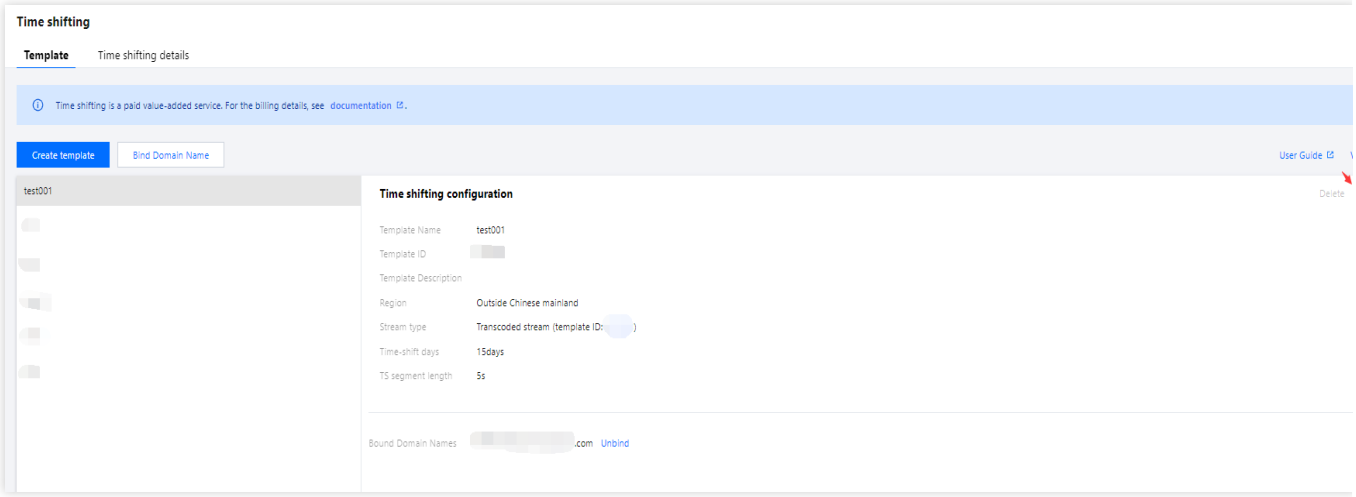


Note：

Unbinding a time shifting template will not affect ongoing live streams.

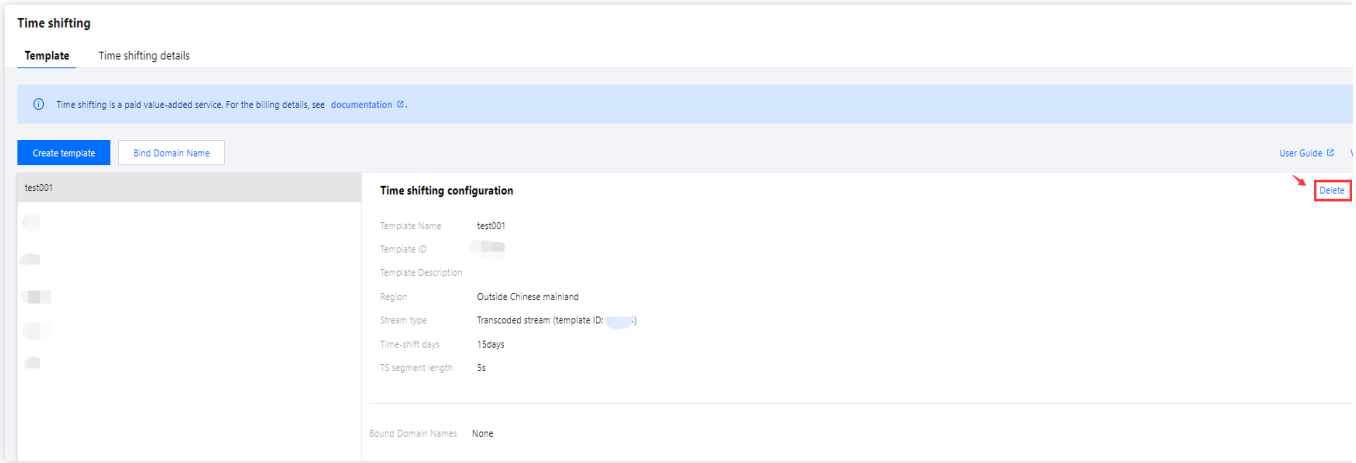
Modifying a Template

1. Go to **Feature Configuration** > Time Shifting.
2. Select the target time shifting template, click **Edit** on the right, modify the settings, and click **Save**.

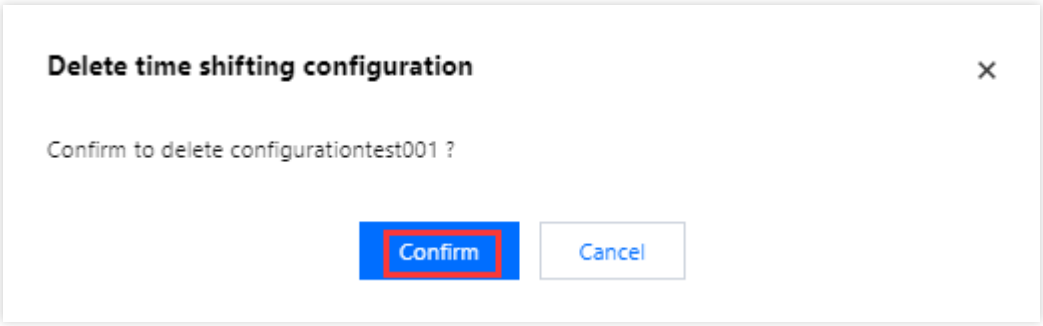


Deleting a Template

1. Log in to the CSS console, and select **Feature Configuration** > Time Shifting on the left sidebar.
2. Select the target time shifting template, and click **Delete** in the upper right.



3. In the pop-up window, click **Confirm**.



Note:

If domain names are bound to a template, you need to unbind them before you can delete the template.

In the console, time shifting templates are managed at the domain level. You cannot unbind time shifting rules bound to streams by APIs.

More

You can also **unbind** and **bind** domains and time shifting templates on the **Domain Management** page. For details, see Time Shifting Configuration.

Time Shifting Details

Last updated：2024-07-16 09:36:23

Tencent Cloud Live Broadcast supports time-shift management through index information, including functions such as viewing time-shift details, configuring time-shift playback, and live broadcast editing.

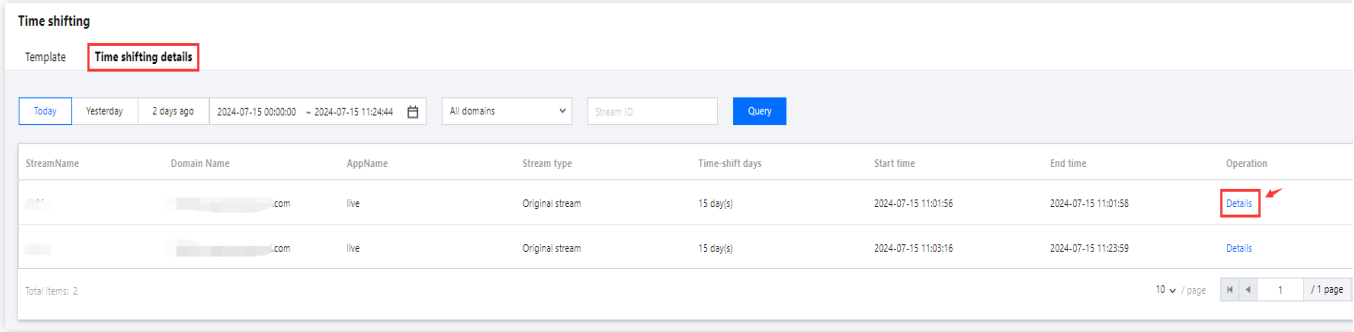
Prerequisites

You have logged in to the CSS console.
You have created a time shifting template, bound it to a push domain, and successfully pushed a stream.
To use the live video editing and solidification capability, please make sure that you have activated the Tencent Cloud MPS. The solidified content will be stored in the COS service, and activating the MPS service will automatically activate the COS service.

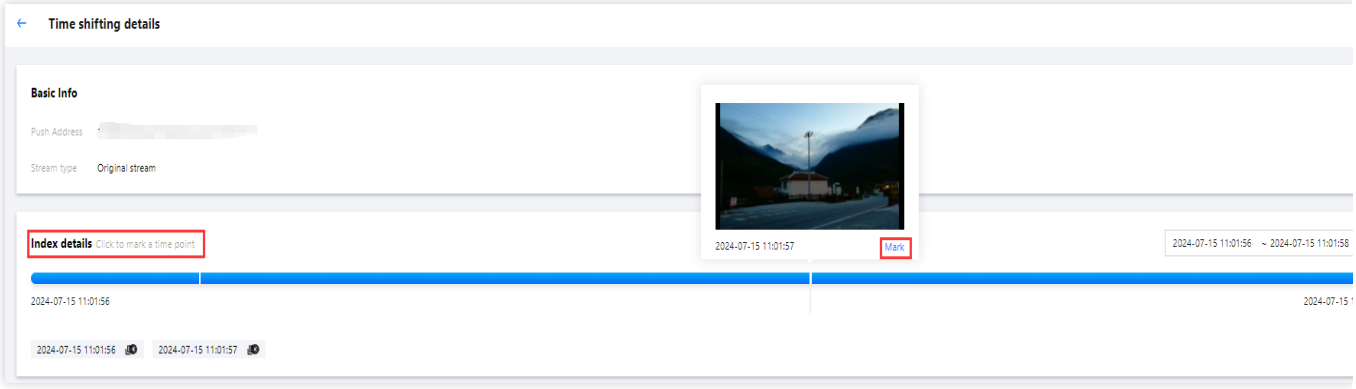
Index Information Operation Guide

Directions

1. Click **Feature Configuration** > **Time Shifting** on the left sidebar and select the Time shifting details tab.
2. Select a domain or enter a stream ID, specify the time period (cannot be longer than 24 hours), and click **Query**.
3. Click **Details** to enter the details page.



4. View the push URL and stream type in the **Basic Info** area.
5. You can move the mouse over the timeline in the **Index Details** page to view the position and time. By clicking on the timeline, you can mark the time.
6. Click the timeline to preview the video at a specific time point and mark that point.



Note:

To preview time-shifted content, the domain used for playback must have an HTTPS certificate. If your playback domain does not have an HTTPS certificate yet, add one in **Domain Management**> Certificate Management. Using the time shifting feature will incur playback traffic/bandwidth fees.

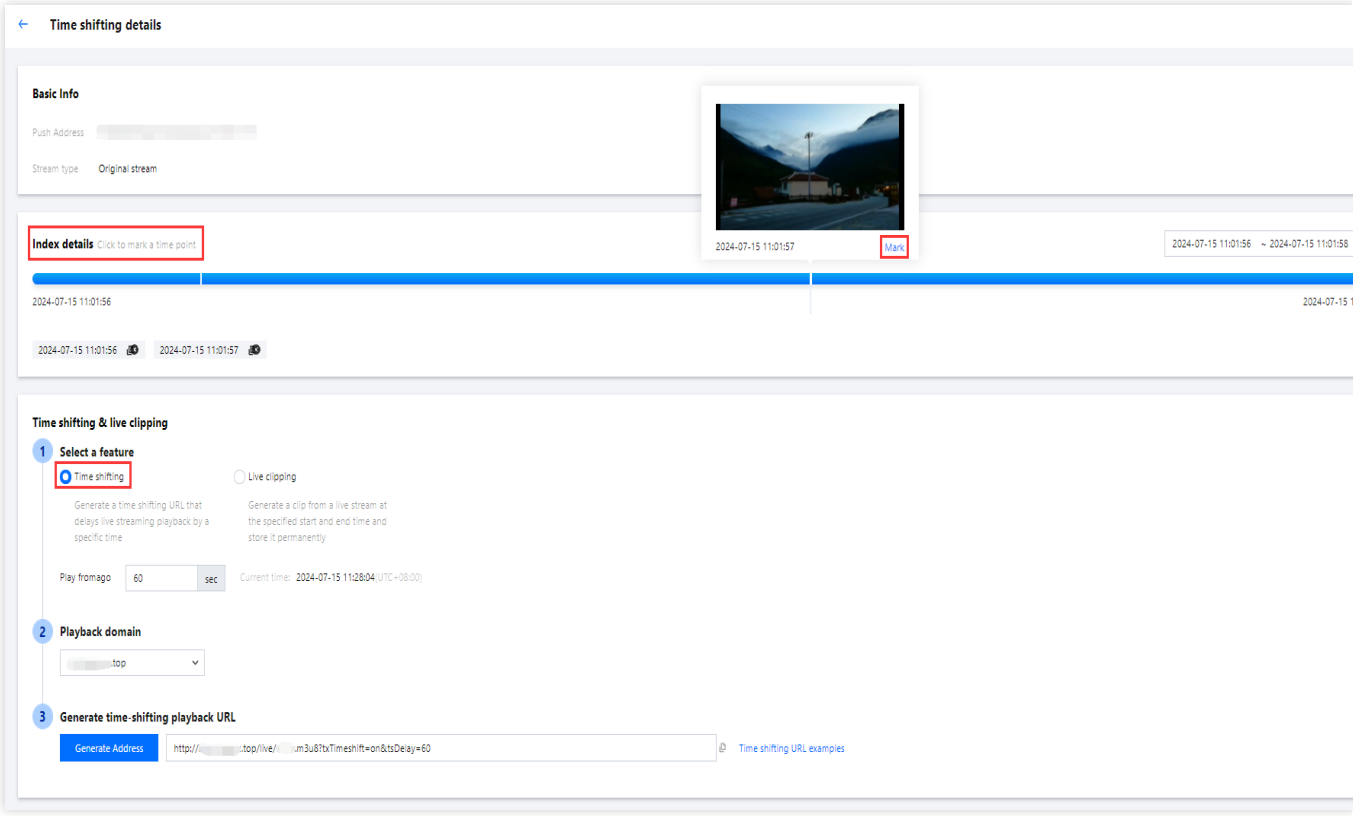
7. **Time Shifting and Live Clipping** can be configured as follows**:**

Item		Description
Select a feature	Time shifting	Generate a time shifting URL that delays live streaming playback by a specific time
	Live clipping	Generate a clip from a live stream at the specified start and end time and store it permanently
Playback domain		Select a playback domain you added to CSS.
Generate time-shifting playback URL		Click **Generate Address** to generate a time-shifting playback URL and copy it.
Navigate to the MPSfor fixed time-shifting content		The encapsulation format can be selected as either **MP4 type** or **HLS type**.

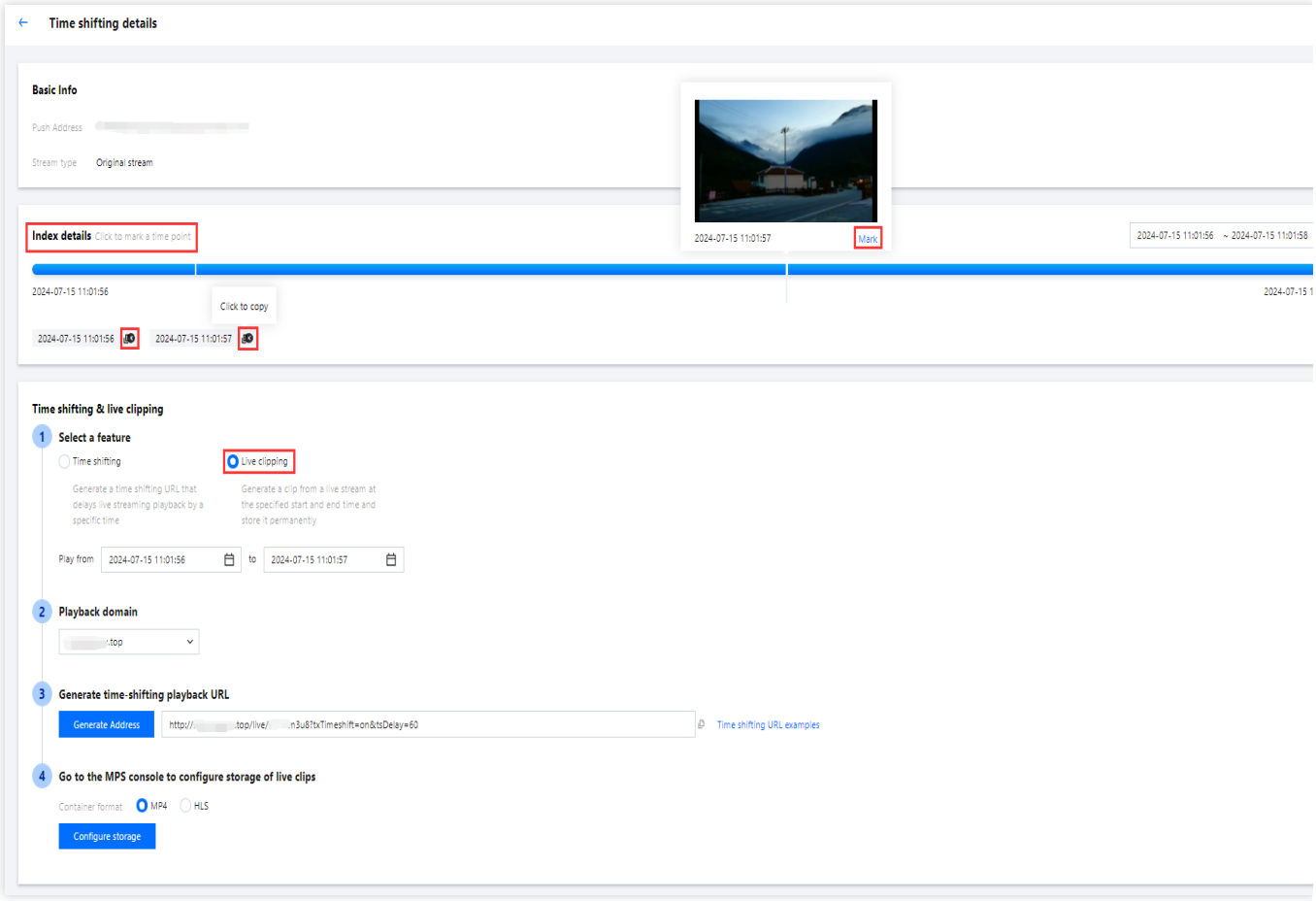
Time shifting

Live clipping

Generate a time shifting URL that delays live streaming playback by a specific time



Generate a clip from a live stream at the specified start and end time and store it permanently



8. Select the function mode as **Live Clipping**. When you have chosen to navigate to the MPS for fixed time-shifting content, click **Configure storage** to enter **MPS** > **Tasks** > VOD. For more details, please refer to the Live Streaming Highlights Clipping document > Create Clip Persistence Task.

Live Screencapture

Last updated：2024-06-25 15:28:19

Cloud Streaming Services (CSS) provides a screenshot feature, supporting the use of screenshot templates configured through the console. After the template is associated with the push domain name, it captures the live streaming screen during the push process and stores the live screenshot data in Tencent Cloud Object Storage (COS). If the push domain name is already associated with a callback configuration, Tencent Cloud will send a request to the customer's server during the live streaming when a callback event is triggered, and the customer's server is responsible for responding to the request. After verification, the customer can obtain a JSON packet containing the screenshot callback information.
This document describes how to create, bind, unbind, modify, and delete screenshot templates through the console.
There are two ways to create a screenshot template:
To create a template via the CSS console, for specific operation steps, see Creating a Screenshot Template.
Call the CreateLiveSnapshotTemplate API to create a template. For information on the parameters and request sample, see CreateLiveSnapshotTemplate.

Must-Knows

The screenshot feature can be used independently, but the porn detection feature can only be enabled after the screenshot feature is enabled and cannot be used independently. Live stream porn detection has been fully upgraded to live stream moderation, which no longer relies on the live screenshot capability. For a better product experience, it is recommended to use the live stream moderation feature. For details, see Live Stream Moderation.
The screencapture and porn detection features are priced at 0.0176 USD and 0.2294 USD per 1,000 screenshots respectively. For details, see Intelligent Porn Detection.
The screenshots and porn detection results are stored in your COS bucket, which will incur COS storage fees. For more information, see COS Pricing.
Screencapturing will fail for audio-only streams, in which case no screencapturing costs will be incurred.
If you want to store the data in a COS bucket of **another account**, you need to first grant CSS the permission to write to that COS bucket. For more information, see Authorizing CSS to Store Screenshots in a COS Bucket.
If your COS bucket allows public read access and has politically sensitive, pornographic, or other inappropriate content, to avoid the bucket being blocked, please delete the content first.
After creating a template, you need to bind it to a push domain. For more information, see Screencapture and Porn Detection Configuration. The configuration takes effect in about 5-10 minutes.
The screenshot template management in the console is at the domain name level and currently, it is not possible to cancel the rules created via API. For screenshot rules bound to specific streams by an API, you need to call DeleteLiveSnapshotRule to unbind them.

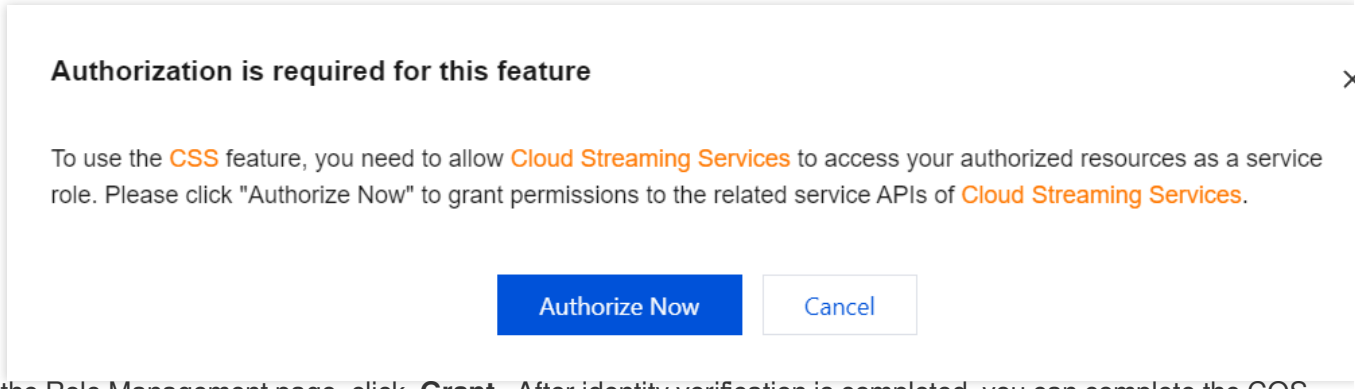
Binding, unbinding, or modifying a template affects only new live streams but not ongoing ones. To apply new rules to ongoing streams, you need to stop them and push them again.

Prerequisites

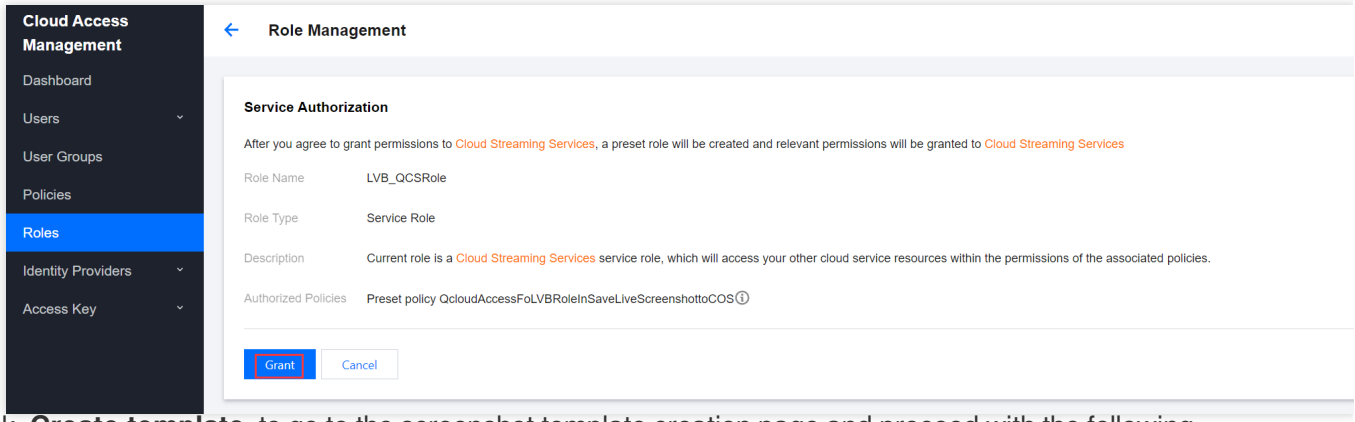
You have activated CSS and added a push domain.
You have created a COS bucket. For detailed directions, see Creating Bucket.

Creating a Screenshot Template

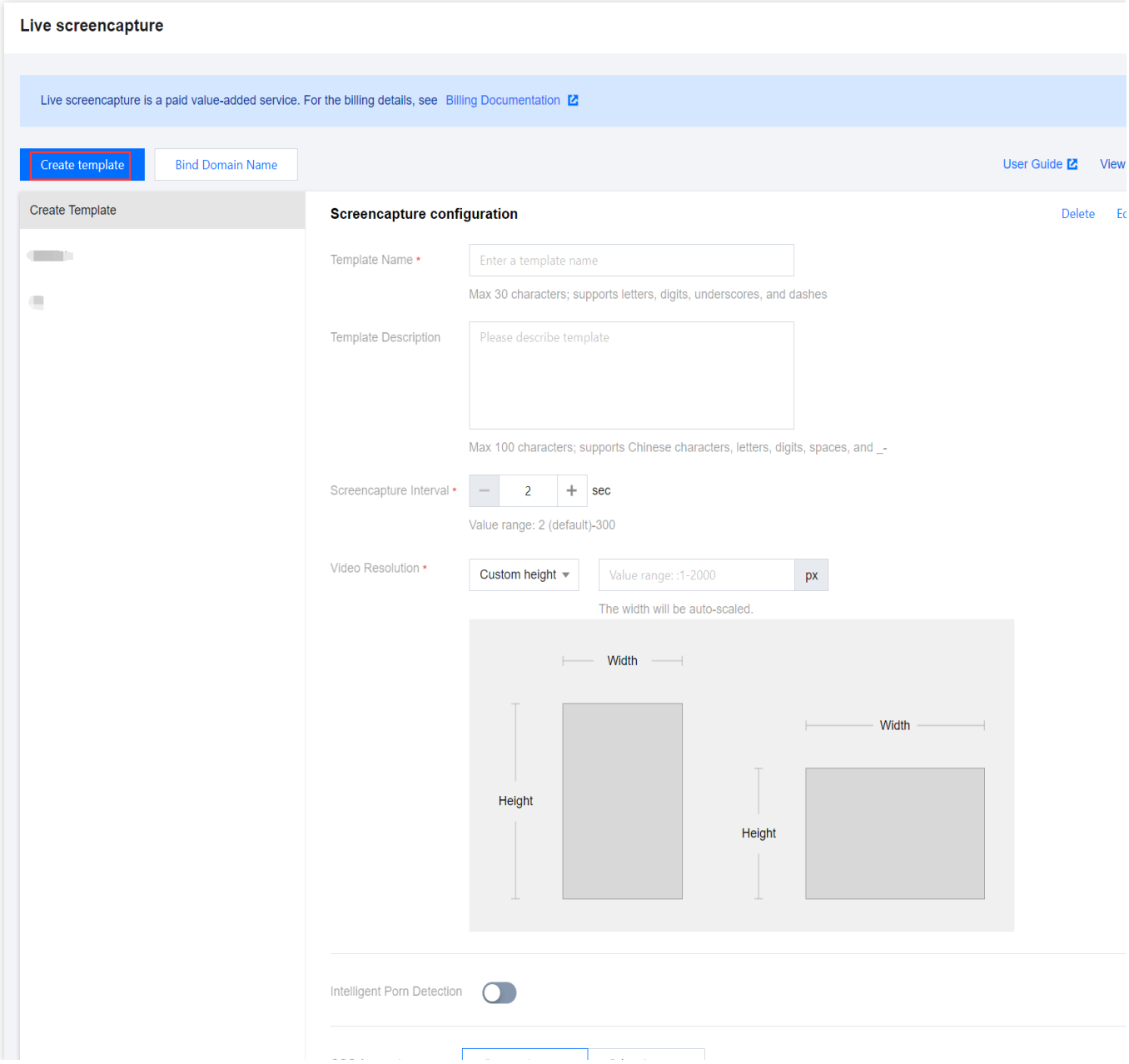
1. Log in to the CSS console, and choose **Feature Configuration** > Live Screencapture.
Note:
Because the CSS screenshot service needs to store screenshots in COS buckets, when creating a screenshot template for **the first time** , you need to create a service role and authorize CSS to have read and write permissions for COS.
2. Click **Create template** .
3. The console will pop up a window to request resource authorization. Click **Authorize Now** to enter the Role Management page.

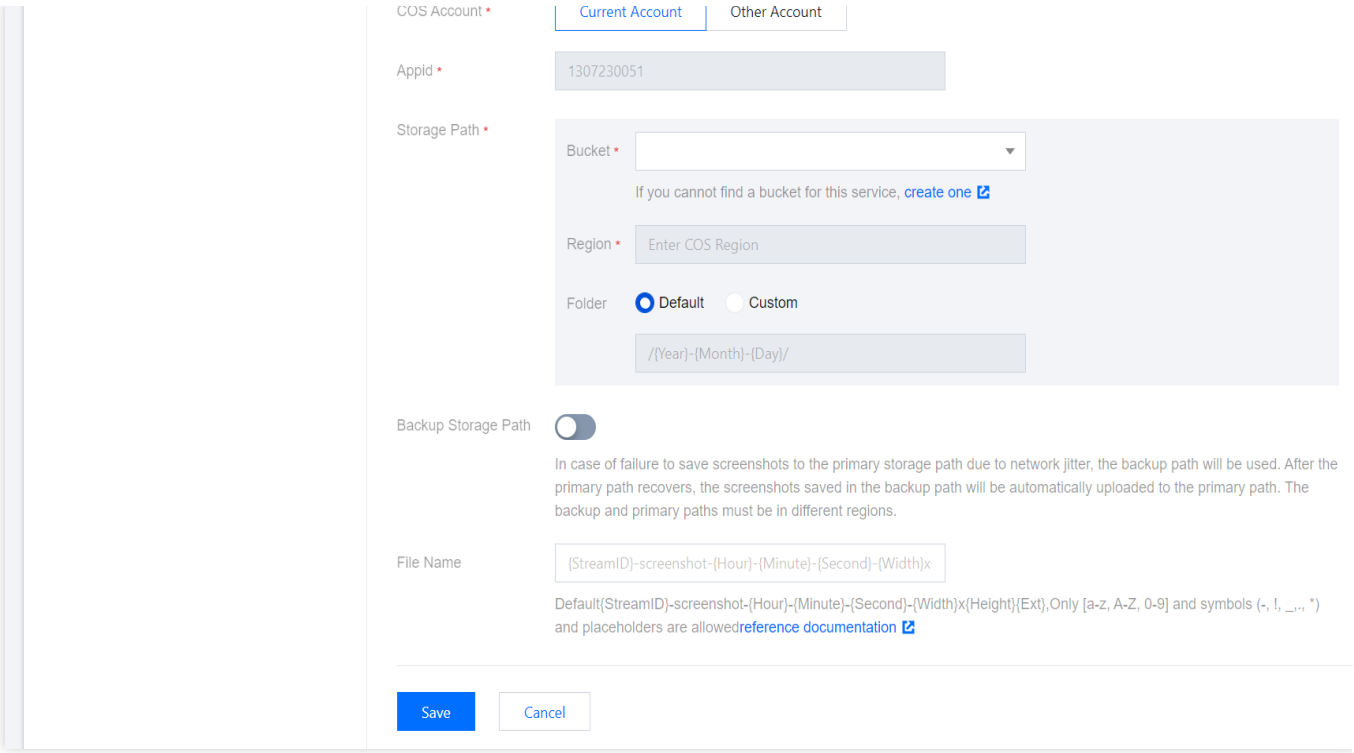


4. On the Role Management page, click **Grant** . After identity verification is completed, you can complete the COS resource authorization and use the live screenshot service normally. Upon successful authorization, you will be redirected to the page for creating screenshot templates.



5. Click **Create template** to go to the screenshot template creation page and proceed with the following configuration:





Configuration Item	Required	Description
Template Name	Yes	The name of the screencapture and porn detection template, which can contain up to 30 Chinese characters, letters, numbers, underscores (_), and hyphens (-).
Template Description	No	Description of the screenshot template, which can contain up to 100 Chinese characters, letters, digits, spaces, underscores (_), and hyphens (-).
Screencapture Interval	Yes	The screencapture interval, which is 2 seconds by default. Value range: 2-300 seconds.
Video Resolution	Yes	By default, the original resolution is maintained, but you have the option to set the screenshot height. The input height range is from 1 px to 2,000 px, and the other side will automatically scale in proportion to the resolution by default.
Intelligent Porn Detection	No	The intelligent porn detection feature is disabled by default and can be enabled manually. After enabling intelligent porn detection, you must configure a callback to receive the results.
COS Account	Yes	**Current Account** or **Other Account.**
AppId	Yes	This is required only if you select **Other Account**. You can view the `APPID` of an account on the Account

			Information page of the console. To save data to a COS bucket of another account, you need to first grant CSS read and write access to that bucket. For details, see Authorizing CSS to Store Screenshots in a COS Bucket.
Storage Path	Bucket	Yes	You can select a COS bucket in Bucket, which you have already created and authorized in **COS** .
	Region	Yes	The region corresponds to the regional information of the aforementioned bucket and cannot be modified.
	Folder	No	Click the box to choose a COS folder. The default is: {Year}-{Month}-{Day}/. Note: COS folder names can only contain [a-z, A-Z, 0-9] and the symbols -, !, _, ., * as well as placeholders.
Backup Storage Path		No	The backup storage path feature is disabled by default. You can manually enable this feature based on your business needs. When network jitter prevents the screenshot from being stored in the primary storage path, the system will automatically store the file to the backup storage path to prevent file loss. Once the primary storage path is restored, screenshots under the backup storage path will be automatically synchronized to the primary storage path. Primary and backup storage paths should be in different regions.
File Name		No	The format of screenshot filenames. You can customize your own format. The default is `{StreamID}-screenshot-{Hour}-{Minute}-{Second}-{Width}x{Height}{Ext}` : {AppName}: The push app name. {PushDomain}: The push domain. {StreamID}: The stream ID. {Year}: The screenshot time (year). {Month}: The screenshot time (month). {Day}: The screenshot time (day). {Hour}: The screenshot time (hour). {Minute}: The screenshot time (minute). {Second}: screenshot time (second) {Width}: The width of the screenshot. {Height}: The height of the screenshot. {Ext}: The extension (.jpg). **Note:** The filename can contain only letters, digits, placeholders, and symbols (-, !, _, ., *).

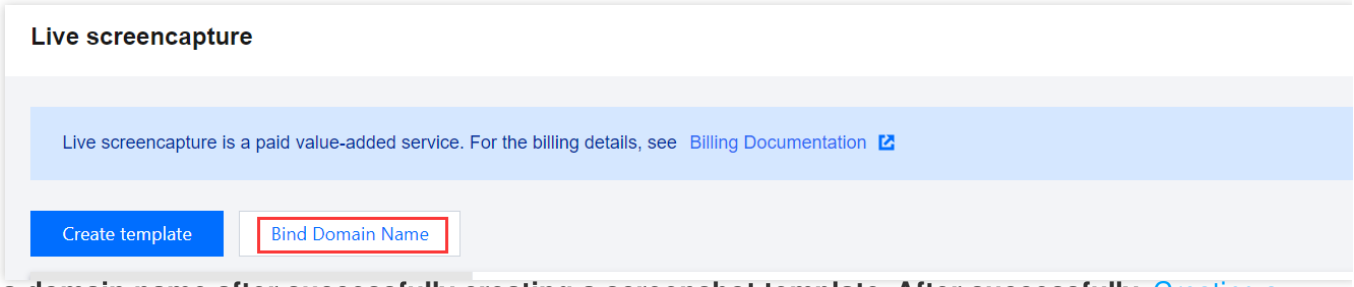
		Example: If the filename format is `{Year}-{Month}-{Day}- {Hour}-{Ext}` , a screenshot captured at 14:00:00 on January 1, 2020 would be named `2020010114.jpg` in COS.

6. Click **Save** to save the current template.

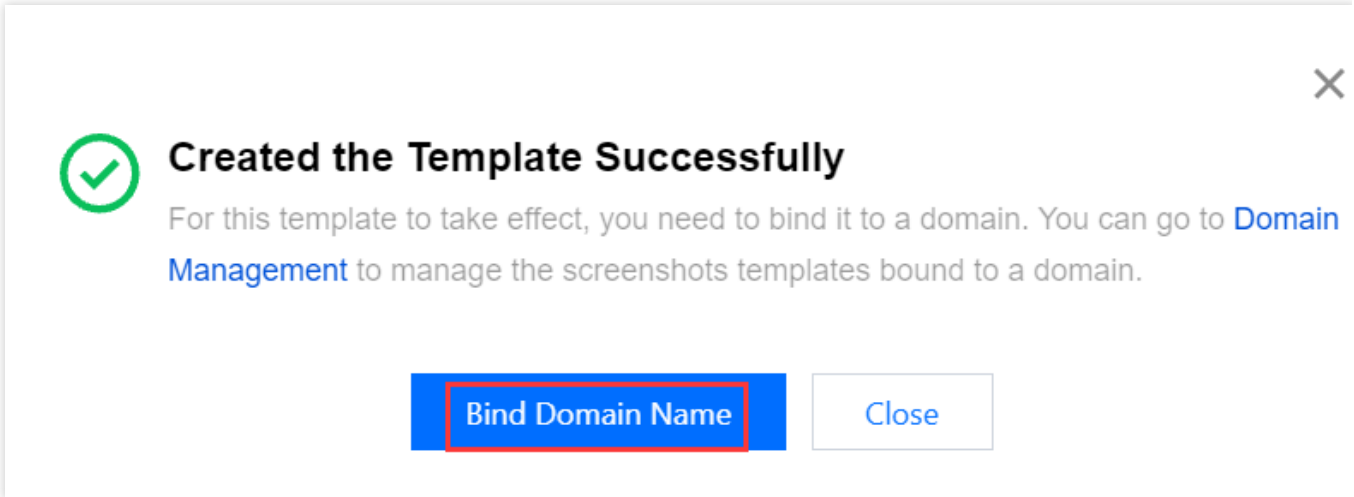
Binding a Domain Name

1. Log in to the CSS console, and choose **Feature Configuration** > Live Screencapture.
2. Bind a domain name in either of two ways:

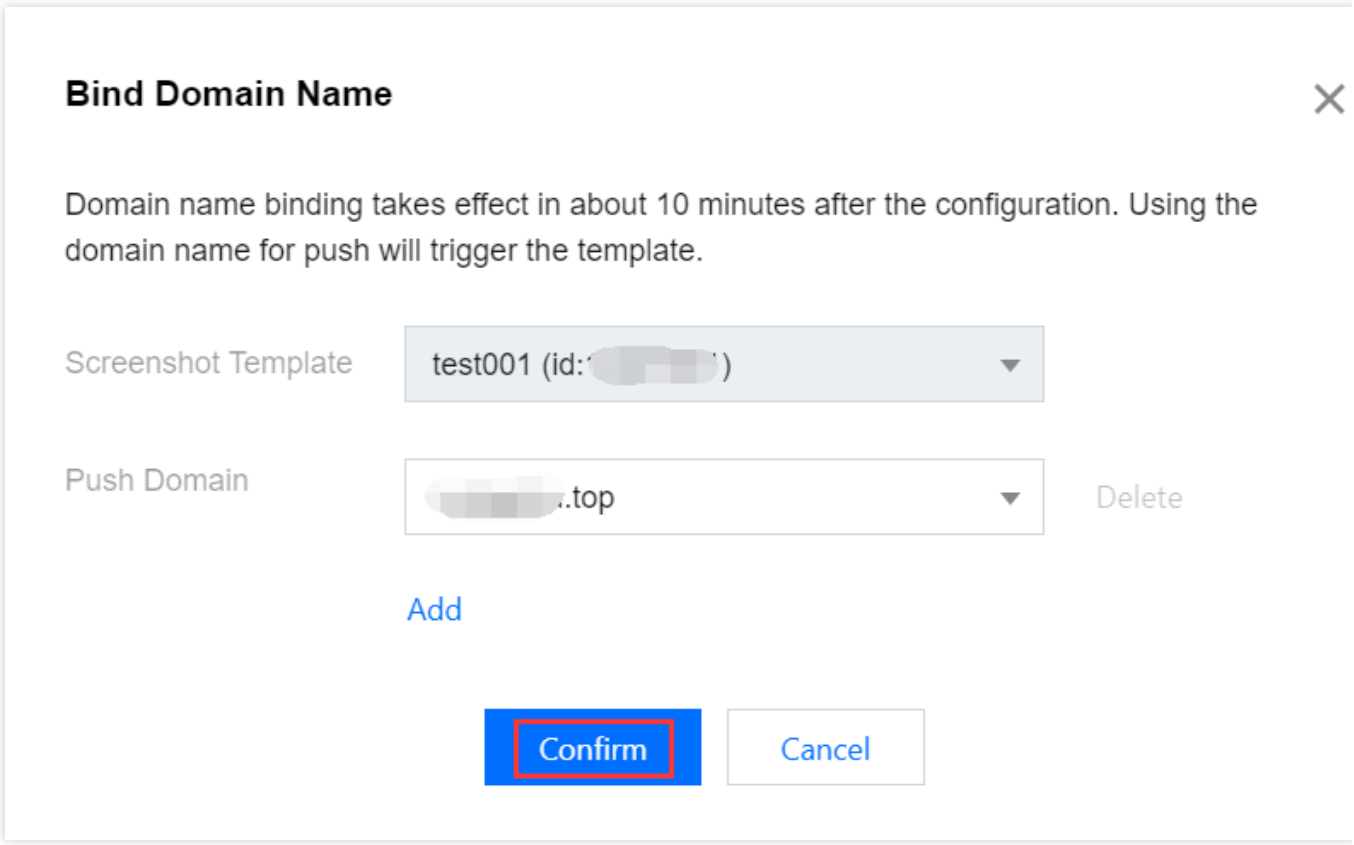
Bind a domain to an existing template: Click **Bind Domain Name** in the top left.



Bind a domain name after successfully creating a screenshot template: After successfully Creating a Screenshot Template, click **Bind Domain Name** in the reminder box .



3. In the domain binding window, select the **screenshot template** and **push domain name** you need to bind, and then click **Confirm** .

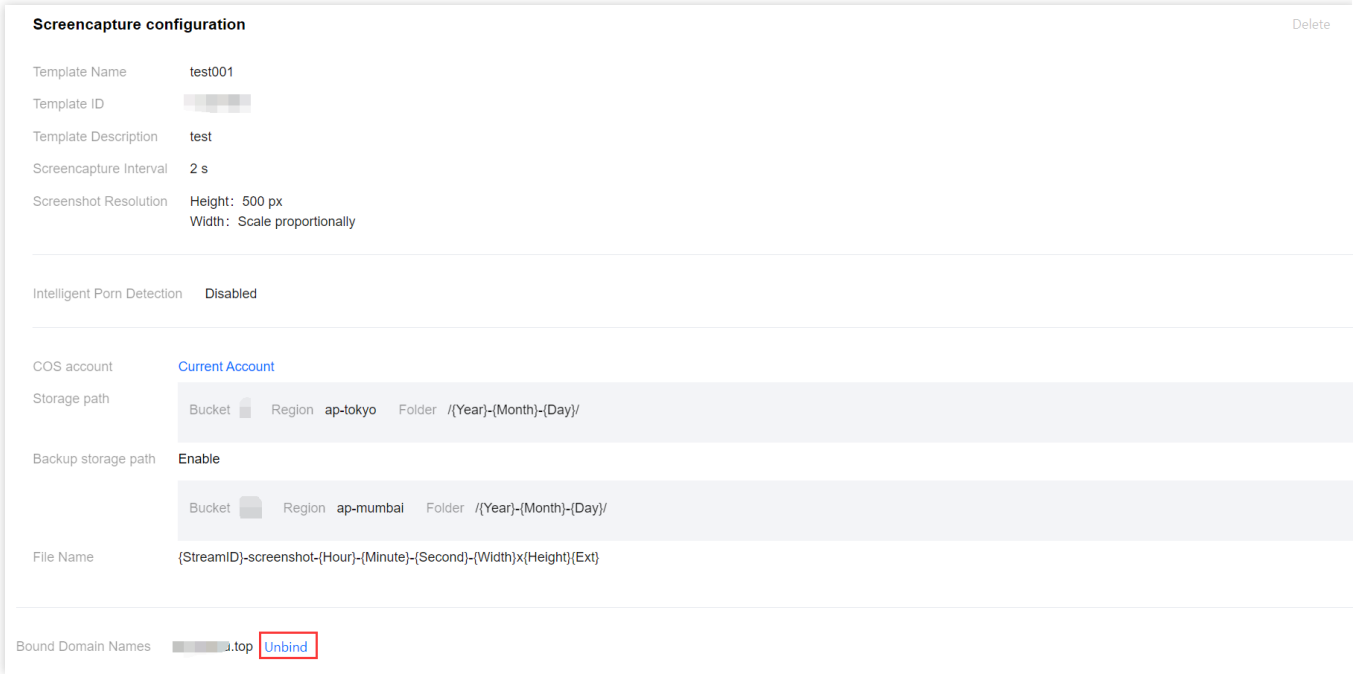


Note:

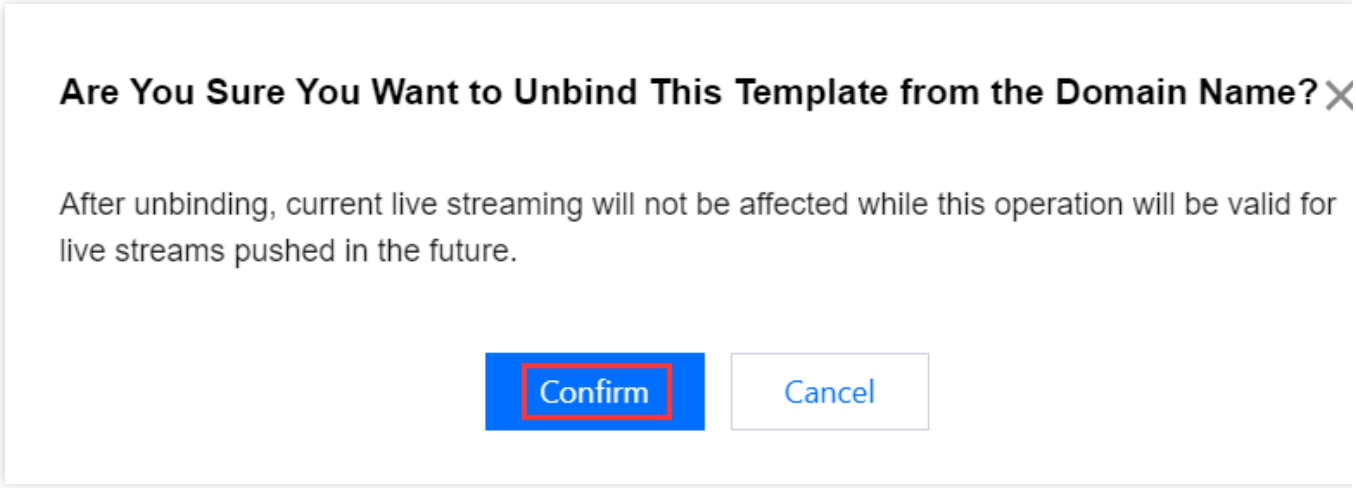
You can click **Add** to bind multiple push domains to a template.

Unbinding a Domain Name

1. Log in to the CSS console, and choose **Feature Configuration** > Live Screencapture.
2. Select the target screencapture and porn detection template, find the domain you want to unbind, and click **Unbind**.

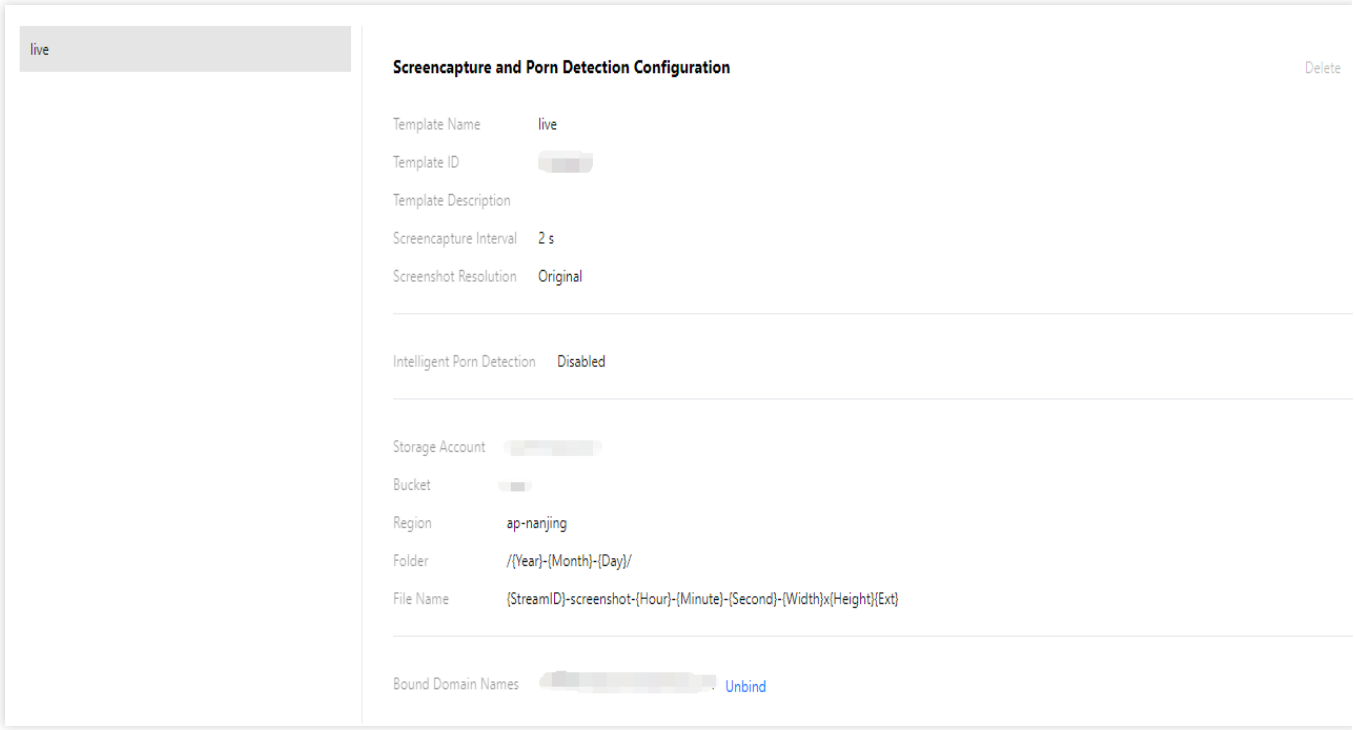


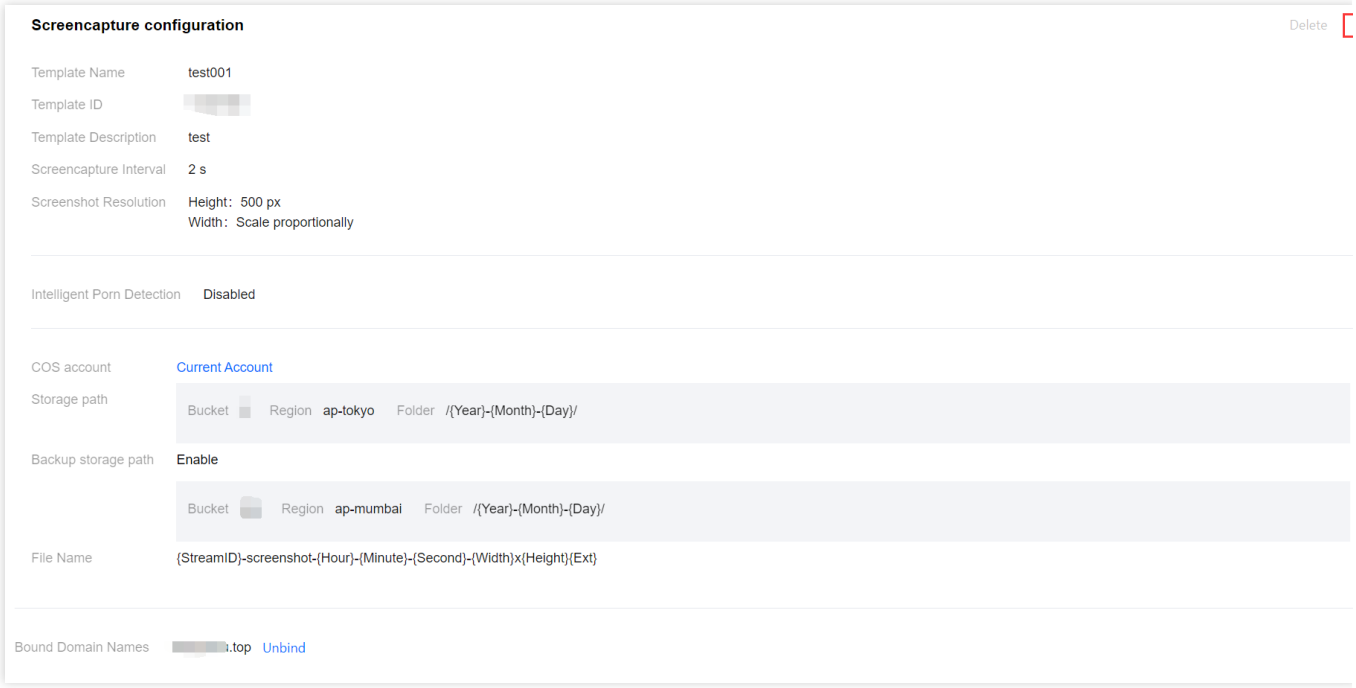
3. In the pop-up window, click **Confirm**.



Modifying a Template

1. Log in to the CSS console, and choose **Feature Configuration** > Live Screencapture.
2. Select a screencapture and porn detection template, click **Edit** on the right, and modify its information.
3. Click **Save**.





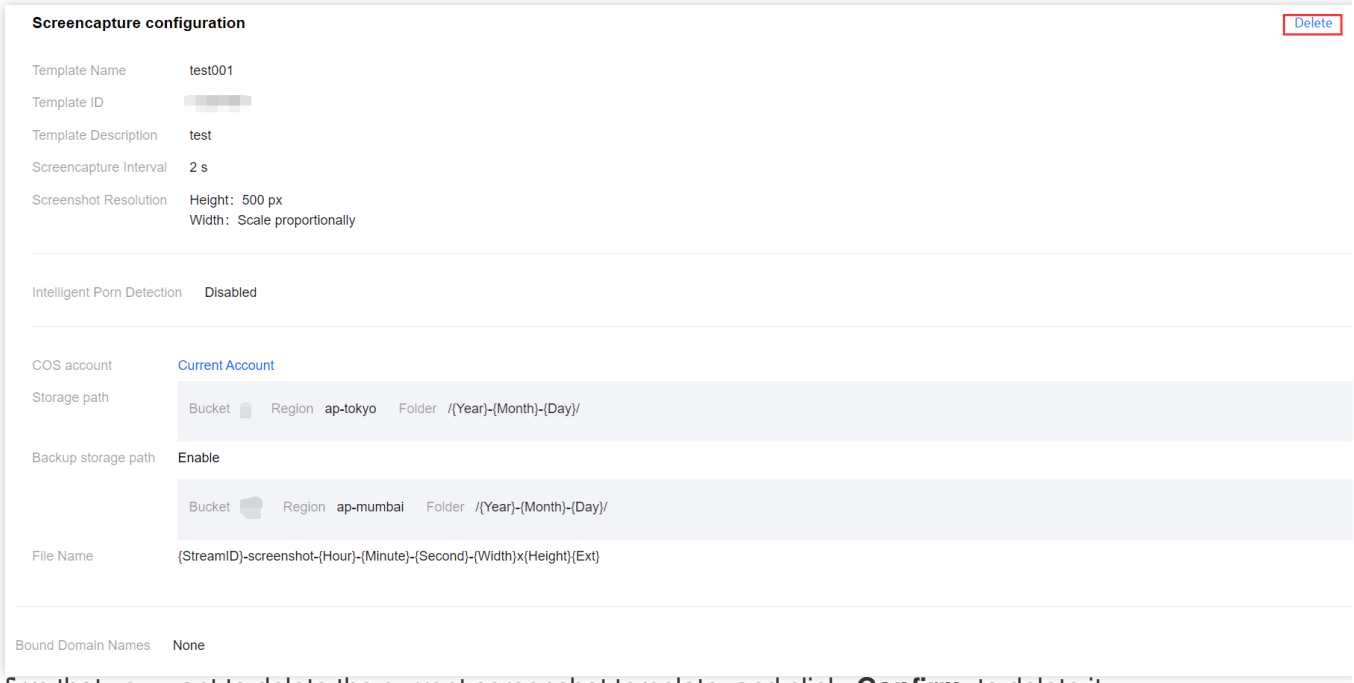
Deleting a Template

Note:

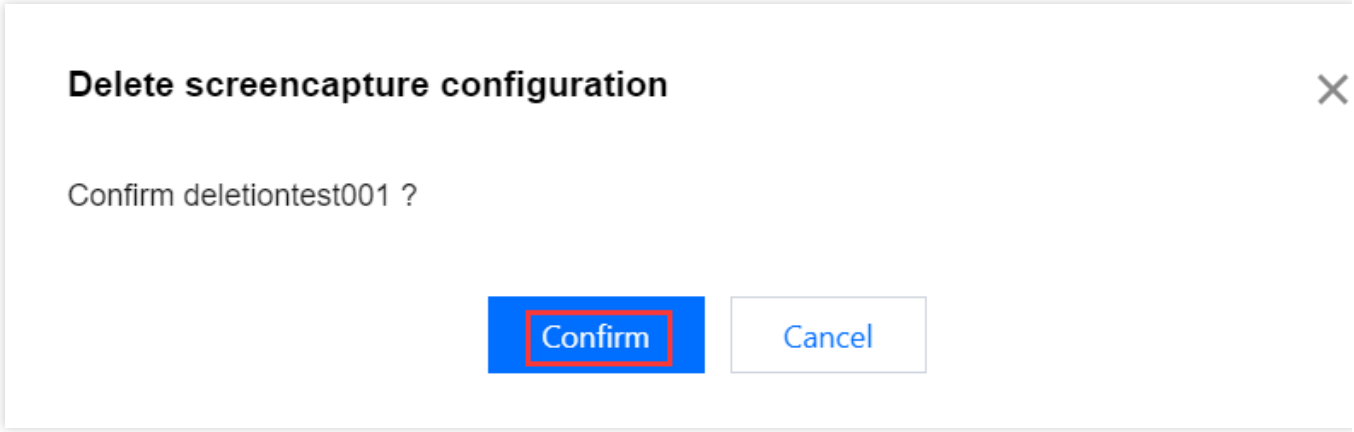
If a template has been bound to domains, you need to unbind them before you can delete the template.

Note that once a template is deleted, it cannot be recovered. Proceed with caution.

1. Log in to the CSS console, and choose **Feature Configuration** > Live Screencapture.
2. Select the screenshot template you have successfully created and click **Delete** above.



3. Confirm that you want to delete the current screenshot template, and click **Confirm** to delete it.



More

For specific operations and related instructions on **binding and unbinding screenshot templates at the domain name level**, refer to Screenshot Configuration.

Live Stream Moderation
Moderation Templates

Last updated：2025-06-04 17:33:12

CSS offers a live stream moderation feature. You can configure moderation templates in the console. Once the streaming domain is associated with the template, this service will obtain live screenshots and the audio during streaming, storing any non-compliant screenshots or audio data in Tencent Cloud COS. If the streaming domain is linked to the callback configuration, Tencent Cloud will send a request to the customer's server once a callback event is triggered during the live stream. Customer's server is responsible for handling the request. After verification, a JSON packet containing the moderation callback information can be obtained. This document provides instructions on how to create, bind, unbind, modify, and delete moderation configuration templates via the console.

Notes

Live stream moderation is a paid feature. Image moderation is charged 0.2294 USD per thousand images, while audio moderation is charged 0.0021 USD per minute. For more information, please refer to Live Stream Moderation.For more information, see Value-Added Services - Live Stream Moderation.
Screenshots or audio flagged during live stream moderation are stored in Tencent Cloud COS, which will generate storage costs. For pricing details, please refer to COS Product Pricing.
If your COS bucket allows public read access and has politically sensitive, pornographic, or other inappropriate content, to avoid the bucket being blocked, please delete the content first.
After a template is created, it can be bound with a push domain. For more information, see Live Stream Moderation Configuration. The association of the template is usually effective within 5-10 minutes.
Binding, modifying, or unbinding a template only affects new live streams and not ongoing ones. To apply new rules to ongoing live streams, you need to stop them and push them again.
To use a custom keyword library for image recognition, make sure "OCR" of "Image recognition" is selected. When OCR is on, the system will moderate the text in video screenshots. OCR-based moderation detects all non-compliant content regardless of the recognition policy configured.

Prerequisites

You have activated the Tencent CSS service and added a push domain.
You have created a COS bucket. For more details, see Creating a Bucket.

Creating Live Stream Moderation Templates

1. Log in to the CSS console and choose **Feature Configuration** > **Content moderation** from the left navigation bar.

Note:

CSS stores video screenshots and audio data in COS buckets. Therefore, if it's your first time creating a moderation template, you need to create a service role and grant CSS read and write access to COS.

2. Click **Create template**.

3. A pop-up window will appear for you to grant CSS authorization to access COS resources. Click **Authorize Now** to go to the **Role Management** page.

4. On the **Role Management** page, click **Grant**. After authentication, CSS will have access to COS resources, and you can start using the live stream moderation feature.

5. After authorization, you will be redirected to the Create template page, where you can fill in the configuration items.

Steps

Step 1: Configuring Moderation

Click **Create template** to configure moderation:

Configuration Item	Description
Template Name	The template name can include up to 30 Chinese characters, letters, digits, underscores (_), and hyphens (-).
Template Description	The template description can include up to 100 Chinese characters, letters, digits, spaces, underscores (_), and hyphens (-).

Step 2: Configuring Screencapture/Segment Policy

In Screencapture/Segment policy, you can configure what content you want to moderate.

Configuration Item	Required Item	Description

Content type to moderate	Yes	Screenshot images Screencapture interval: The interval at which screenshots are taken during a live stream. The shorter the interval, the finer the moderation granularity, and the higher the cost. The screencapture interval can be 2-300 seconds. The default value is 2 seconds. Audio The audio moderation feature only supports Chinese audio. Audio segment duration refers to the length of each audio segment extracted from a live stream. It determines the duration of the non-compliant audio segments returned and does not affect billing. The audio segment duration can be 15-60 seconds. The default value is 15 seconds. Audio text recognition Audio text recognition is only used for features such as smart erase but will not trigger review.The Smart Erase feature utilizes its configured policies to identify and eliminate audio content that violates regulations.

Step 3: Configuring Recognition Policy

1. On the recognition policy configuration page, you can configure policies for both **Image Recognition** and **Audio Recognition**.

2. You can expand each category of **Image Recognition** and **Audio Recognition** to select sub-categories for moderation.

Note:

The system will recognize and perform moderation on the content according to the categories you select. If no categories are selected, no recognition or moderation will be performed.

To use a custom keyword library for image recognition, make sure "OCR" of "Image recognition" is selected.

Image Recognition Configuration

Audio Recognition Configuration

Audio text recognition configuration

3. From the drop-down list of custom keyword libraries, you can select a custom library to use for image recognition or audio recognition.

Note:

If you need to use a custom keyword library for content recognition, you need to configure one in the console first. For more information, see Custom Keyword Libraries.
4. Configure the storage path for saving screenshots or audio for moderation. Then, click **Save** to save the moderation template.

Configuration Item	Required Item	Description
Storage Location	–	The screenshot will be stored in your configured COS bucket, and make sure that the COS bucket has authorized CSS write request. Please create a COS bucket and authorize, reference documentation.
Storage path	Yes	Choose a COS bucket that you have created and authorized in COS. Region refers to the geographic information of the selected bucket, which cannot be edited.
Backup storage path	No	Backup storage is supported. If the primary bucket does not work properly, the moderation content will be automatically stored in the backup bucket. The backup bucket will be used only if the primary bucket is down, and only one copy of data will be stored. The primary Region and backup Region cannot be identical.
Folder	Yes	Click the input box to select a COS folder. The default is `/Audit/{Year}-{Month}-{Day}/` . Note: COS folder names only allow `[a-z, A-Z, 0-9]` characters and the symbols `-,!, _,., *` along with placeholders.
File Name	Yes	The file name format can be customized through parameter assembly. Default is: {StreamID}-Audit-{Hour}-{Minute}-{Second}{Ext}, wherein: {StreamID}: Stream ID {Audit}: Moderation {Hour}: Moderation time (Hour) {Minute}: Moderation time (Minute) {Second}: Moderation time (Second) {Ext}: Extension (.jpg) Note: It only accepts [a-z, A-Z, 0-9], symbols `-,!,_,.,*` , and placeholders. For example, if you enter the file format as {Hour}-{Minute}-{Second}-{Ext}, a screenshot taken during a live stream at 14:00:00 will be stored in COS with the filename `140000.jpg` .

Binding Domain Names

1. Log in to the CSS console and choose **Feature Configuration** > **Content moderation** from the left navigation bar.
2. You can bind the moderation template to a push domain with the following methods:
Directly bind a domain: Click **Bind Domain Name** in the top left.

Bind a domain after creating a new moderation template: After successfully creating a moderation template, click **Bind Domain Name** in the pop-up window.

3. In the **Bind Domain Name** window, select the moderation template and push domain you want to bind together, and click **Confirm** to bind them.

Note:
You can click **Add** to bind multiple push domains to the current template.

Unbinding

1. Log in to the CSS console and choose **Feature Configuration** > **Content moderation** from the left navigation bar.
2. Select the live stream moderation template from which you want to unbind the push domain and click **Unbind**.

3. In the pop-up window, click **Confirm**.

Modifying a Template

1. From the left navigation bar, choose **Feature Configuration** > **Content moderation**.
2. Select the successfully created moderation template, click **Edit** on the right to go to modify the template information.

Deleting a Template

Note:
If the template is already bound to a push domain, you must first unbind it before the template can be deleted.

A deleted template cannot be recovered. Proceed with caution when deleting templates.

1. From the left navigation bar, choose **Feature Configuration** > **Content moderation**.
2. Select a previously created moderation template and click **Delete**.

3. Click **Confirm** to permanently delete the template.

Related Operations

For detailed instructions and additional information on binding and unbinding moderation templates at the domain level, please refer to Moderation Configuration.

Smart Erasing

Last updated：2025-06-19 15:10:02

The Smart Erasing feature allows users to configure Smart Erase templates via the console. Once a Push Domain is linked to a template, it captures audio during streaming, identifies inappropriate content, and mutes it accordingly, ensuring a positive and well-maintained live streaming environment.
This document describes how to create, modify, and delete smart erase templates through the console.

Notes

After a template is created, it can be bound with a push domain. For more information, see Smart Erase Configuration.
The association of the template is usually effective within 5-10 minutes.
Binding, modifying, or unbinding a template only affects new live streams and not ongoing ones. To apply new rules to ongoing live streams, you need to stop them and push them again.
The Smart Erasing feature is a premium service. Utilizing the Smart Erasing functionality incurs additional charges for live streaming value-added services and intelligent recognition fees under MPS., please refer to billing document.

Prerequisites for Use

The CSS service has been activated.

Creating Smart Erase Template

1. Log in to the CSS console. Choose **Feature Configuration** > **Content moderation** > **Smart Erasing.**
Note:
Due to the use of the smart erase function, creating a service role and authorizing the current account role to use MPS product services are required for the **first** creation of a smart erase template.
2. Click **Grant access** to enter the CAM role management page.
3. On the role management page, click **Grant**. After completing identity authentication to finish the MPS authorization, you can utilize the MPS service normally.

4. After successful authorization, select the service agreement and click **Start**. The system will automatically activate the MPS product and open the Smart Erasing management page.
5. Click **Create template** to enter the smart erase template creation page and configure the template as follows:

Configuration Item		Description
Template Name		Max 30 characters; supports letters, digits, underscores, and dashes.
Template Description		Max 100 characters; supports Chinese characters, letters, digits, spaces, and `_-` .
Recognition Scheme	Erasing Type	Non-compliant audio, Recognize non-compliant text content in the live streaming audio and mute the corresponding audio segments to effectively guarantee live streaming content security. The development of erasure types for non-compliant images, logos, and privacy protection content is currently underway. Please stay tuned.
	Non-compliant Audio Recognition Scheme	Bind a template in the live stream moderation module with Audio text recognition selected for Moderation Content Configuration.You can configure the inappropriate text content you wish to erase in the form of a custom vocabulary within the Audio Text Recognition policy.
Output Information		Output Content is Audio after erasing

Binding Domain Names

1. Log in to the CSS console and choose **Feature Configuration** > **Content moderation** > **Smart Erasing** from the left navigation bar.
2. You can bind the moderation template to a push domain with the following methods:
Directly bind a domain: Click **Bind Domain Name** in the top left.

Bind a domain after creating a new smart erase template: After successfully creating a smart erase template, click **Bind Domain Name** in the pop-up window.

3. In the **Bind Domain Name** window, select the **smart erase template** and push domain you want to bind together, and click **Confirm** to bind them.

Note:
You can click **Add** to bind multiple push domains to the current template.

Unbinding

1. Log in to the CSS console and choose **Feature Configuration** > **Content moderation** > **Smart Erasing** from the left navigation bar.
2. Select the smart erase template from which you want to unbind the push domain and click **Unbind**.

3. In the pop-up window, click **Confirm**.

Modifying a Template

1. From the left navigation bar, choose **Feature Configuration** > **Content moderation>Smart Erasing**.
2. Select the successfully created smart erase template, click **Edit** on the right to go to modify the template information.

Deleting a Template

Note:
If the template is already bound to a push domain, you must first unbind it before the template can be deleted.
A deleted template cannot be recovered. Proceed with caution when deleting templates.
1. From the left navigation bar, choose **Feature Configuration** > **Content moderation** > **Smart Erasing**.
2. Select a previously created smart erase template and click **Delete**.

3. Click **Confirm** to permanently delete the template.

Related Operations

For detailed instructions and additional information on binding and unbinding Smart Erase templates at the domain level, please refer to Smart erase configuration。

Custom Keyword Library

Last updated：2025-06-04 17:33:55

You can use a custom keyword library for image and audio moderation. A custom library may contain keywords to allow or block. The configuration takes effect within 10 minutes.

Creating a New Library

1. Log in to the CSS console and navigate to Feature Configuration > Content moderation > **Keyword libraries**.
2. Click **Create library**. In the pop-up window, fill in the configuration items based on your actual business requirements.

Configuration Item	Required Item	Description
Library name	Yes	Library Name. It can contain up to 32 characters of Chinese characters, letters, digits, and underscores.
Suggestion	Yes	You can select **Block** or **Review**. Block: The information is confirmed to be blocked. Review: The information might be undesirable and requires manual recognition. **Note:** The handling of matched content varies with the suggestion you choose. This corresponds to the "Suggestion" parameter returned by the API.
Match mode	Yes	Exact matching only supports Chinese. Exact matching identifies content that exactly matches the keywords specified.

3. Click **Confirm** to save the library configuration.

Modifying a Keyword Library

Steps

1. On the keyword libraries page, find the library you want to modify, click **Edit** on the right, and modify the configuration in the pop-up window on the right according to your business requirements.

2. Click **Add keyword** and enter keywords in the pop-up window.

You can select a **category** for the **keywords** you add. Separate multiple keywords by pressing Enter. You can enter at most 2,000 keywords at a time.

Note:

Only supports the recognition of sensitive words in Chinese.

Keywords are confirmed by newline. Each keyword length is within 20 Chinese characters.

You can also copy keywords (max 2,000) to the input box. Make sure they are separated with line breaks.

The maximum number of sensitive words that can be added is 10,000.

3. Click **Save** at the bottom to save the new library information.

4. After the custom library is configured, when you create a moderation template, you can associate the custom library with image recognition or audio recognition in Recognition policy.

Deleting a Library

1. On the keyword libraries page, find the library you want to delete, and click **Delete** on the right.

2. A window will pop up asking you to confirm the deletion. Click **Confirm**.

Standby Streams

Last updated：2024-06-19 16:58:48

This document shows you how to create, bind, unbind, modify, and delete a standby stream template. A standby stream shows a video or image that becomes active automatically when your live stream is interrupted, helping you improve viewing experience. Once the original stream is recovered, CSS will switch back.

Notes

After creating a template, you need to bind it to a push domain. The configuration takes effect 5-10 minutes after binding.
Binding, unbinding, or modifying a template affects only new live streams and not ongoing ones. To make the change apply to ongoing live streams, you need to stop them and push them again.
You can create up to **50** standby stream templates.
The standby stream feature cannot differentiate between normal stream interruption and abnormal stream interruption. When the stream is interrupted, the standby stream service is triggered by the system.

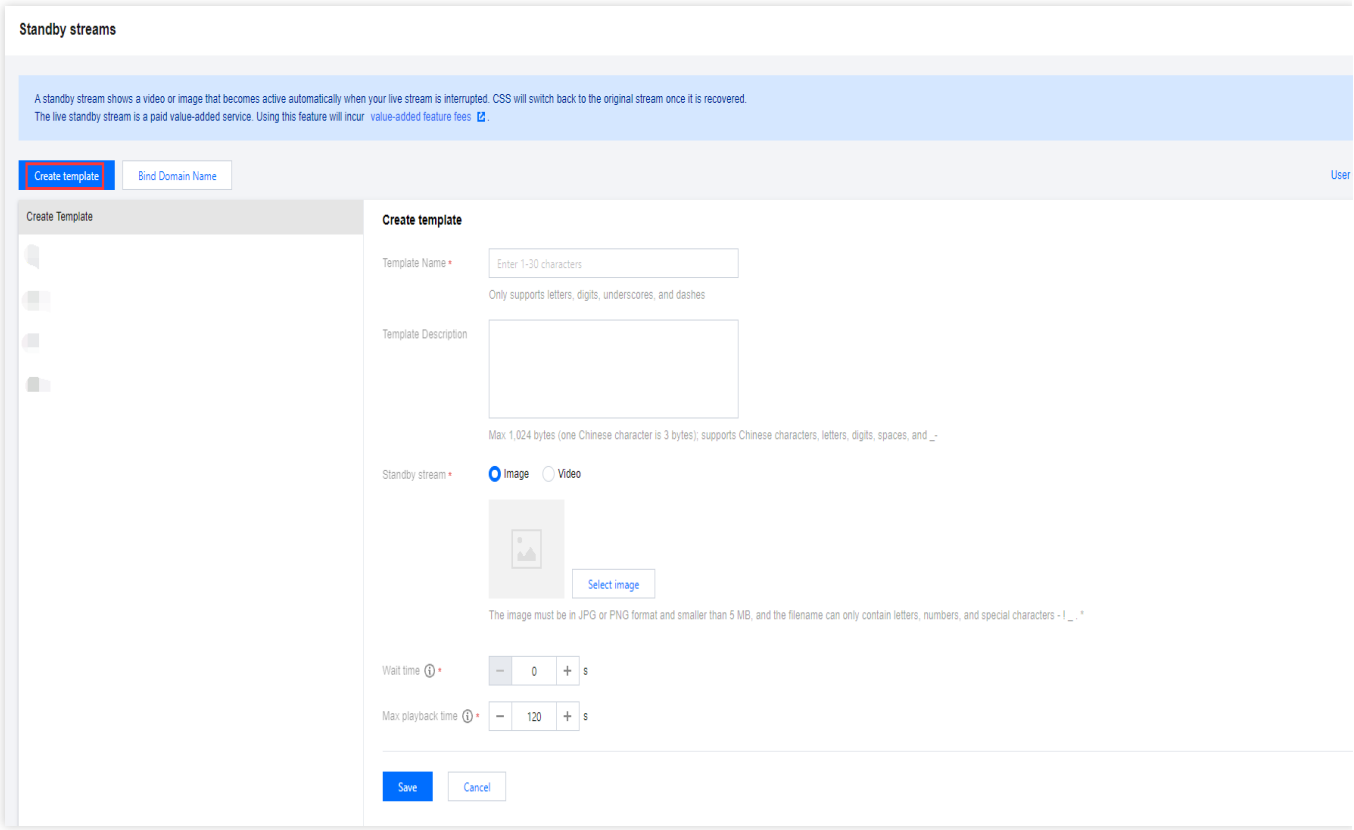
Prerequisites

You have activated CSS and added a push domain.

Creating a Standby Stream Template

1. Log in to the CSS console. Select **Feature Configuration > Standby Streams** on the left sidebar.
2. Click **Create template**.
3. Enter a template name, which can be up to 30 characters long and can contain Chinese characters, letters, numbers, underscores (_), and hyphens (-).
4. Fill in the template description, which only supports Chinese, English, numbers, spaces, underscores, and hyphens, not exceeding 1024 bytes (Note: Chinese characters are counted as 3 bytes each).
5. Select the stream type, which can be image or video.
You can choose to upload images in JPG or PNG format, with a file size less than 5MB. The uploaded image file names only support: English, numbers, and the symbols `- ! _ . *`
You can enter a video URL, which supports FLV and MP4 format audio and video files. The required audio encoding format is AAC.

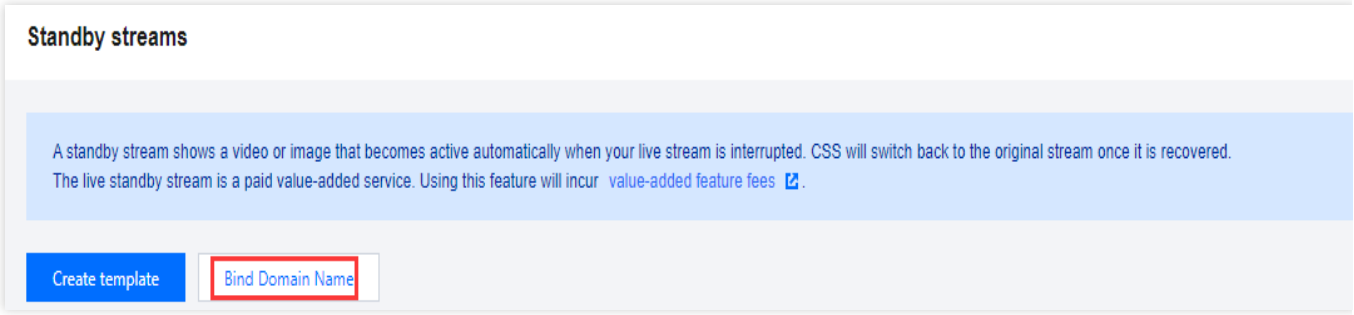
6. Set the stream interruption waiting time (the waiting duration after the stream interruption before playing the standby content) to a value between 0 and 6 seconds.
7. Set the maximum standby content duration, with a default value of 120 seconds. This is the maximum playback duration for the standby content. If the standby content is shorter than this duration, it will be looped. The value cannot be greater than 1,000,000.
8. Click **Save**.



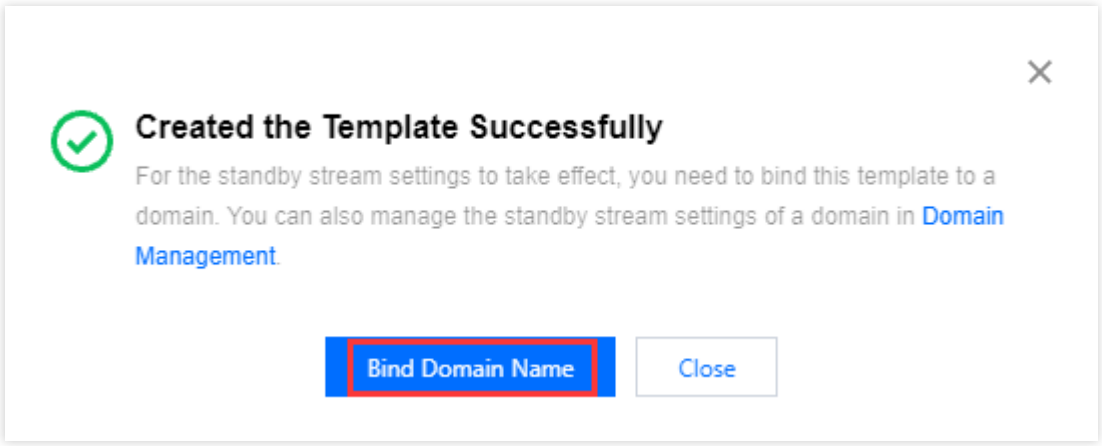
Binding a Domain Name

1. Log in to the CSS console and select **Feature Configuration** > Standby Streams on the left sidebar.
2. You can bind a domain to a template in one of two ways:

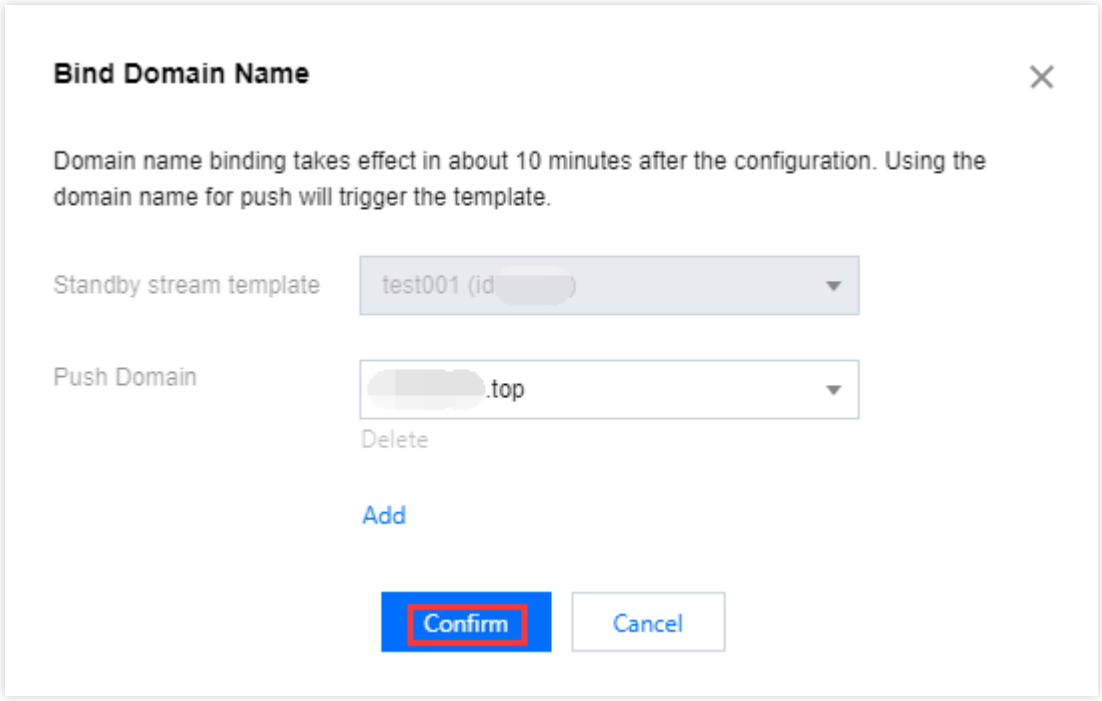
Bind a domain to an existing template: Click **Bind Domain Name** in the top left.



Bind a domain after creating a template: After creating a standby stream template, click **Bind Domain Name** in the dialog box that pops up.



3. In the pop-up window, select a **standby stream template** and a **push domain** and then click **Confirm**.

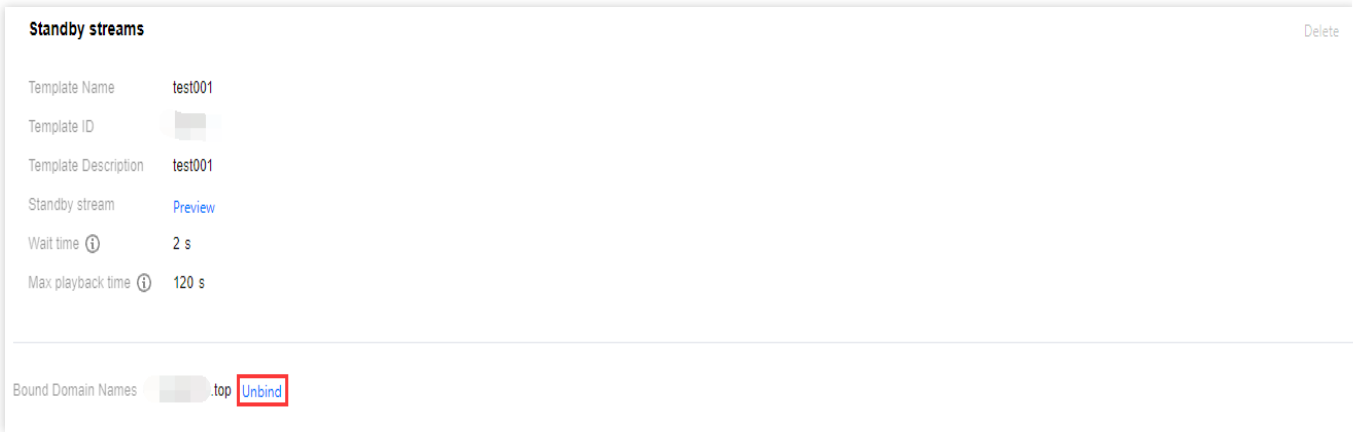


Note:

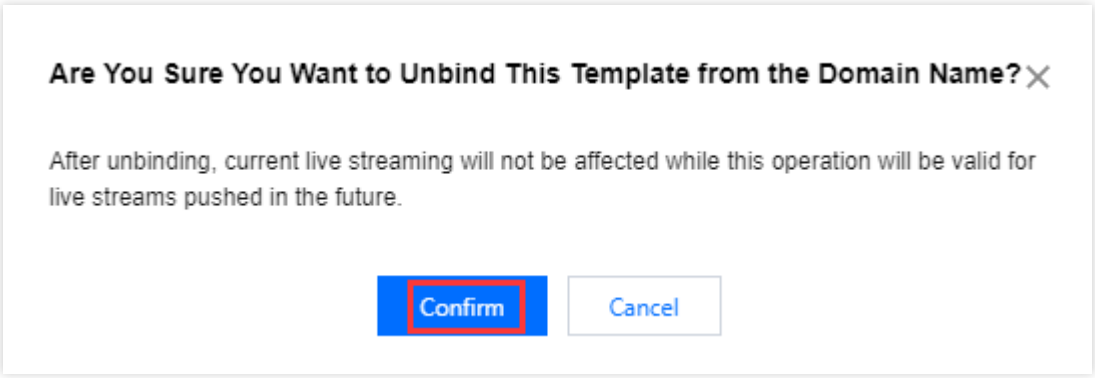
You can click **Add** to bind multiple push domains to a template.

Unbinding a Domain Name

1. Log in to the CSS console and select **Feature Configuration** > Standby Streams on the left sidebar.
2. Select the target template and click **Unbind**.

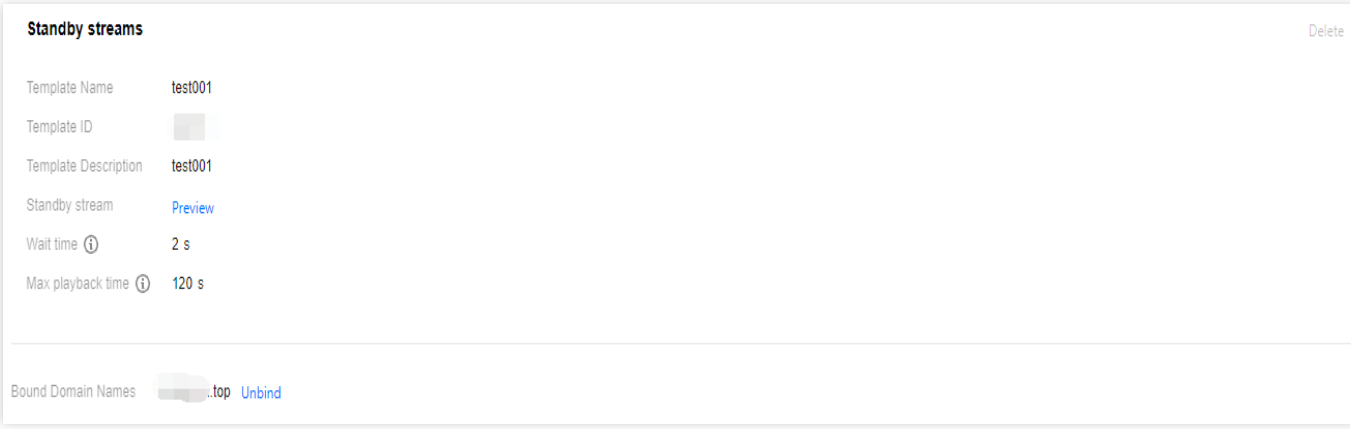


3. In the pop-up window, click **Confirm**.



Modifying a Template

1. Go to **Feature Configuration** > Standby Streams.
2. Select the target template and click **Edit** on the right to modify the template information.
3. After modification, click **Save**.



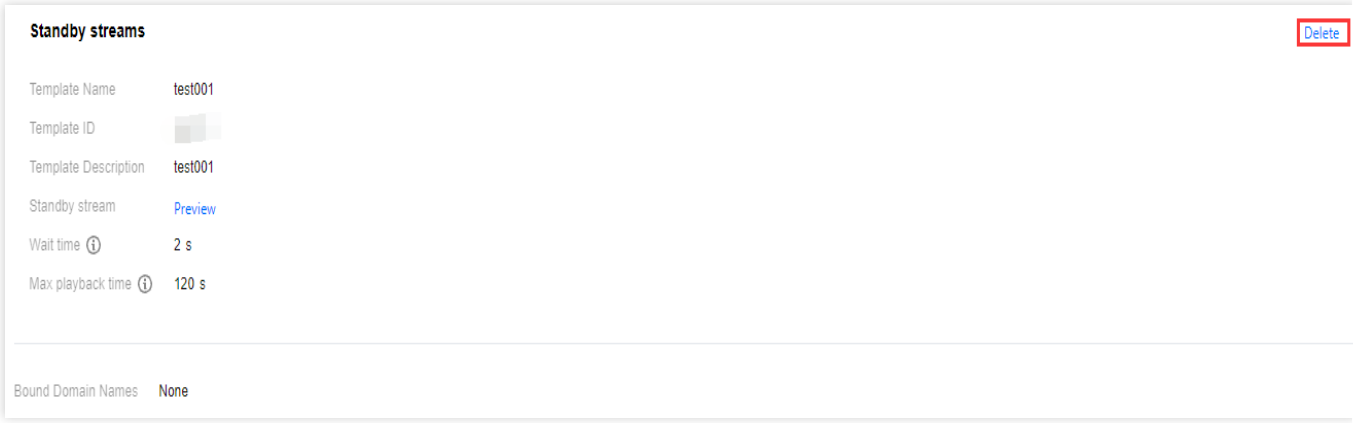
Deleting a Template

Note:

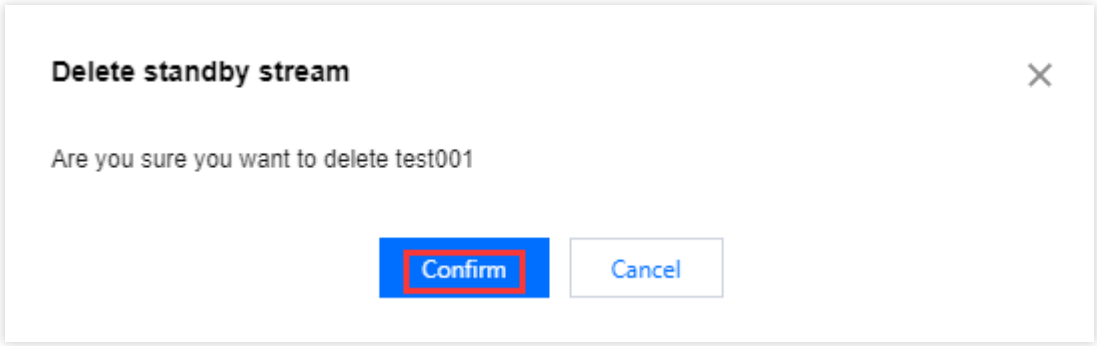
If the template is already associated, you need to Unbind Template before you can perform the delete operation.

Once a template is deleted, it cannot be recovered. Please proceed with caution.

1. Go to **Feature Configuration** > Standby Streams.
2. Select the template you want to delete and click **Delete** in the top right.



3. In the pop-up window, click **Confirm**.



More

You can also **unbind** and **bind** domains and standby stream templates on the **Domain Management** page. For details, see Standby Stream Configuration.

Live Stream Callback

Last updated：2025-03-20 17:55:12

CSS supports callbacks. To use this feature, you need to create a callback template in the console, configure an address to receive callbacks for an event, and then bind the template with your push domain name. If the event triggers a callback during live streaming, Tencent Cloud will send a request to your server, which is responsible for responding to the request. After successful verification, the server will obtain a JSON packet of the callback through the address configured.

This document describes how to create, modify and delete a callback template in the console.

You can create a callback template in the following ways:

Create a template in the CSS console. For details, see Creating a Callback Template.

Create a template with APIs. For the parameters and request sample, see CreateLiveCallbackTemplate.

Must-knows

After creating a template, you need to bind it with a push domain name. The binding takes effect in about 5-10 minutes.

Make sure the HTTP or HTTPS server you use to receive callbacks are able to receive requests and respond normally.

In the console, you can only bind and unbind callback templates at the domain level. For callback rules bound to specific streams by APIs, you need to call DeleteLiveCallbackRule to unbind them.

For information on callback protocols, see How to Receive Event Notification.

For information about the parameters in a callback, see the following documents:

Stream pushing

Stream interruption

Recording Event Notification

Recording Status Event Notification

Screencapturing Event Notification

Image Audit Event Notification

Audio Auditing Service Event Notification

Relay

Push errors

Recording Error Event Notifications

Creating a Callback Template

Recording Event Notification

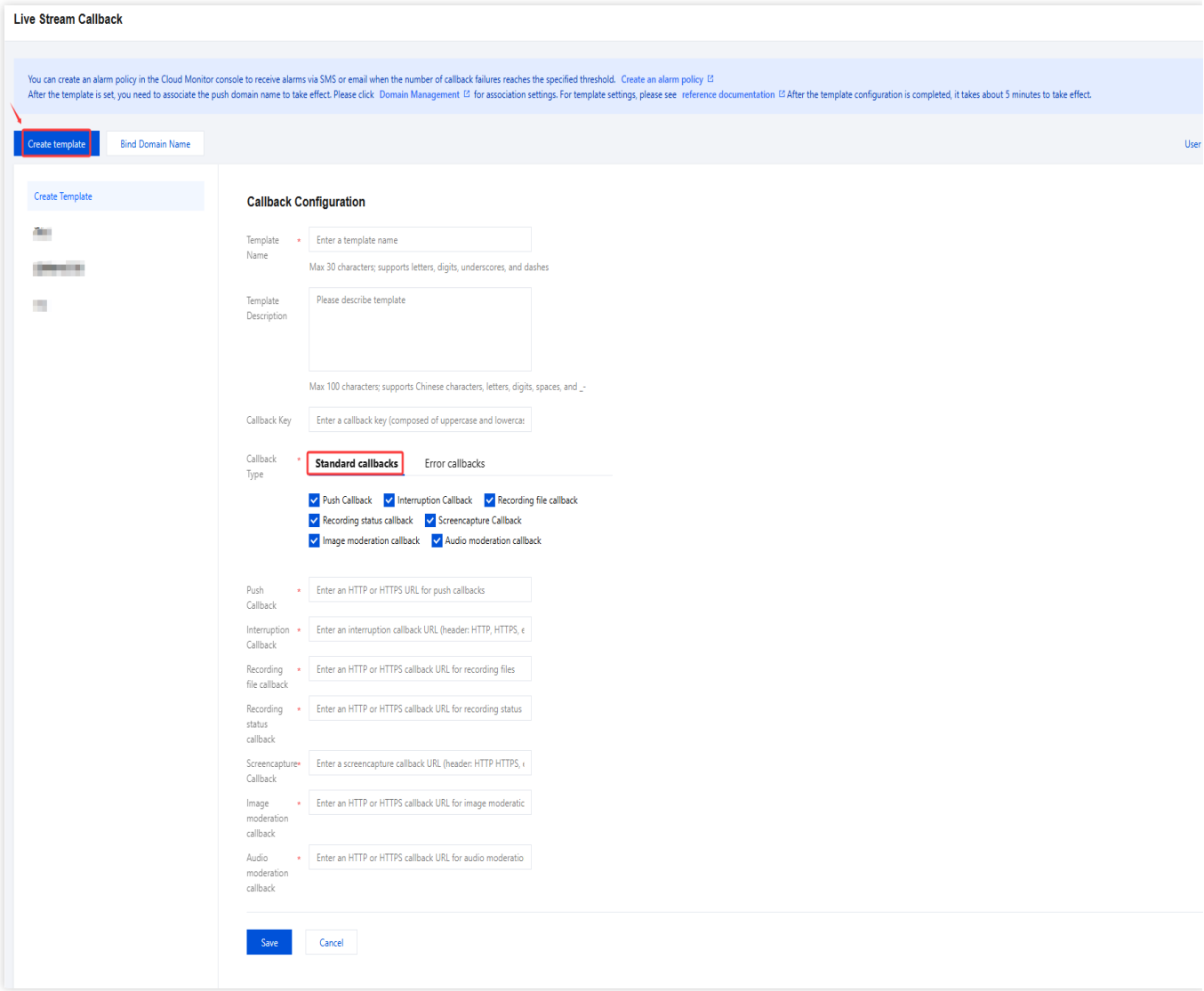
1. Log in to the CSS console.

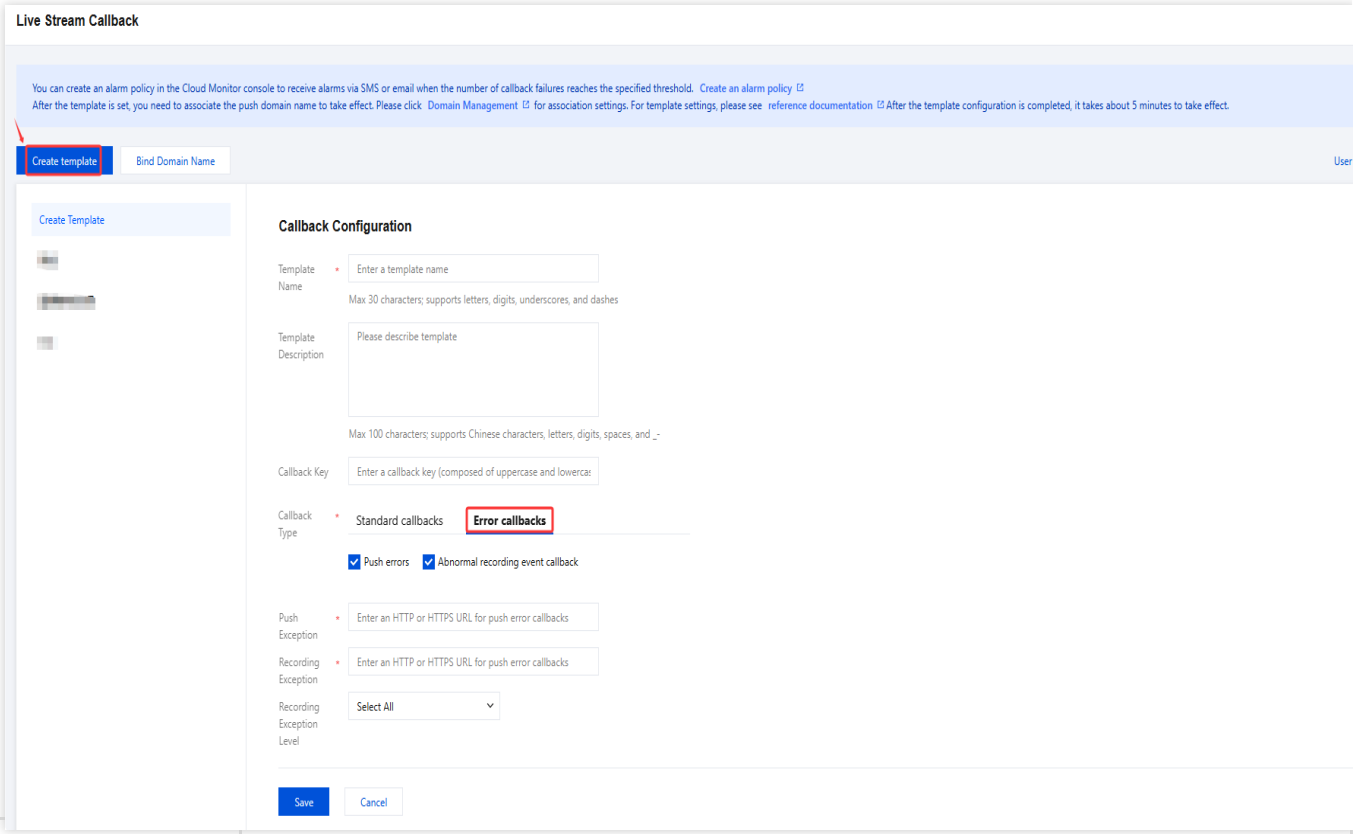
2. Select **Feature Configuration**> Live Stream Callback in the left sidebar.

3. Click **Create Template**, fill in the information, select the types of callbacks you want to receive, enter the callback URLs, and click **Save**.

Callback Type-Standard callbacks

Callback Type-Error callbacks





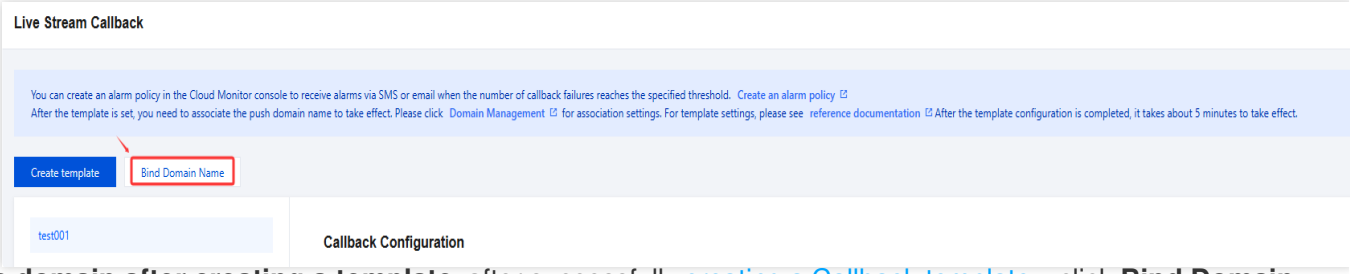
Item	Description
Template Name	The callback template name, which can contain up to 30 Chinese characters, letters, numbers, underscores (_), and hyphens (-).
Template Description	The description of the callback template, which can contain up to 100 Chinese characters, letters, numbers, underscores (_), and hyphens (-).
Callback Key	A custom callback key. It can contain up to 32 letters and numbers. For details, see Common callback parameters.
Push Callback	Enter an HTTP or HTTPS address to receive push callbacks.
Interruption Callback	Enter an HTTP or HTTPS address to receive push interruption callbacks.
Recording file callback	Enter an HTTP or HTTPS address to receive push Recording file callback.
Recording status callback	Enter an HTTP or HTTPS address to receive push Recording status callback.
Recording Callback	Enter an HTTP or HTTPS address to receive recording callbacks.
Screencapture Callback	Enter an HTTP or HTTPS address to receive screencapture callbacks.
Porn Detection	Enter an HTTP or HTTPS address to receive porn detection callbacks.

Callback	
Error callbacks	Enter an HTTP or HTTPS address to receive push error callbacks.
Recording Error Callback	Enter an HTTP or HTTPS address to receive push Recording callbacks. The Recording Exception Level defaults to "Error", but supports the selection of "Alarm" and allows multiple selections.

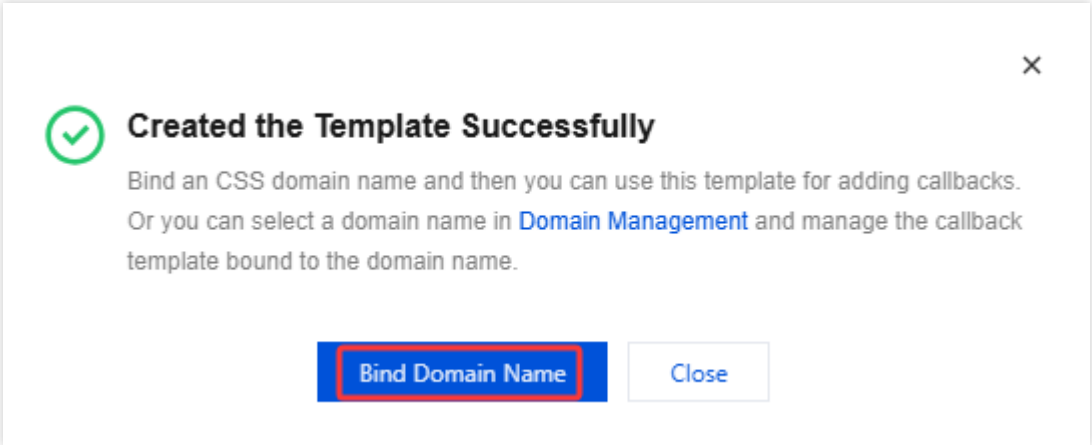
Binding a Domain Name

1. Log in to the CSS console and select **Feature Configuration** >Live Stream Callback on the left sidebar.
2. You can bind a domain to a template in one of two ways:

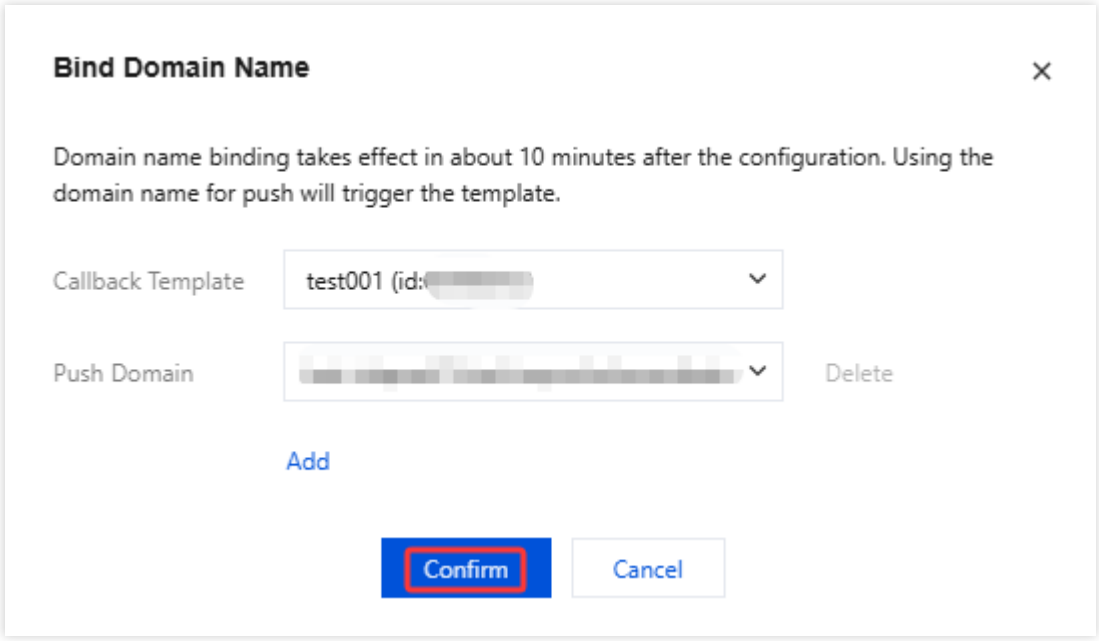
Bind a domain to an existing template: Click **Bind Domain Name** in the top left.



Bind a domain after creating a template: after successfully creating a Callback template, click **Bind Domain Name** in the dialog box that pops up.



3. In the Bind Domain Name window, select the desired **Live creating template** and **Push Domain**, then click on Confirm to successfully bind them.

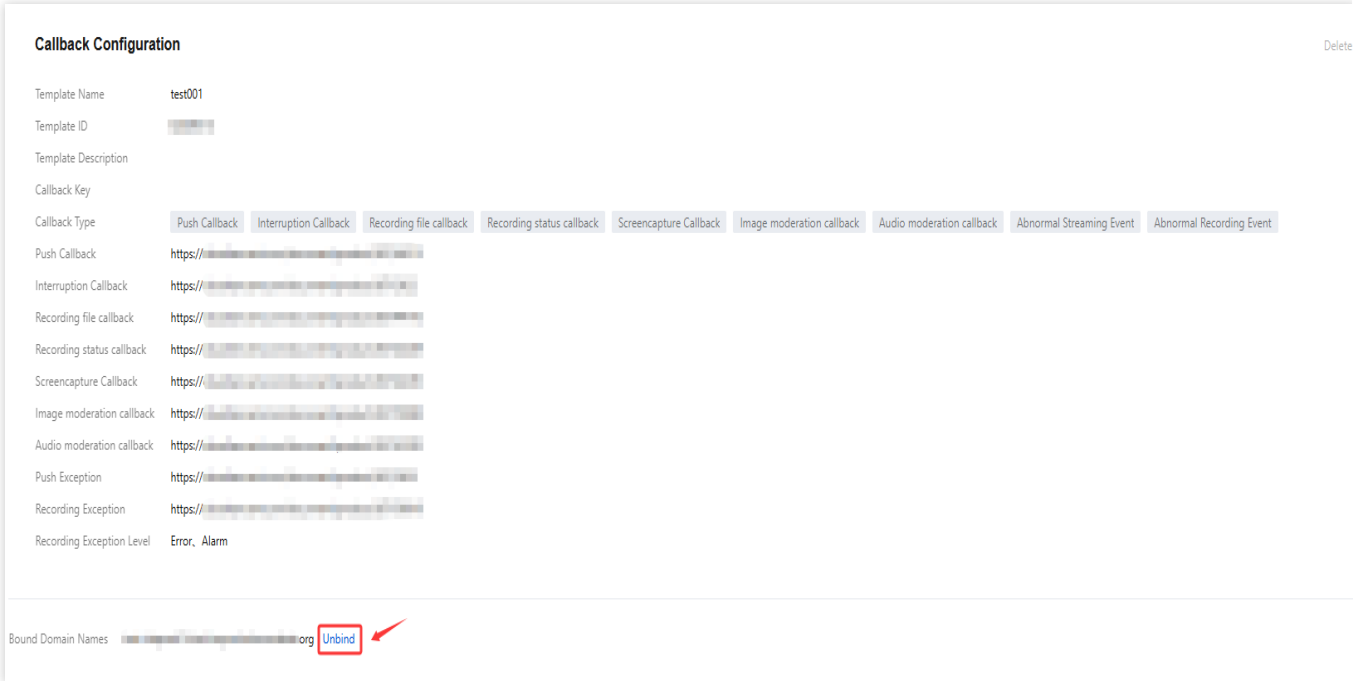


Note:

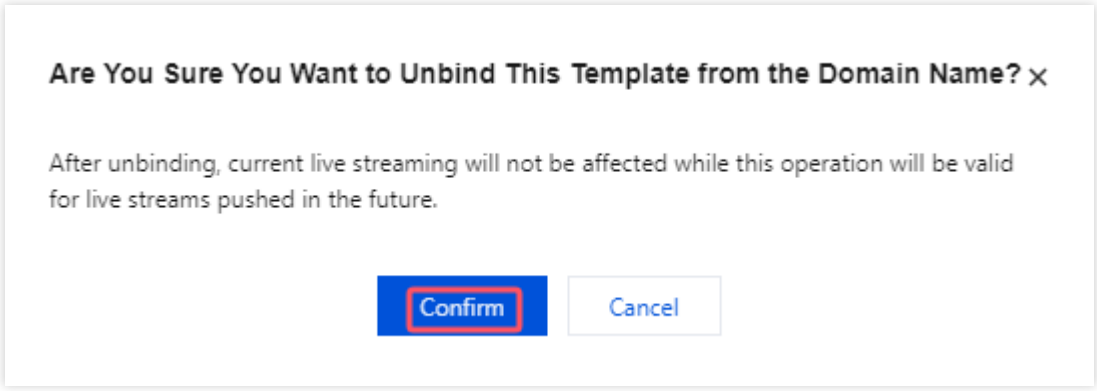
You can click **Add** to bind multiple push domains with the current template.

Unbinding

1. Log in to the CSS console and select **Feature Configuration** >Live Stream Callback on the left sidebar.
2. Select the Callback template of the bound domain that you want to unbind, then click **Unbind**.

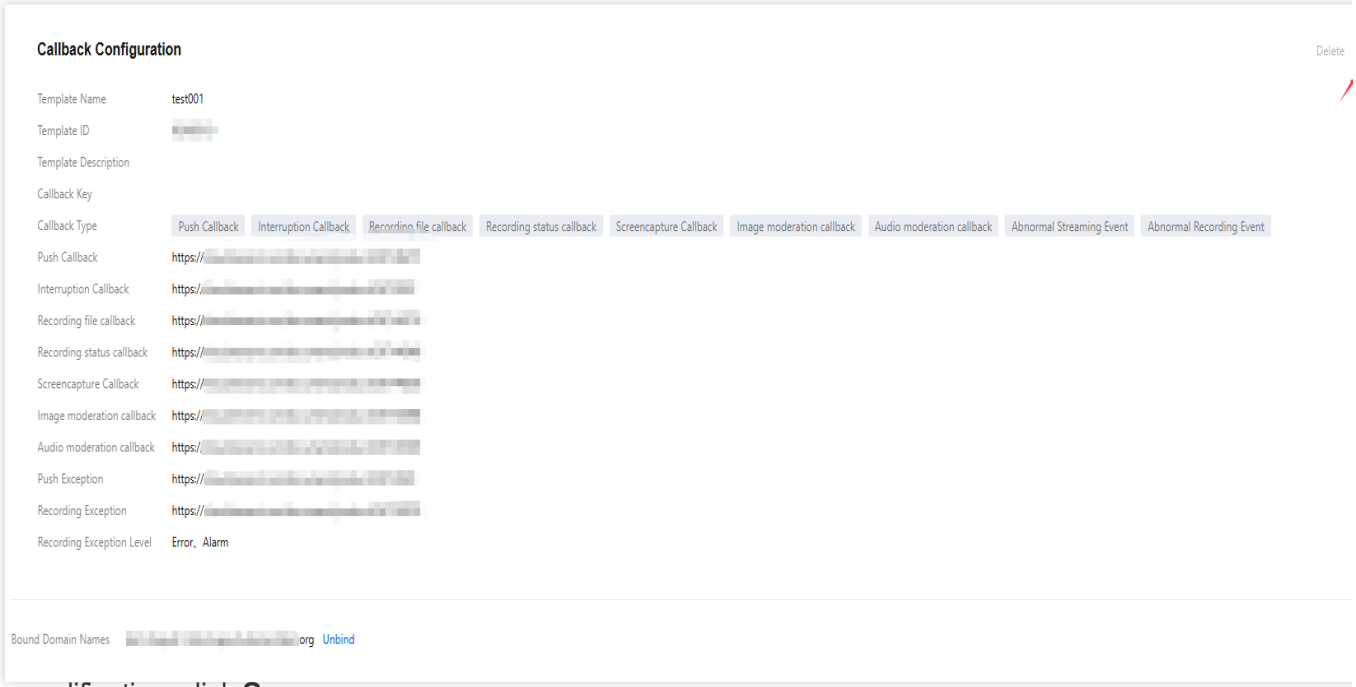


3. Confirm it if you wish to unbind the current linked domain, and click **Confirm** to proceed with unbinding.



Modifying a Callback Template

1. Log in to the CSS console and select **Feature Configuration** >Live Stream Callback on the left sidebar.
2. Select the target callback template and click **Edit** to modify its information.



3. After modification, click **Save**.

Deleting a Callback Template

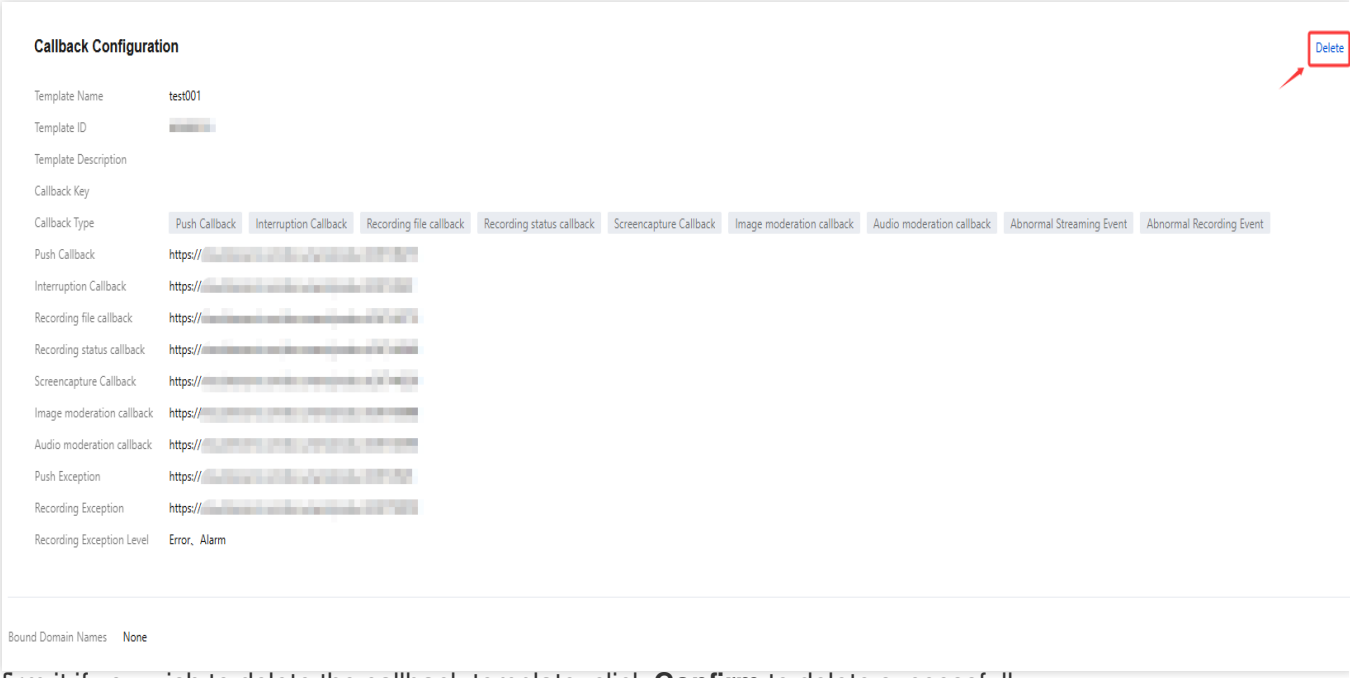
Note:

If the template has been associated, you must first Unbinding it before performing a deletion process.

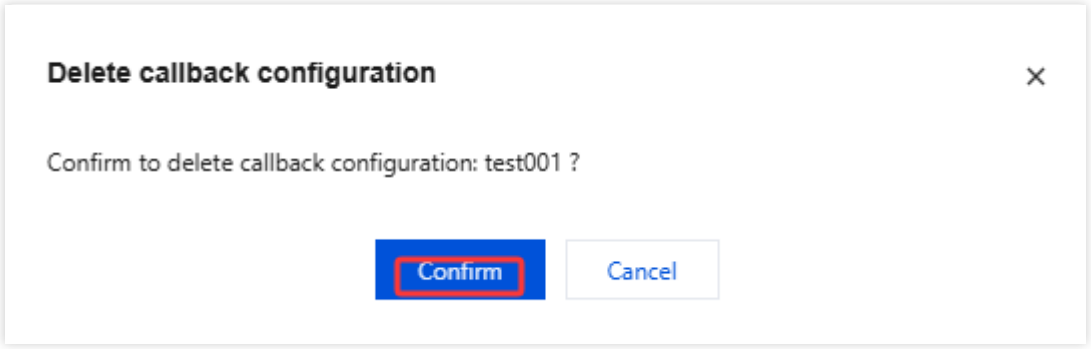
Note that a deleted template cannot be recovered. Proceed with caution.

1. Log in to the CSS console and select **Feature Configuration** >Live Stream Callback on the left sidebar.

2. Select the successfully created callback template, click **Delete** in the upper part.



3. Confirm it if you wish to delete the callback template, click **Confirm** to delete successfully.



Related Operations

You can also unbind and bind domains and callback templates on the Domain Management page. For details, see Callback Configuration.

DRM
Configuring DRM Encryption

Last updated：2024-10-11 09:59:24

CSS offers DRM encryption capabilities based on Widevine, FariPlay, and NormalAES to help you protect your content and prevent piracy and hotlinking. This document shows you how to configure DRM encryption in the CSS console.

Must-Knows

Tencent Cloud only encrypts your content. DRM licenses are offered by third party licensing services SDMC and DRMtoday, which charge a licensing fee. To learn more details, please contact the companies.

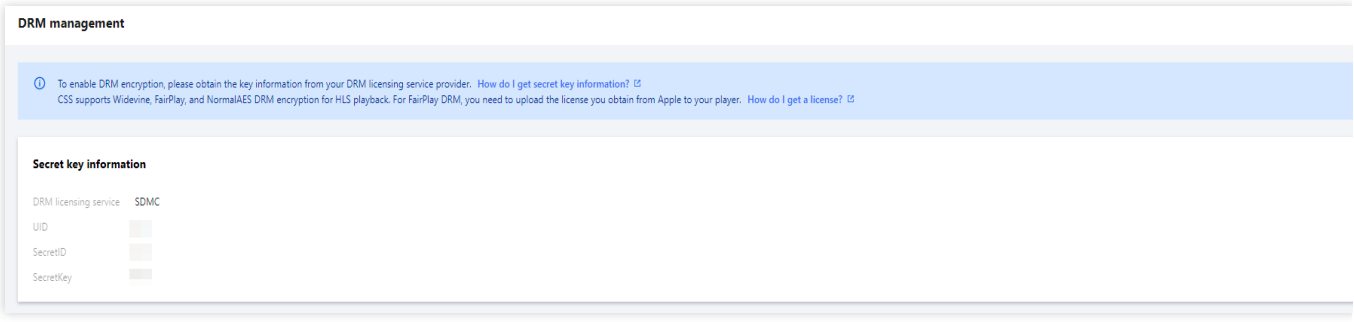
Prerequisites

You have activated CSS and added a playback domain name.
You have created an account at SDMC DRM or DRMtoday and configured an access key.

Console Settings

Configuring DRM key information

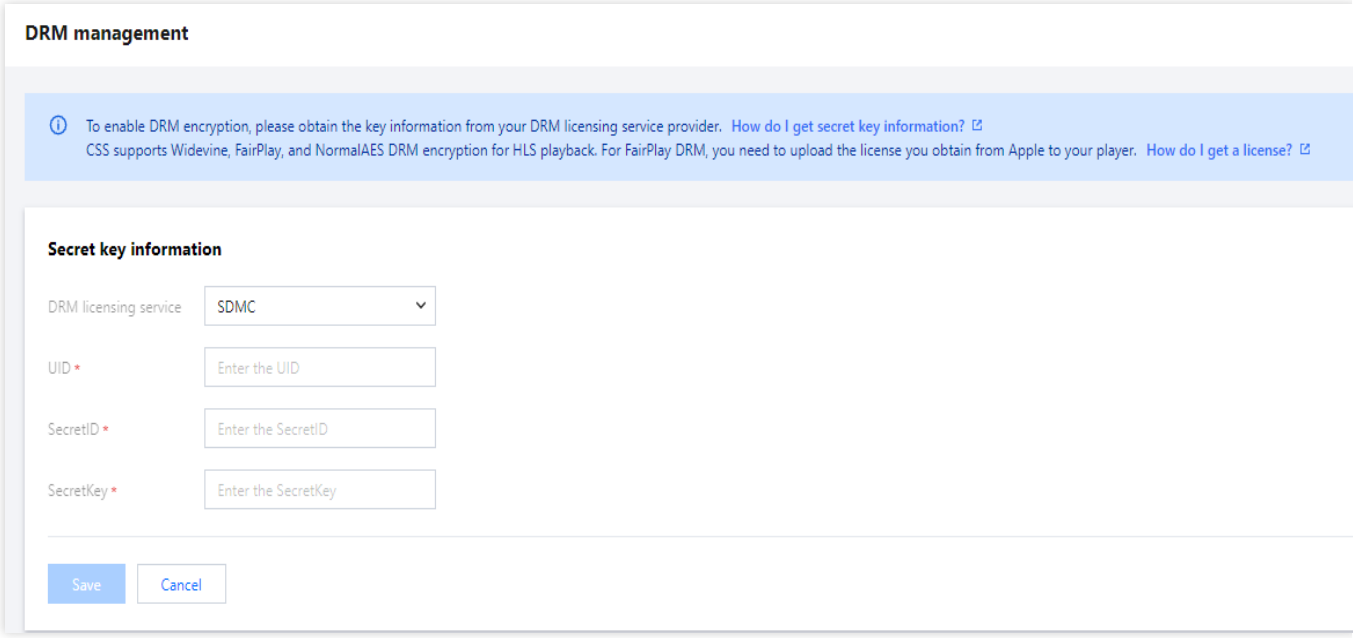
1. Log in to the CSS console and select **Feature Configuration** > DRM management on the left sidebar.
2. Click **Edit** on the right to enter the DRM management configuration page.



3. Fill in the **secret key information** and select your certificate management provider. You can choose SDMC or DRMtoday. The specific configuration is as follows:

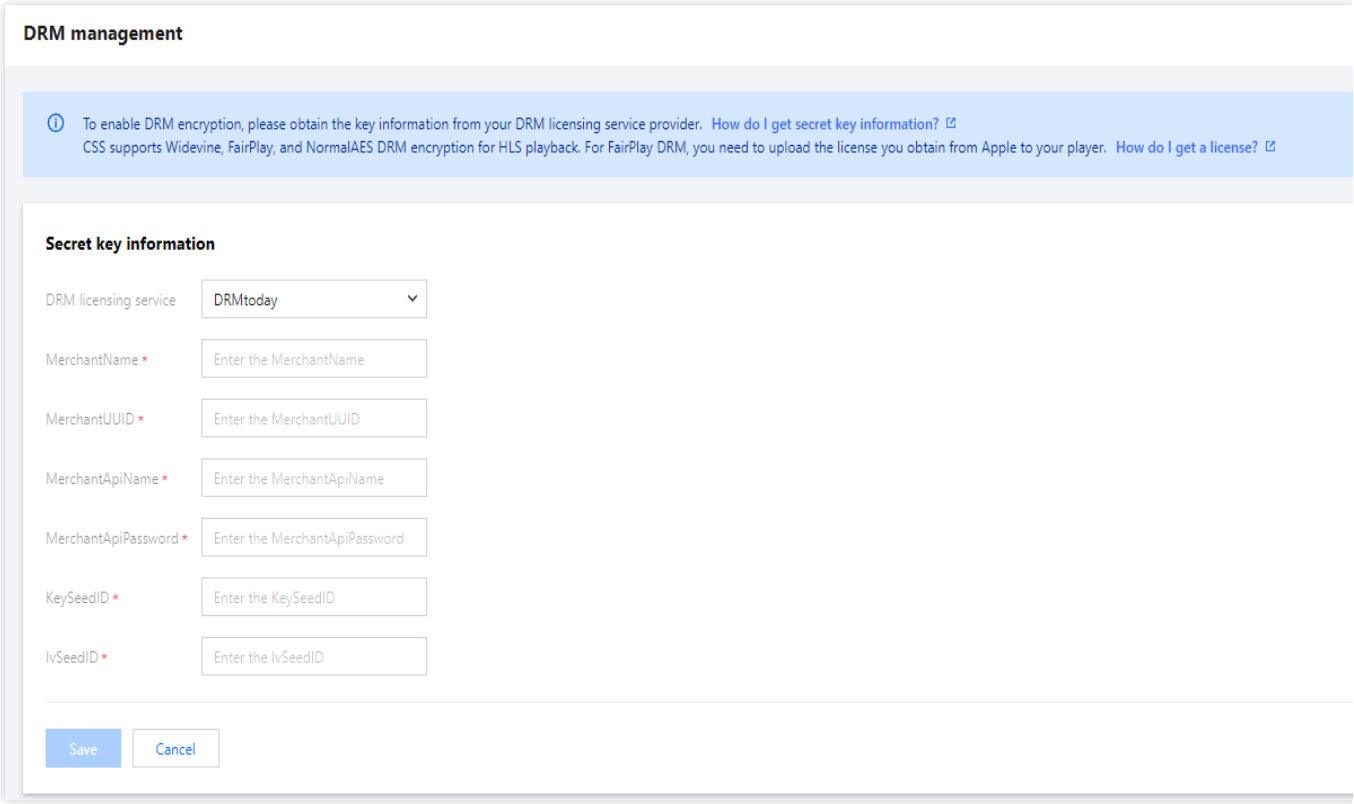
If your licensing service provider is **SDMC**:

Enter your SDMC UID, Secret ID, and Secret key (you need to obtain the information from SDMC).



If your licensing service provider is **DRMtoday**:

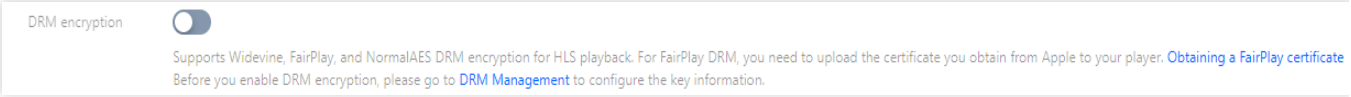
Enter your DRMtoday `Merchantname`, `MerchantUUID`, `MerchantAPIName`, `MerchantAPIPassword`, `KeySeedID`, and IVSeedID (you need to obtain the information from DRMtoday).



Setting Transcoding Templates

1. Log in to the CCS console and enter the **Feature Configuration** > Live Transcoding.
2. Click **Create Transcoding Template** to enter the transcoding configuration page. Click

to enable the DRM encryption. Set the DRM encryption information.



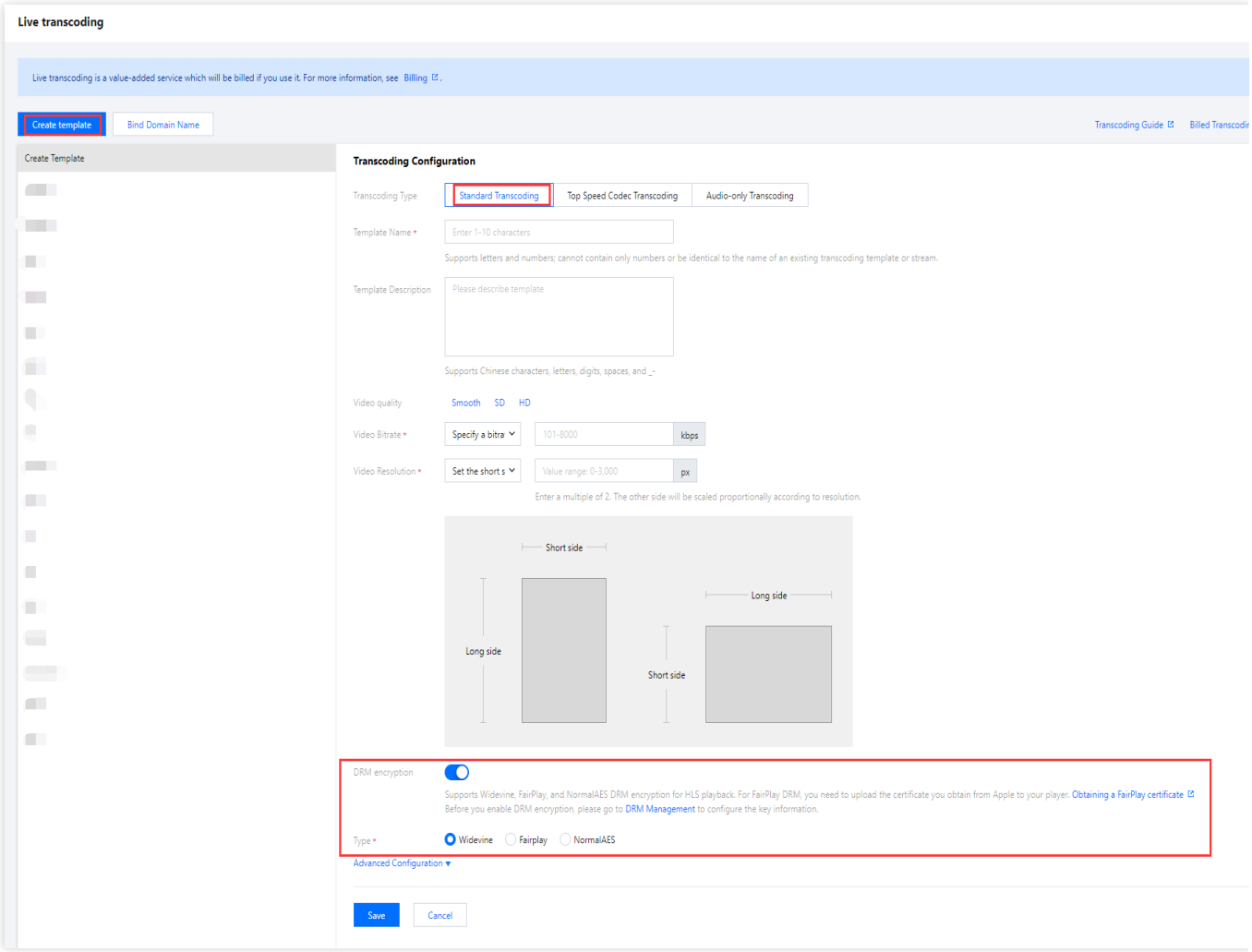
Configuration Item	Required	Description
DRM encryption	No	Whether to enable DRM encryption. It's disabled by default. Before enabling this feature, you need to configure DRM key information in "DRM management".
Type	Yes	Widevine, FairPlay, or NomalAES. For FairPlay encryption, you need to upload the certificate you obtain from Apple to your player. For details, see Obtaining a FairPlay certificate.

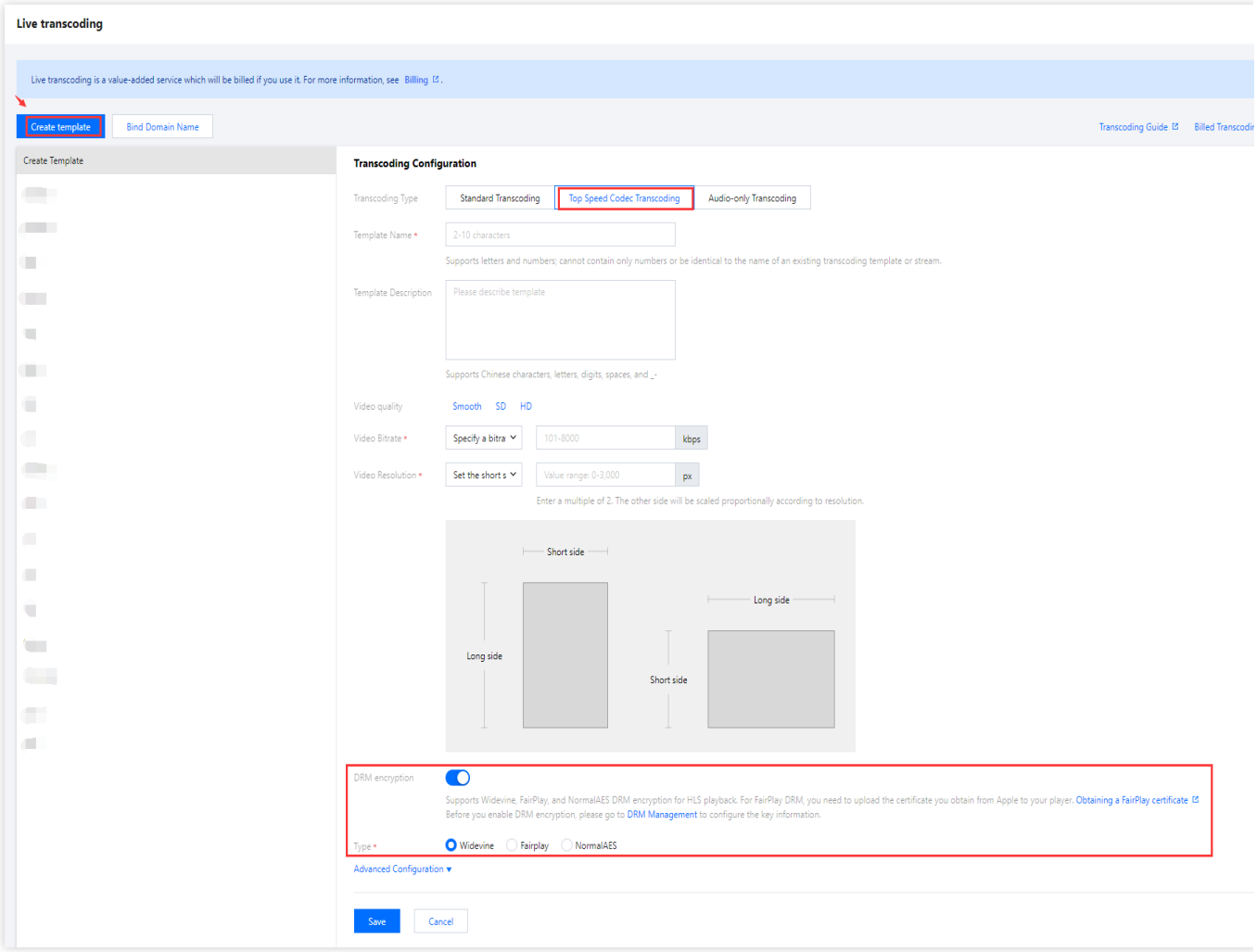
2.1 You can switch between different tabs to view the DRM encryption configuration requirements for standard transcoding, top speed codec transcoding, and audio-only transcoding.

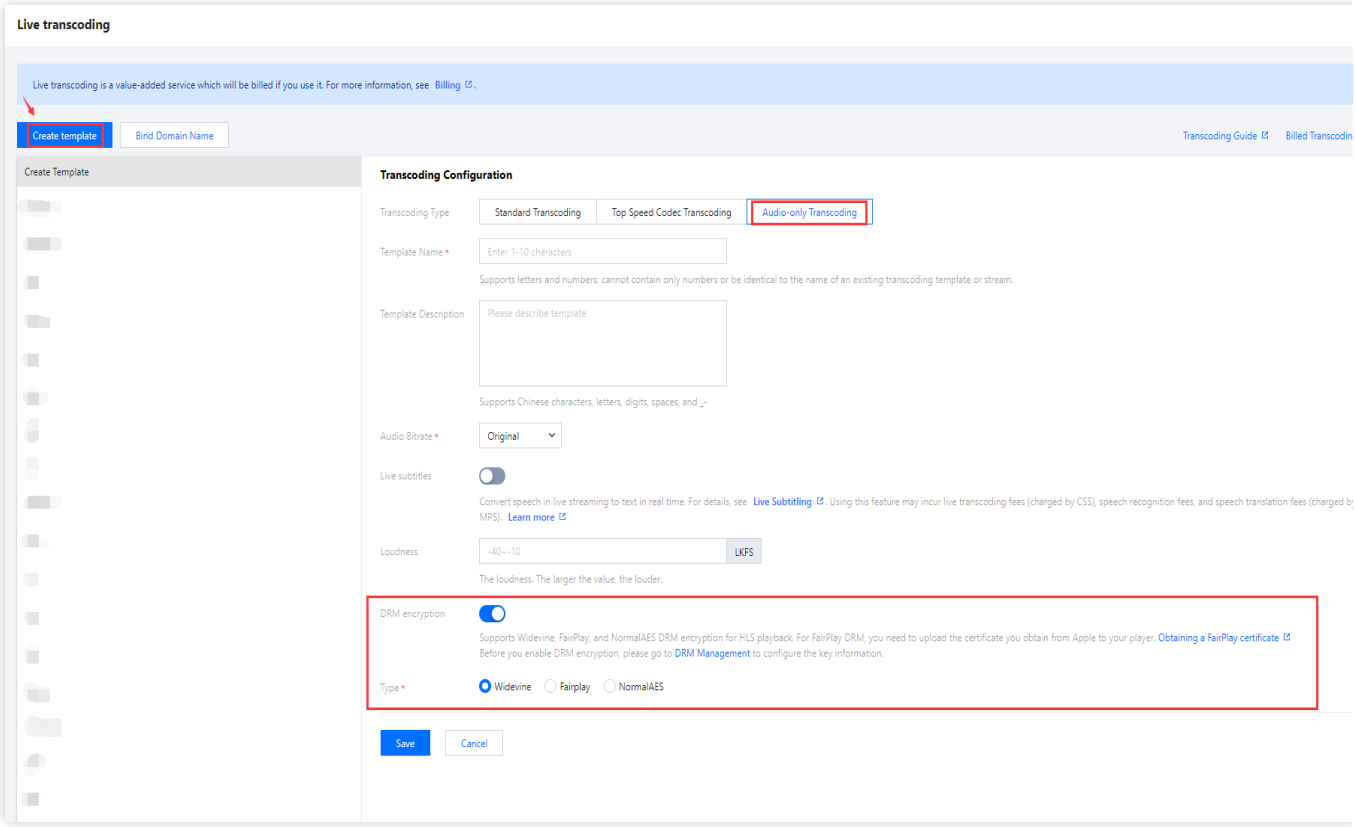
Standard Transcoding

Top Speed Codec Transcoding

Audio-only Transcoding




Live transcoding
Live transcoding is a value-added service which will be billed if you use it. For more information, see Billing .
Create template
Bind Domain Name
Transcoding Guide
Billed Transcodir
Create Template
Transcoding Configuration
Transcoding Type
Standard Transcoding
Top Speed Codec Transcoding
Audio-only Transcoding
Template Name *
2-10 characters
Supports letters and numbers; cannot contain only numbers or be identical to the name of an existing transcoding template or stream.
Template Description
Please describe template
Supports Chinese characters, letters, digits, spaces, and _-
Video quality
Smooth
SD
HD
Video Bitrate *
Specify a bitra
101-8000
kbps
Video Resolution *
Set the short s
Value range: 0-3,000
px
Enter a multiple of 2. The other side will be scaled proportionally according to resolution.
Short side
Long side
Long side
Short side
DRM encryption
Supports Widevine, FairPlay, and NormalAES DRM encryption for HLS playback. For FairPlay DRM, you need to upload the certificate you obtain from Apple to your player. Obtaining a FairPlay certificate
Before you enable DRM encryption, please go to DRM Management to configure the key information.
Type *
Widevine
Fairplay
NormalAES
Advanced Configuration
Save
Cancel

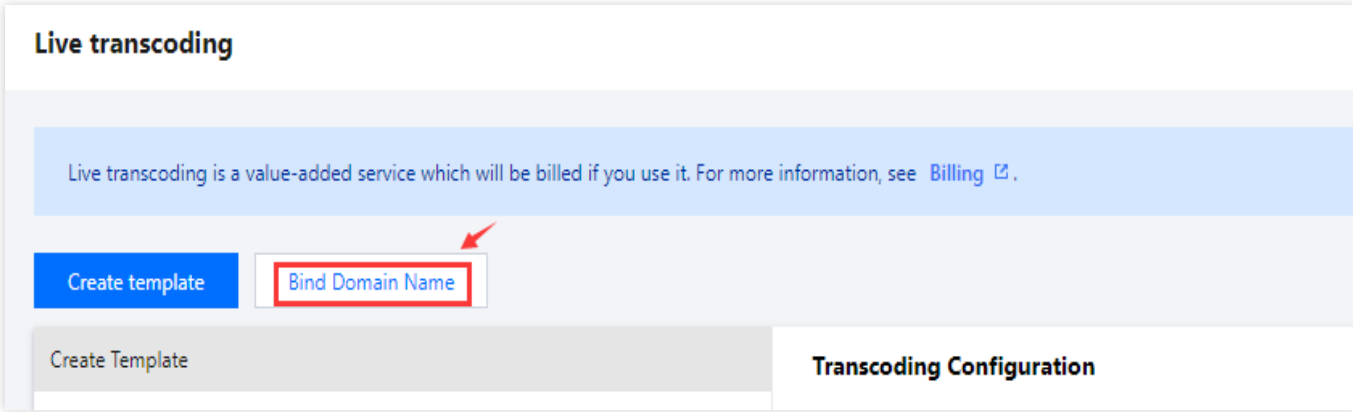


3. After the configuration is completed, click **Save** .

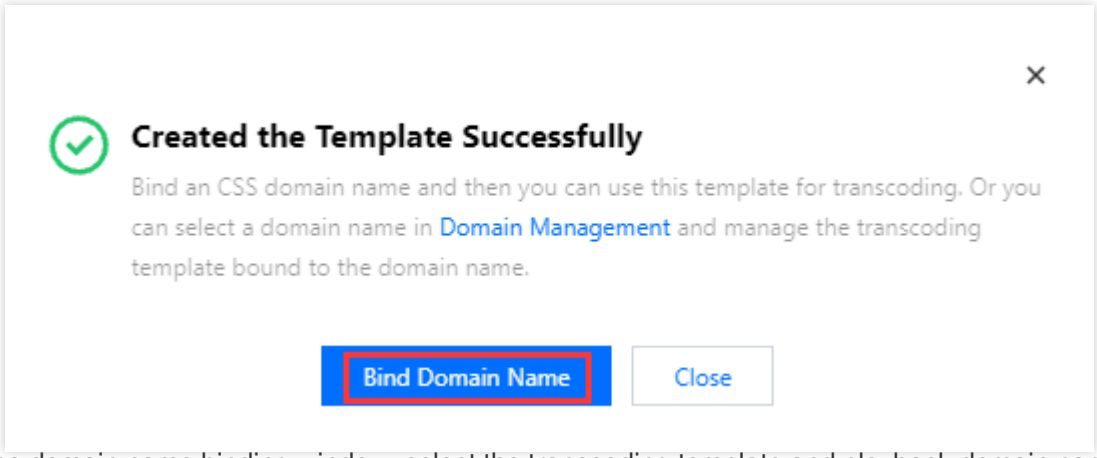
Binding Domain Names

1. Log in to the CSS console and enter the **Feature Configuration** > Live Transcoding.
2. Enter the domain name binding window in the following ways:

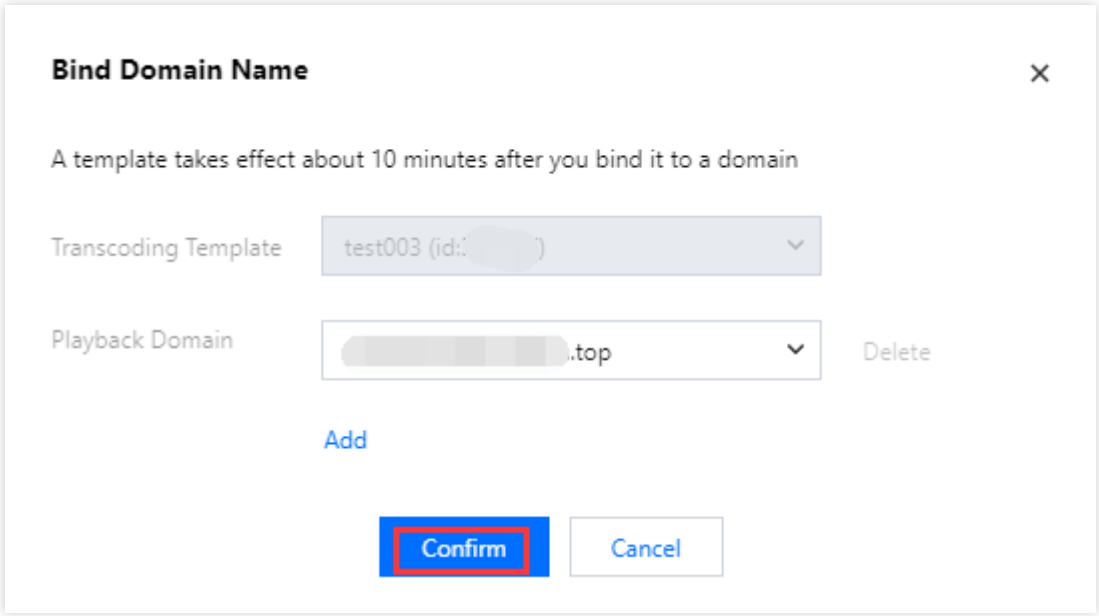
Directly bind the domain name : Click **Bind Domain Name** on the top left.



After successfully creating a new transcoding template, bind the domain name : After successfully setting the transcoding template, click **Bind Domain Name** in the prompt dialog box.

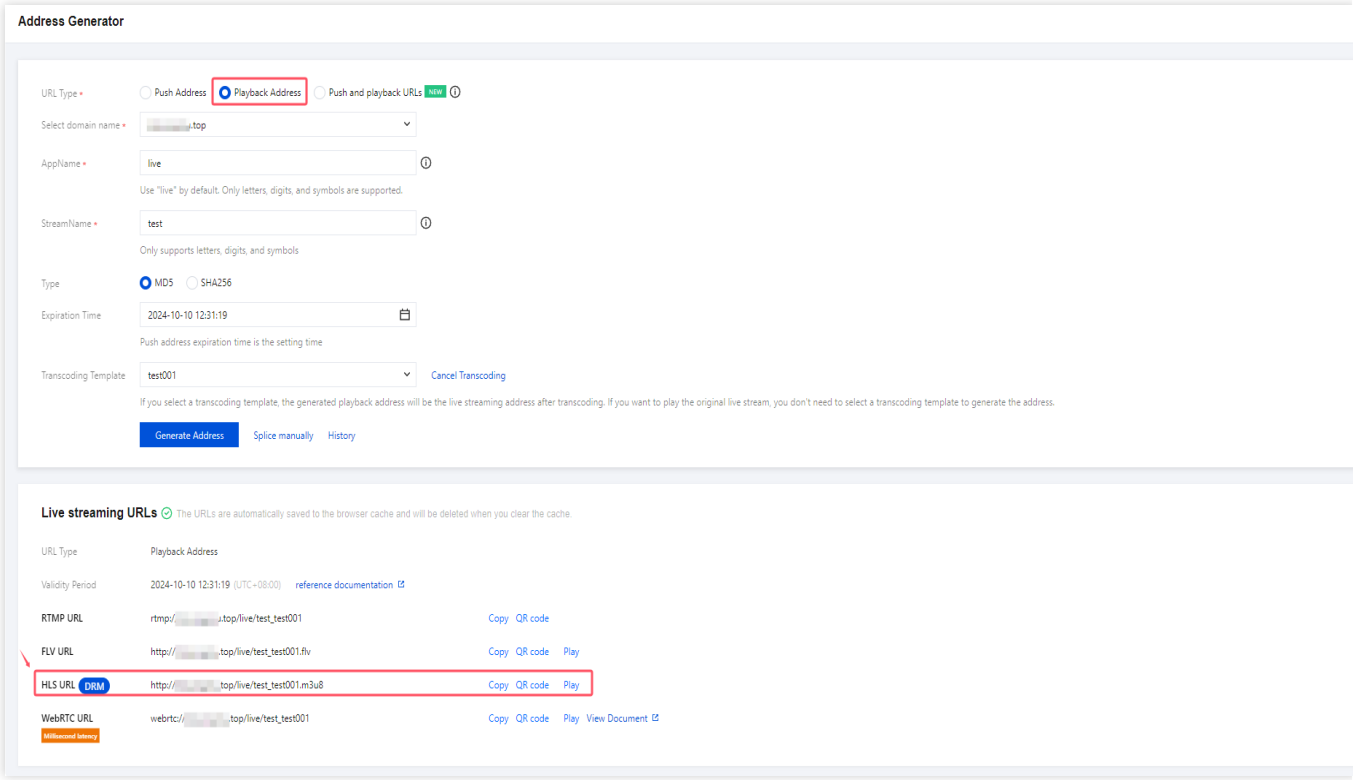


3. In the domain name binding window, select the transcoding template and playback domain name you want to bind, and click **Confirm** to finish.



Obtaining the DRM-encrypted playback URL

Only HLS playback supports DRM encryption. Use the Address Generator to generate playback URLs (select the template you created). The HLS URL generated is DRM-encrypted.



Configuring Your Player

For the DRM encryption feature to work, your player must meet the following requirements:

It must have been equipped by SDMC with the ability to obtain and decrypt license information from video data.

Use FairPlay encryption for iOS players and Widevine or NormalAES for Android players.

On iOS, you need to apply for a certificate and upload it to the SDMC console.

Note:

You need to create an account first before you can visit the SDMC console. For detailed directions on how to create an SDMC account, see Obtaining the UID and Key Information. If you encounter any problems, please submit a ticket. We will help you navigate the process.

Obtaining a FairPlay Certificate

Last updated：2023-11-20 16:32:40

To encrypt your content with FairPlay, you need to obtain an FPS deployment package from Apple and upload the following files to SDMC's server.

FPS certificate file (`.der` or `.cer`)

Private key file (`.pem`)

Private key password file (`.txt`)

Application secret key (ASK) (`.txt`)

Directions

Step 1. Create an Apple developer account and request an FPS package

1. Create an Apple developer account.

2. At the bottom of the FairPlay Streaming page, click **Request FPS Deployment Package**, and log in with your Apple developer account.

3. Fill out the form and submit it. After your request is approved, Apple will send you a package containing the FPS certificate generation guide.

Note

When asked if you have implemented and tested Key Security Module (KSM), you can paste the answer below:

```
I am using a 3rd party DRM company and the company has already built and tested KSM
```

Step 2. Create a private key and a certificate signing request (CSR)

Create a private key file (`privatekey.pem`) and a CSR file (`certreq.csr`) as instructed in the FPS certificate generation guide. The following describes the OpenSSL method in the guide.

Note

Make sure OpenSSL is installed on the computer or server environment where this process is performed.

1. **Create a private key file (`privatekey.pem`)**:

1.1 Run the command below to create a private key file:

```
openssl genrsa -aes256 -out privatekey.pem 1024
```

1.2 Set a password (not longer than 32 characters) for the private key. Note it for later use.

2. **Create a CSR file**:

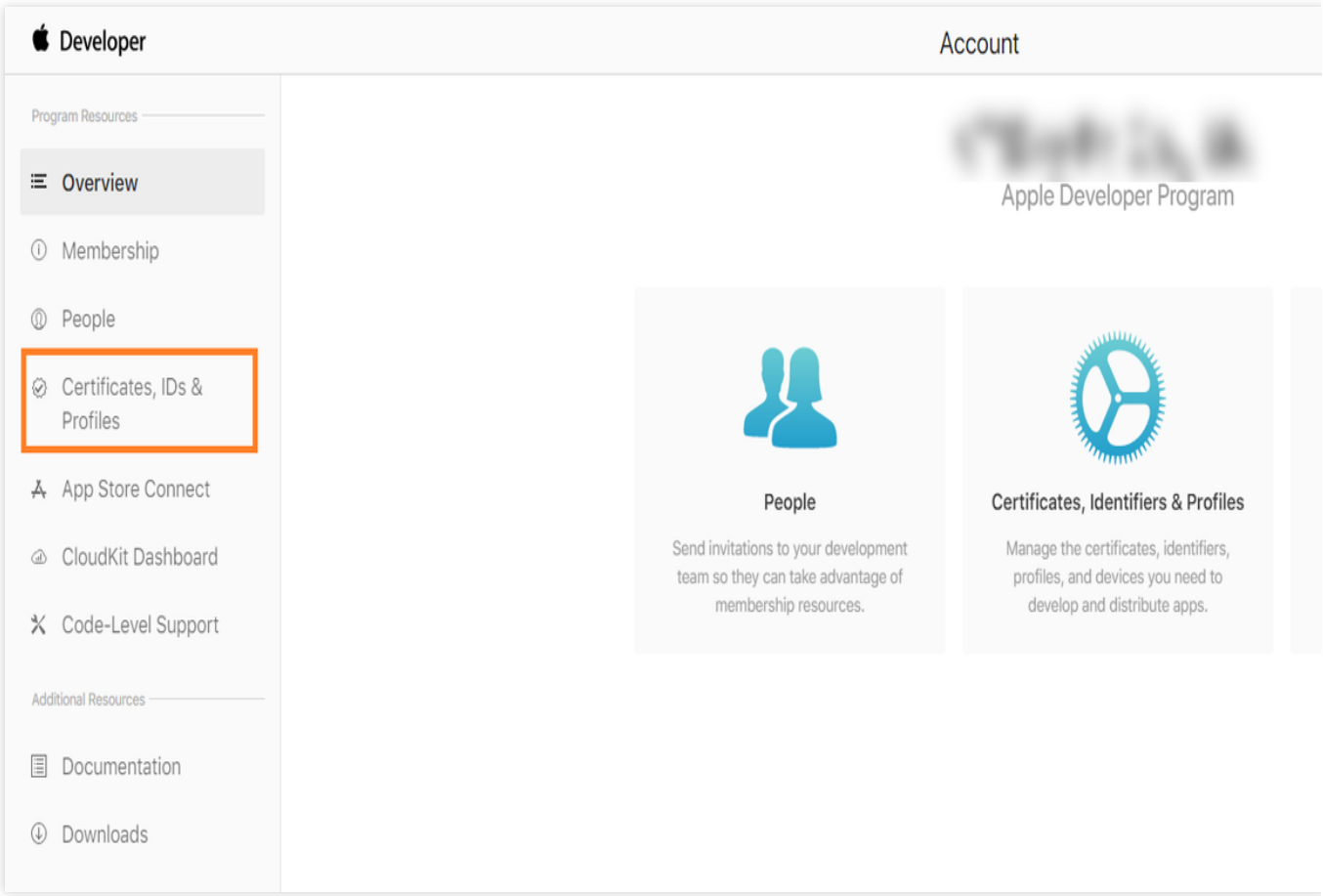
2.1 Run the command below (you can modify `-subj`):

```
openssl req -new -sha1 -key privatekey.pem -out certreq.csr -subj
"/CN=SubjectName/OU=OrganizationalUnit/O=Organization/C=US"
```

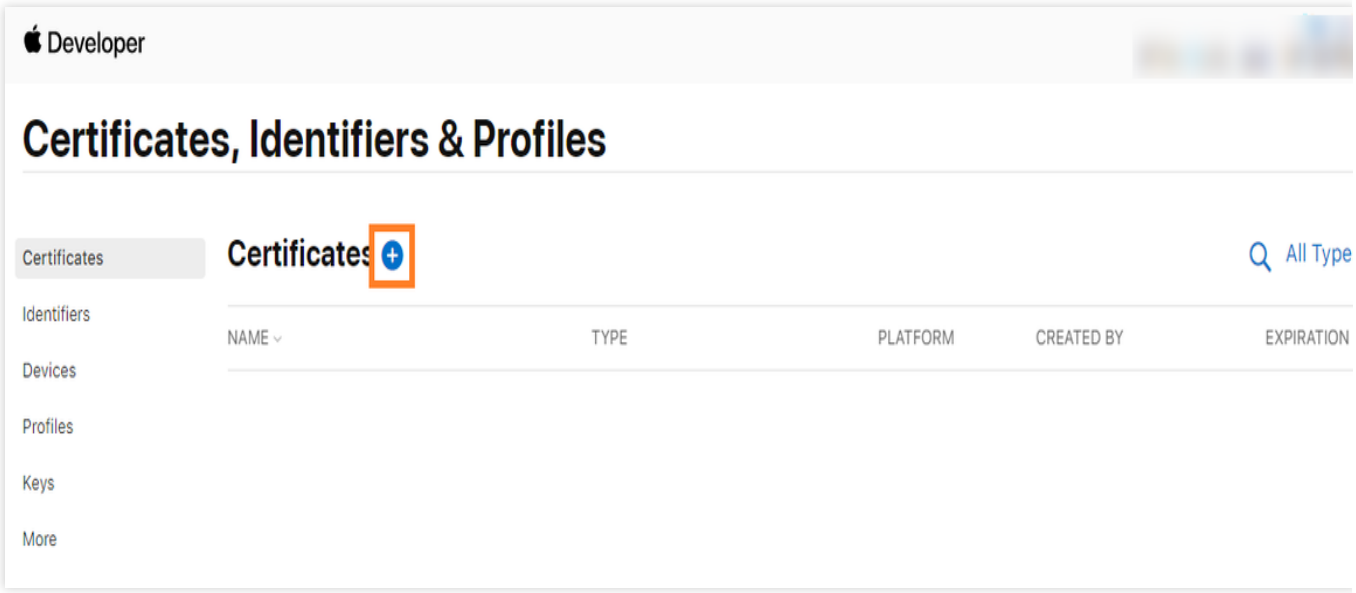
2.2 Enter the private key password configured in the previous step.

Step 3. Generate the FPS certificate

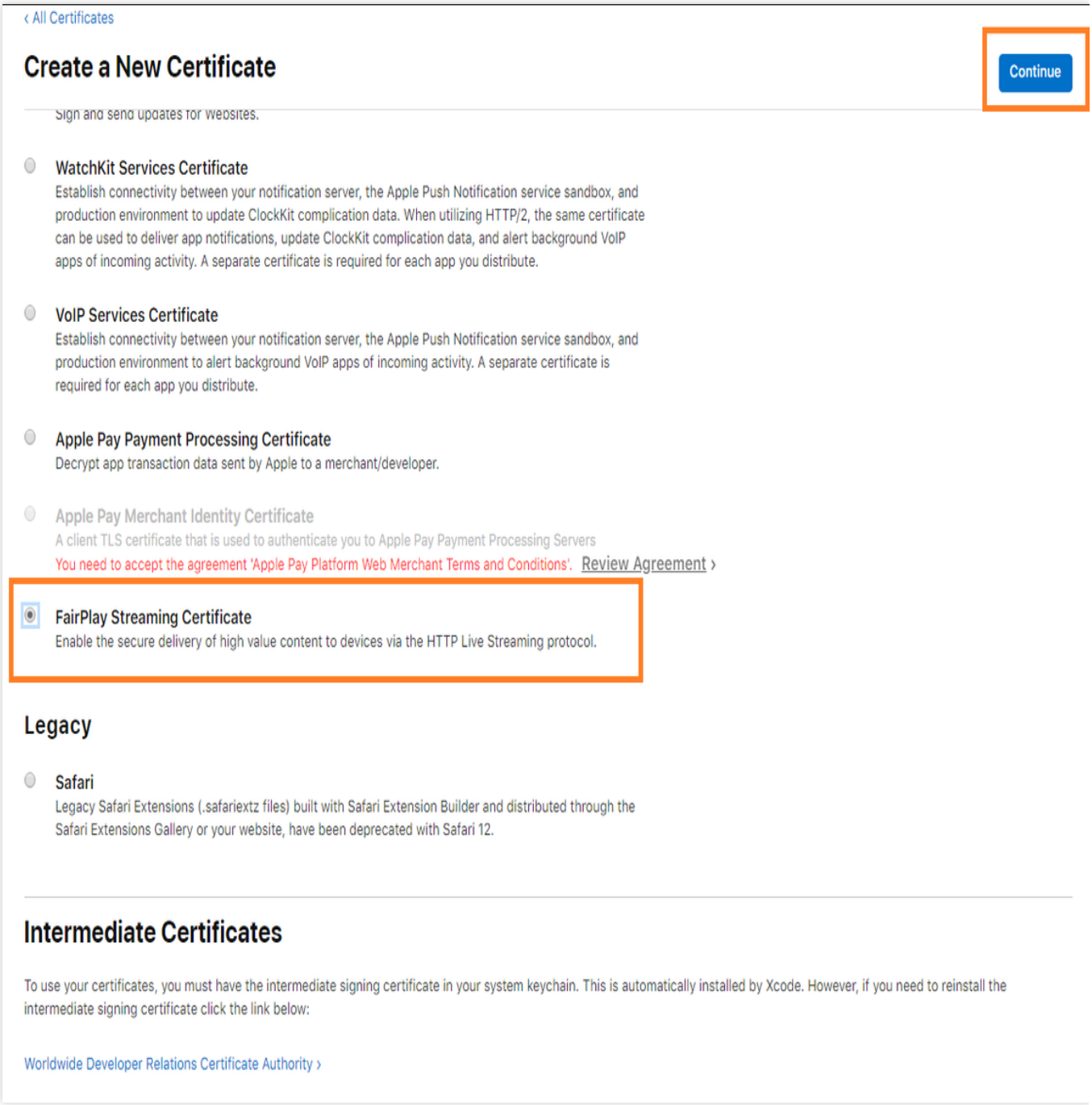
1. Log in to Apple Developer and click Certificates, IDs & Profiles.



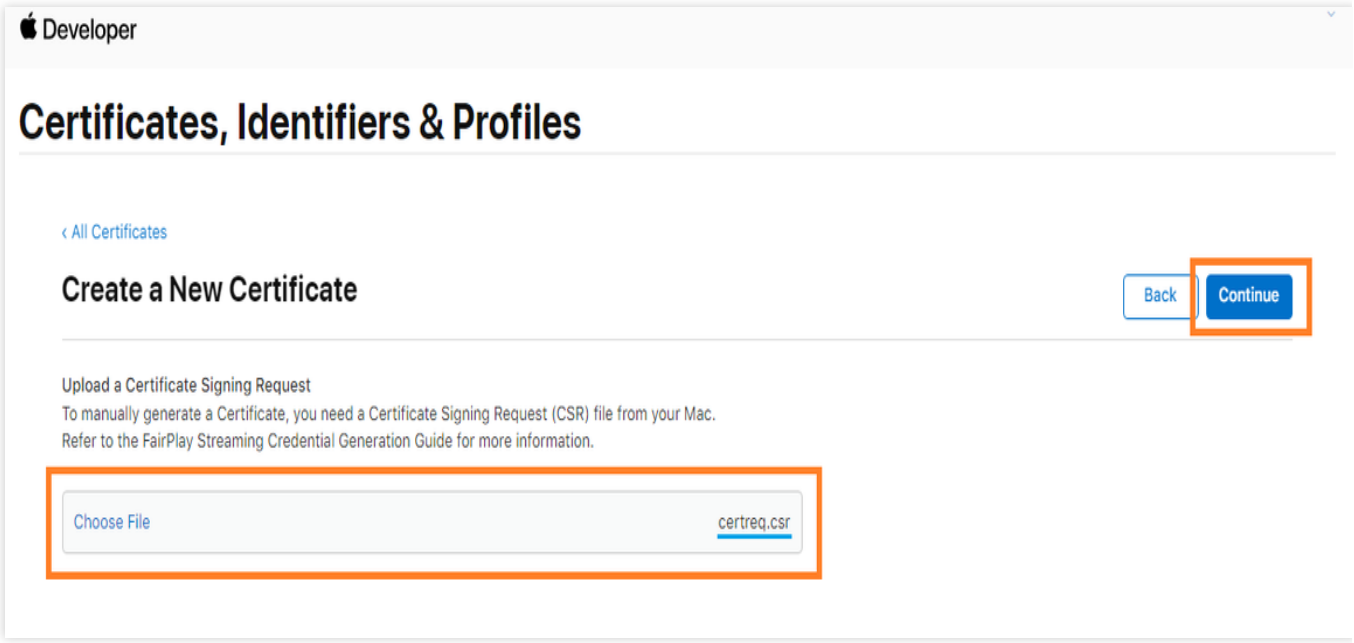
2. Click **+** to enter the **Create a New Certificate** page.



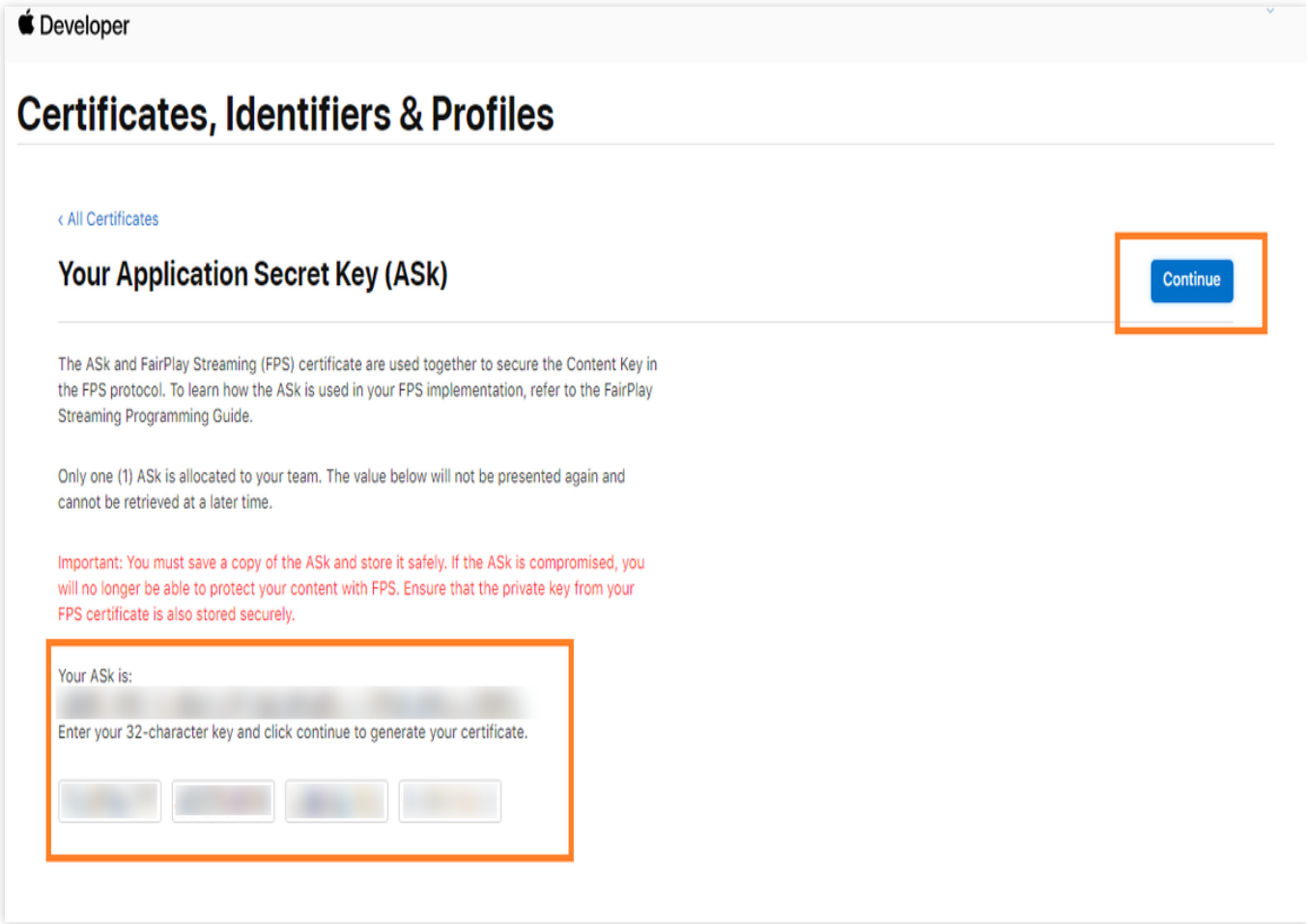
3. Select **FairPlay Streaming Certificate** and click **Continue**.



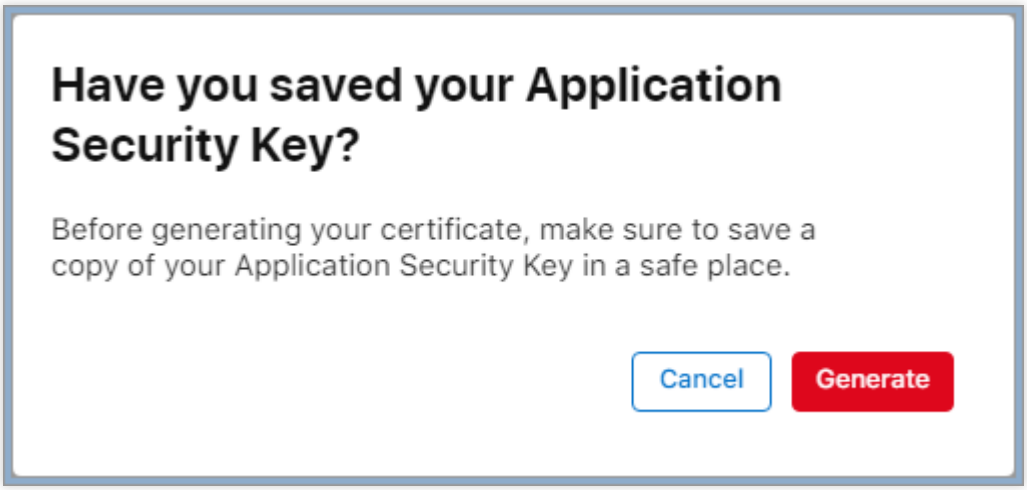
4. Click **Choose File**, select the `certreq.csr` file created, and click **Continue**.



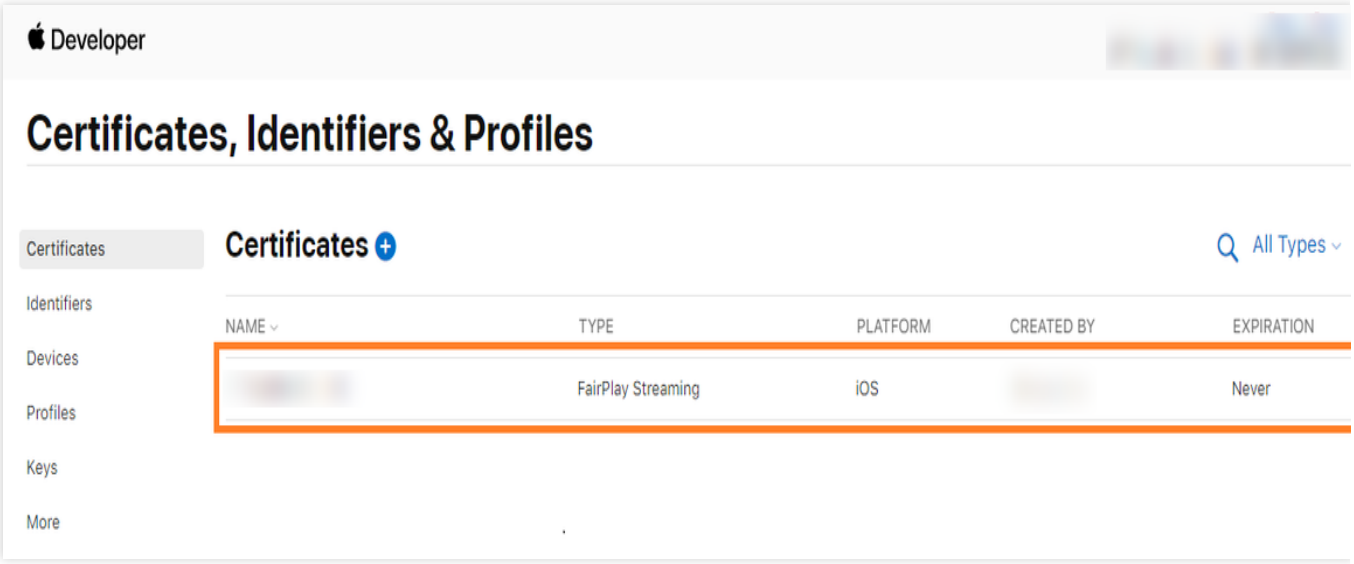
5. Copy and save the ASK, paste it in the input field below, and click **Continue**.



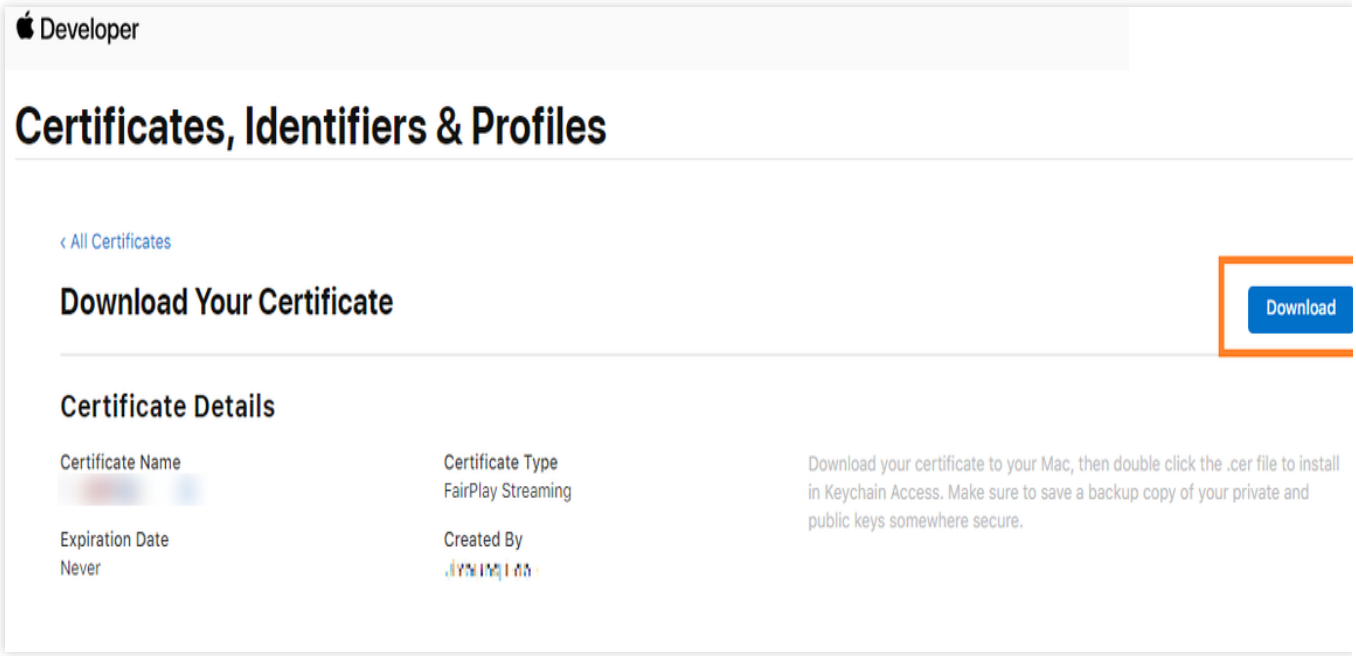
6. A window will pop up to confirm that you have saved the ASK. Click **Generate**.



7. After the above steps are completed, the FPS certificate generated will appear in the certificate list.

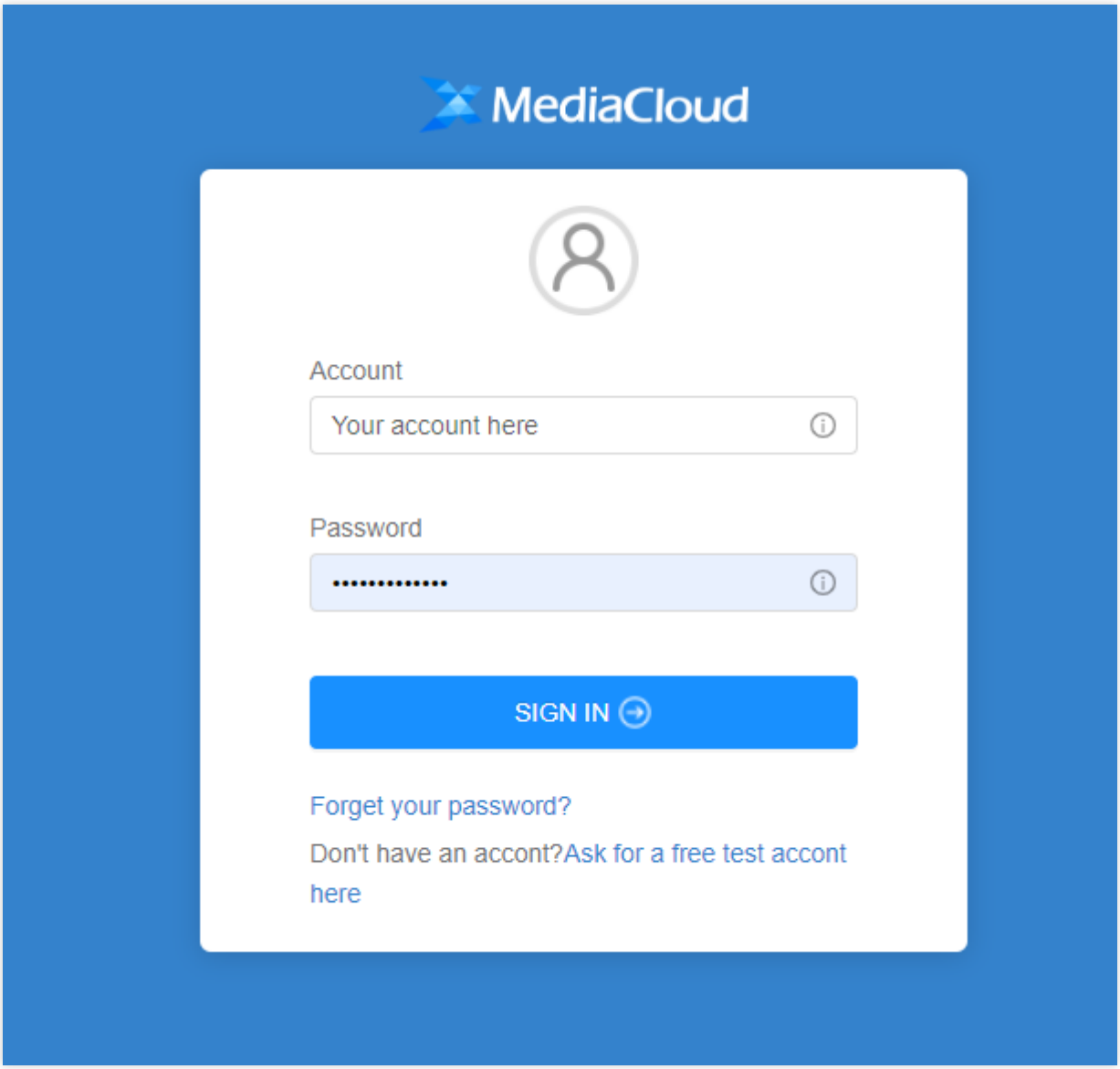


8. Click **Download** to download the FPS certificate (`fairplay.cer`).

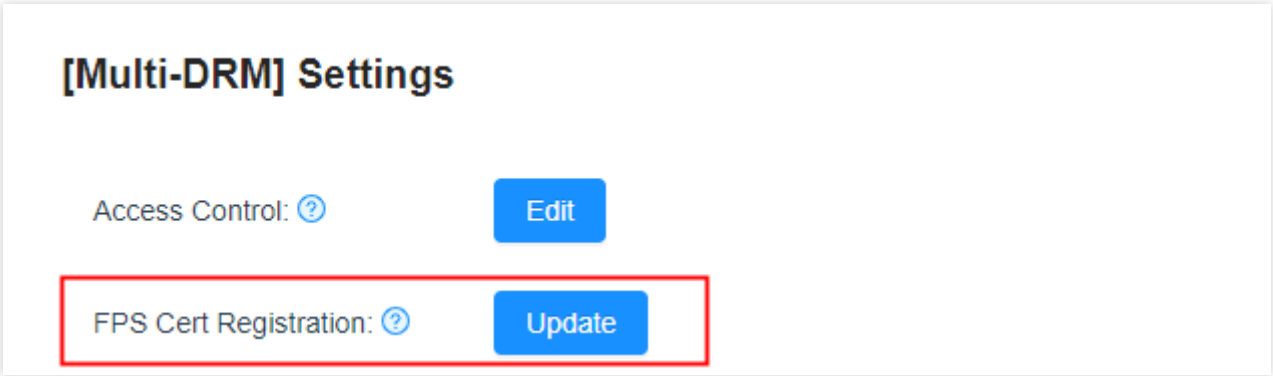


Step 4. Upload the certificate to SDMC's platform

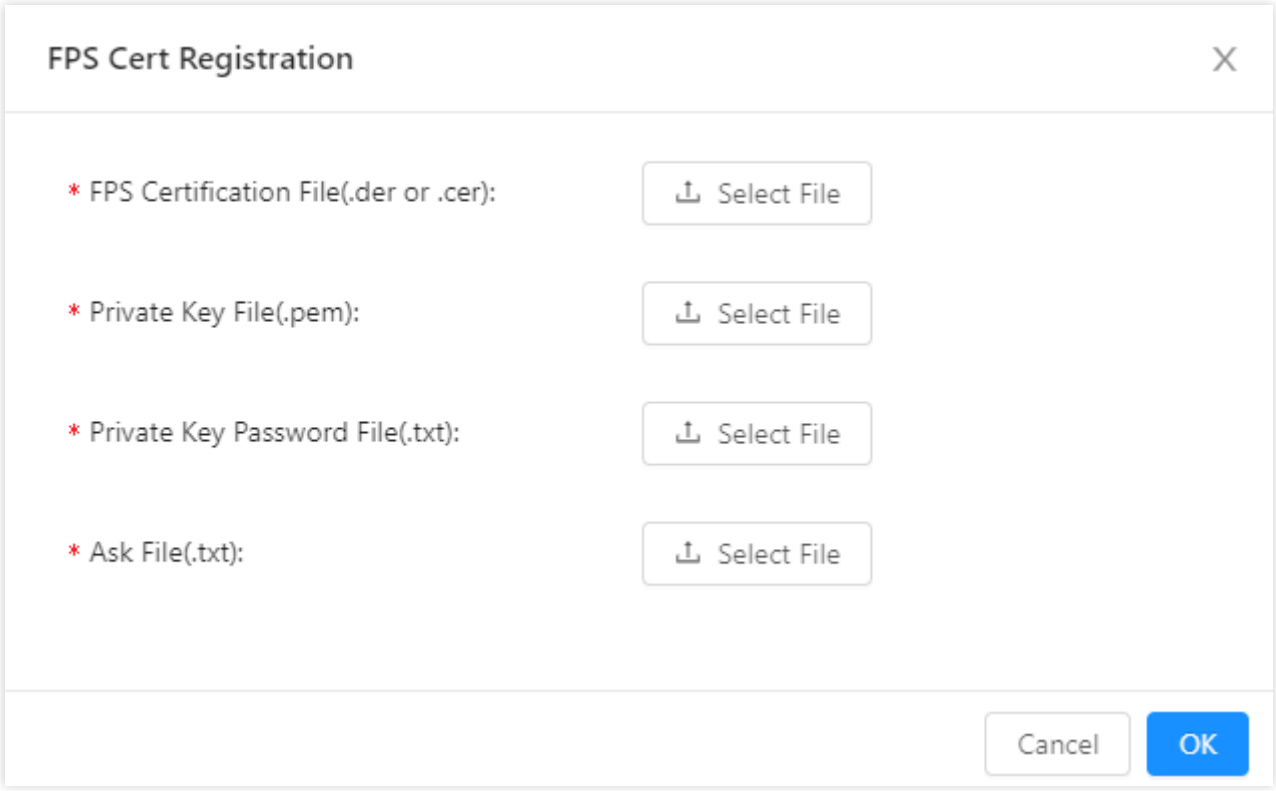
1. Log in to SDMC's DRM console and find DRM settings in the menu.



2. On the DRM settings page, find **FPS Cert Registration**, and click **Update**.



3. Upload the FPS certificate, private key file, private key password file, and ASK file, and click **OK**.



Note

If you have any questions, please submit a ticket.

Obtaining the UID and Key Information

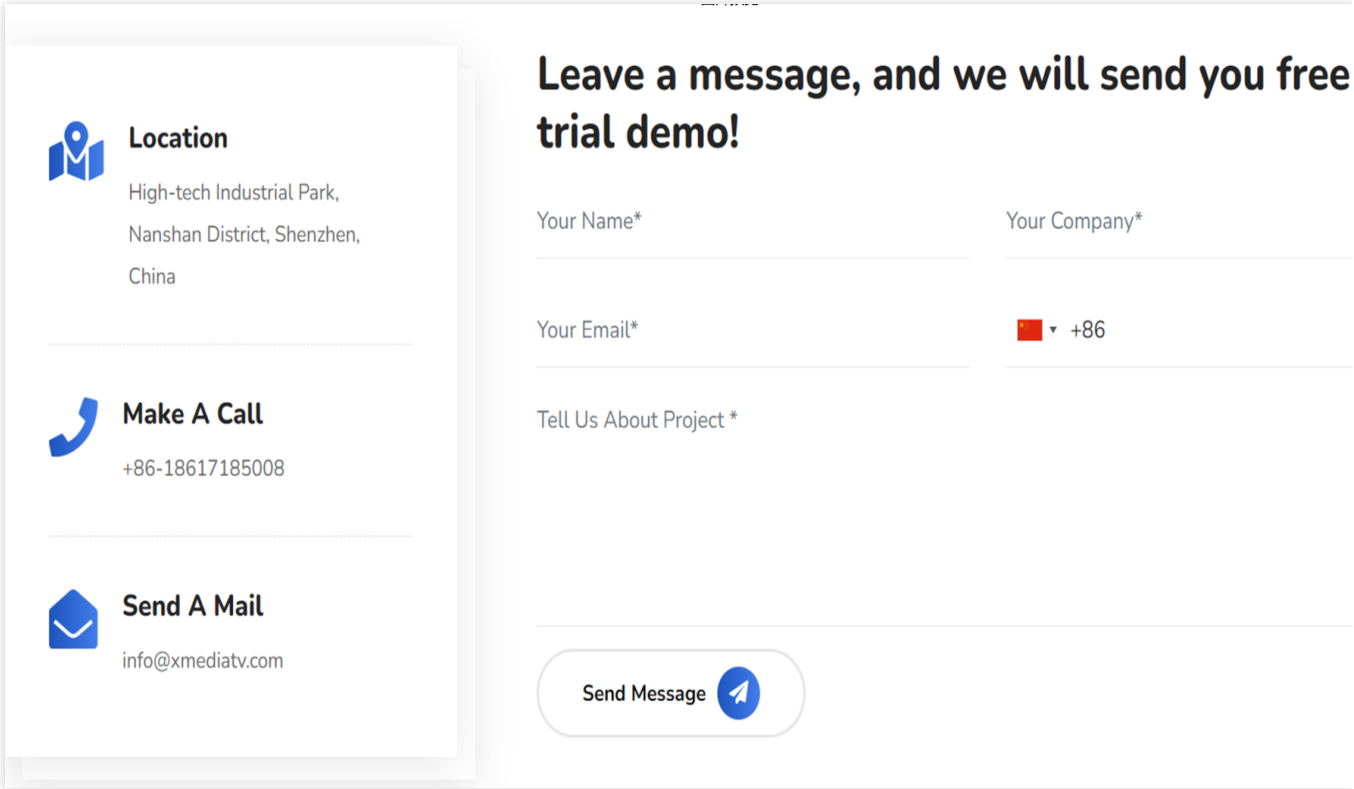
Last updated：2023-02-27 15:47:12

The licensing services of DRM encryption in CSS are provided by the third-party vendors SDMC and DRMtoday. To use DRM encryption, you need to provide CSS with your SDMC or DRMtoday user key. This document shows you how to obtain an SDMC or DRMtoday user key.

SDMC

Directions

1. Visit SDMC's DRM service registration page.



2. Enter your information and click **Send Message**. You will receive an acknowledgement email from SDMC in a few hours, and the company's salespeople will contact you to confirm your information.

Thanks for your interesting in our solution. This is XMediaTV Business Team from SDMC, taking charge of OTT platform & Cloud business. Glad to work togehter with you.

Regarding to your project, we have the corresponding solution to meet your requirements and we also have delivered many global similiar projects successfully. May i know your whatsapp or Skype to discuss directly?

who we are:

SDMC is invested by Tencent, which is one of the biggest internet company in China. SDMC and Tencent joint together launched Cloud Online Video SaaS platform TXMedia to provide high quality video streaming service to customers.

Grow your video business in:

We glad to invite you to video and audio streaming service community, here we freely sharing and answering any streaming related questions, helping you empower your video business by content share, white-label platform, video revenue model, cutting-ed infos....come and talk to our experts in:
Whatsapp group → https://chat.whatsapp.com/
Facebook group → https://www.facebook.com/groups/
Linkedin group → https://www.linkedin.com/groups/

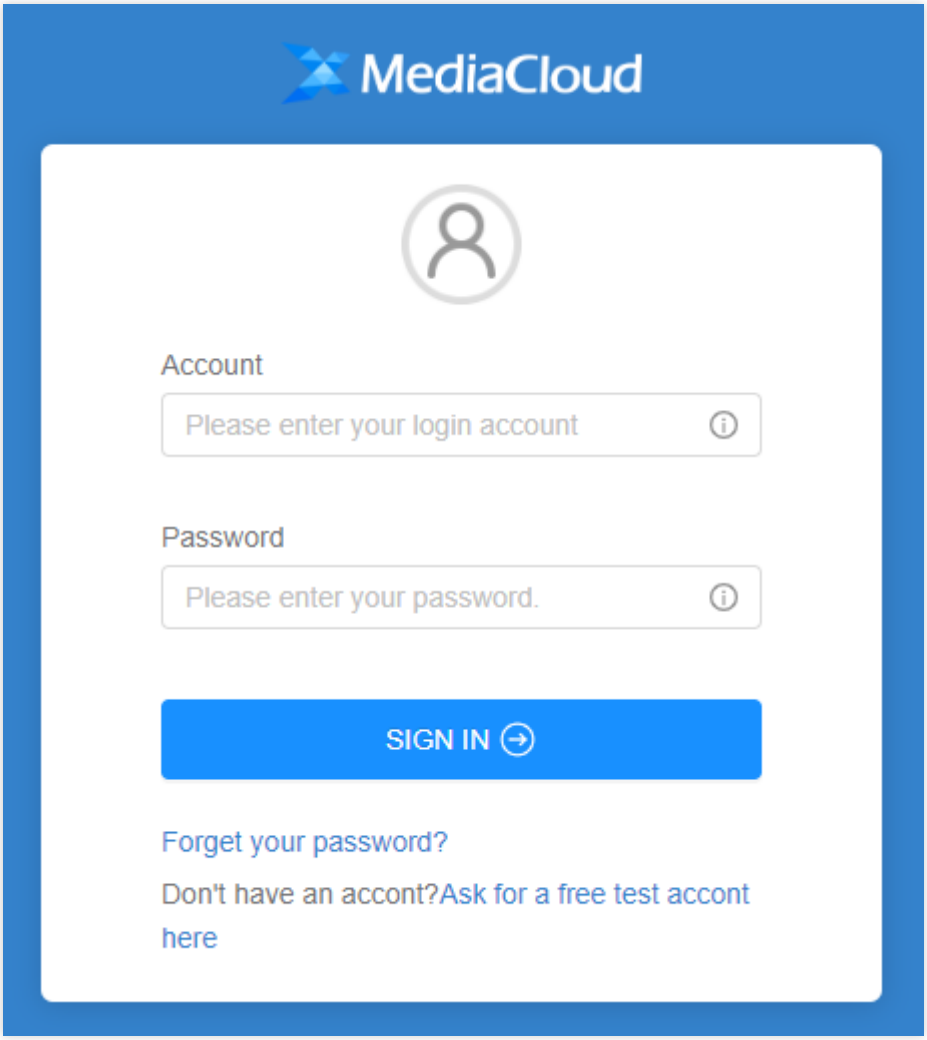
Know our streaming solution first!
SDMC XMediaTV Introduction V4.7 20210626.pdf

Please grab some time with me whenever you're ready - Schedule a Meeting

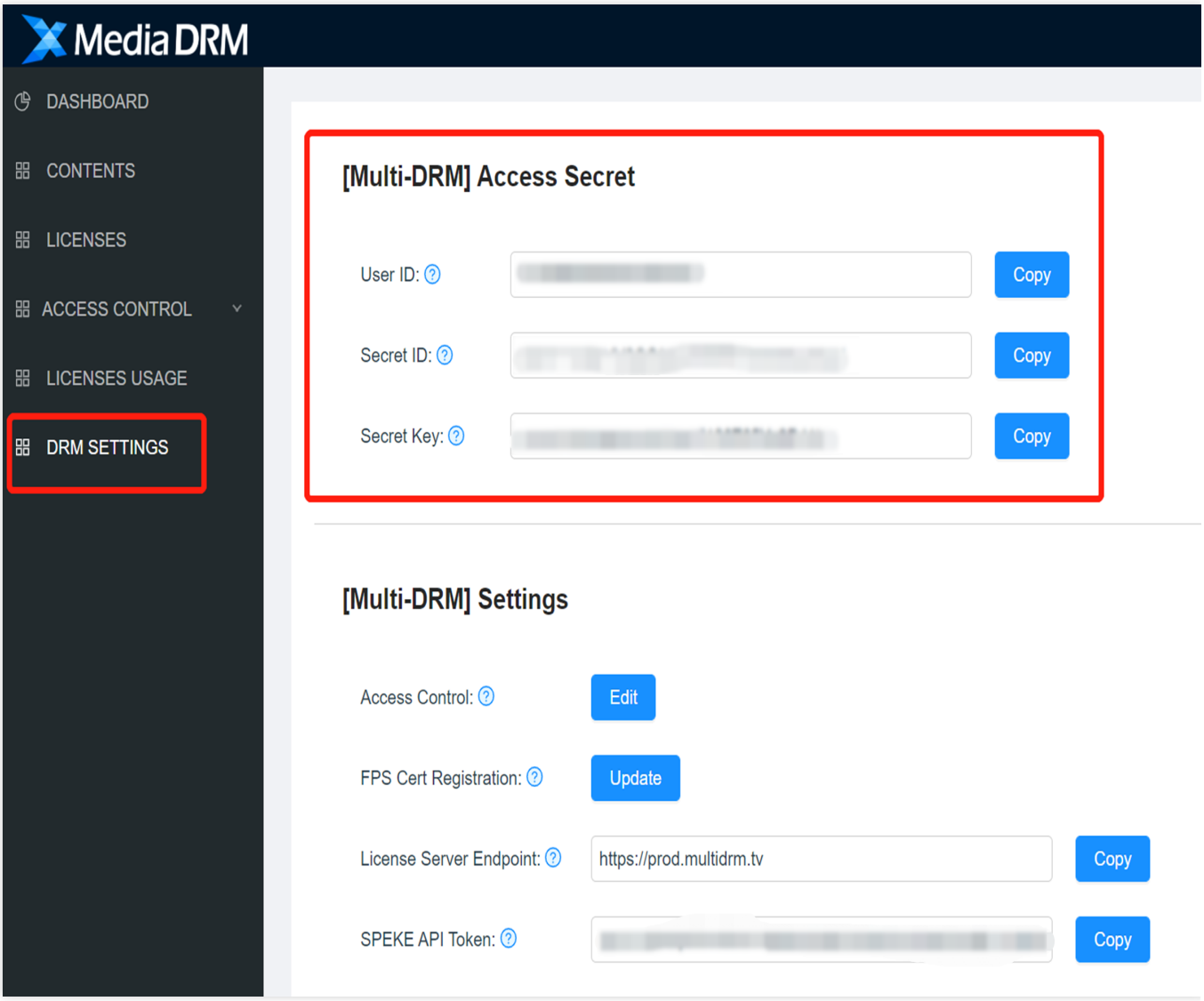
Best regards.

Xmedia Business Team

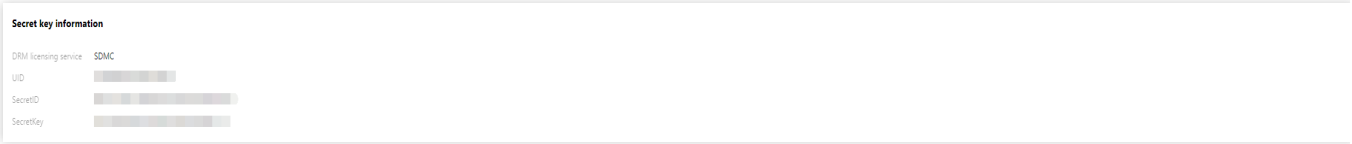
3. SDMC will review your application and email you the address of its DRM console and your initial password.
4. Log in to the SDMC DRM console with the account and password you received.



5. Click **DRM SETTINGS** to view your user ID, secret ID, and secret key.



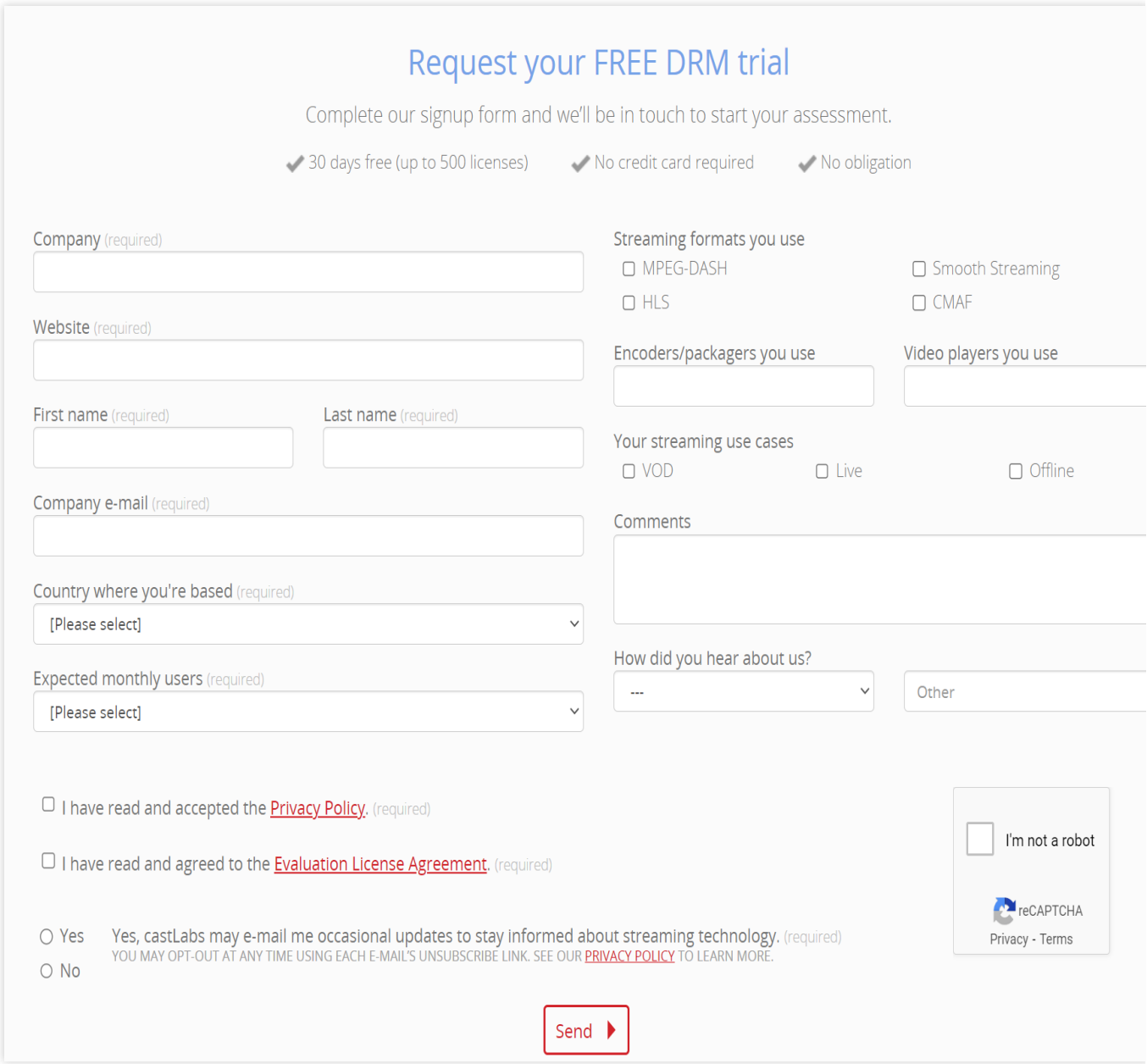
6. Go to DRM management of the CSS console and enter the information obtained.



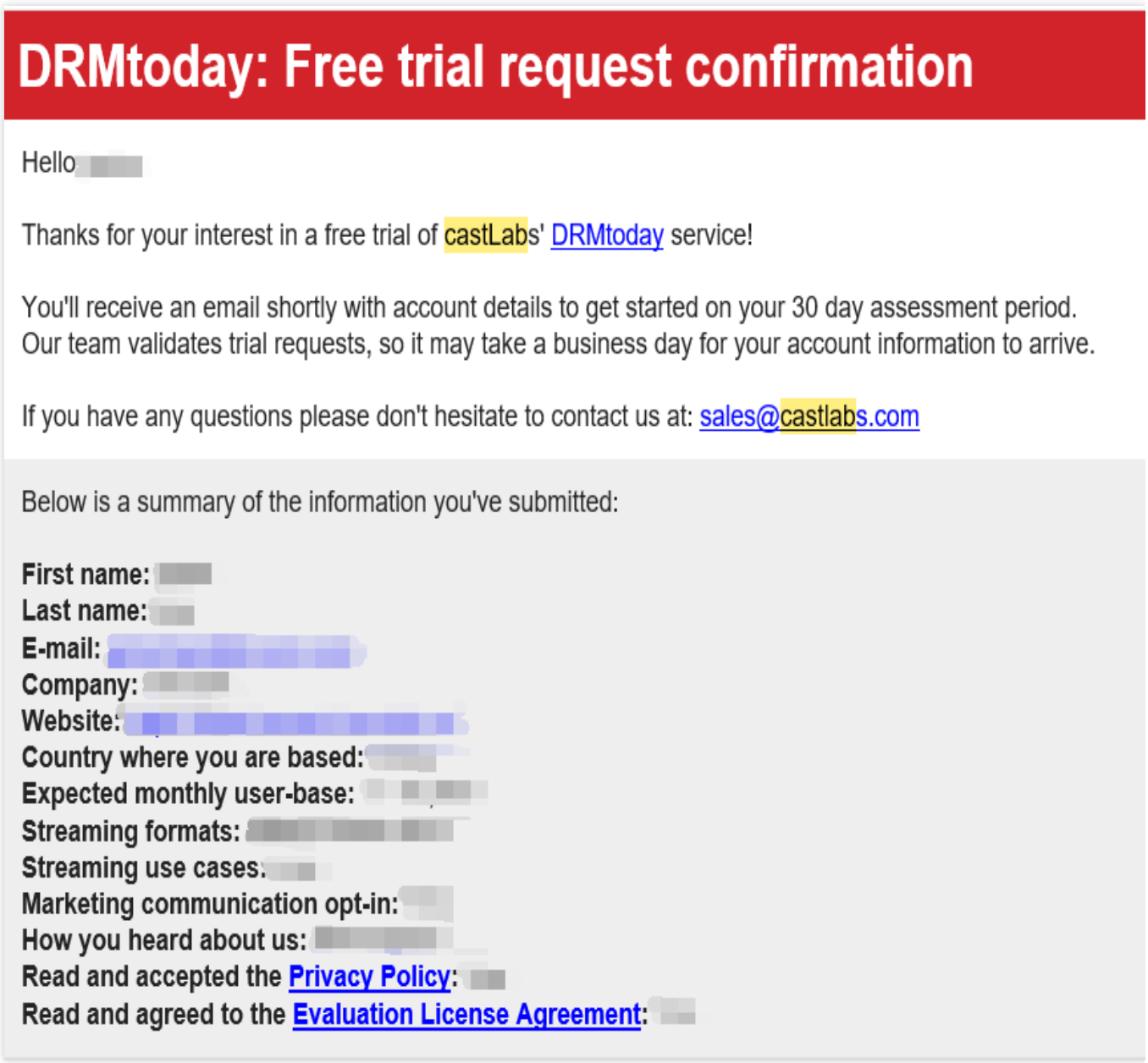
DRMtoday

Directions

1. Visit the DRMtoday website and fill in the information as required.



2. Click **Send**. Normally, you will receive a system email from DRMtoday within a few hours.



DRMtoday: Free trial request confirmation

Hello

Thanks for your interest in a free trial of castLabs' DRMtoday service!

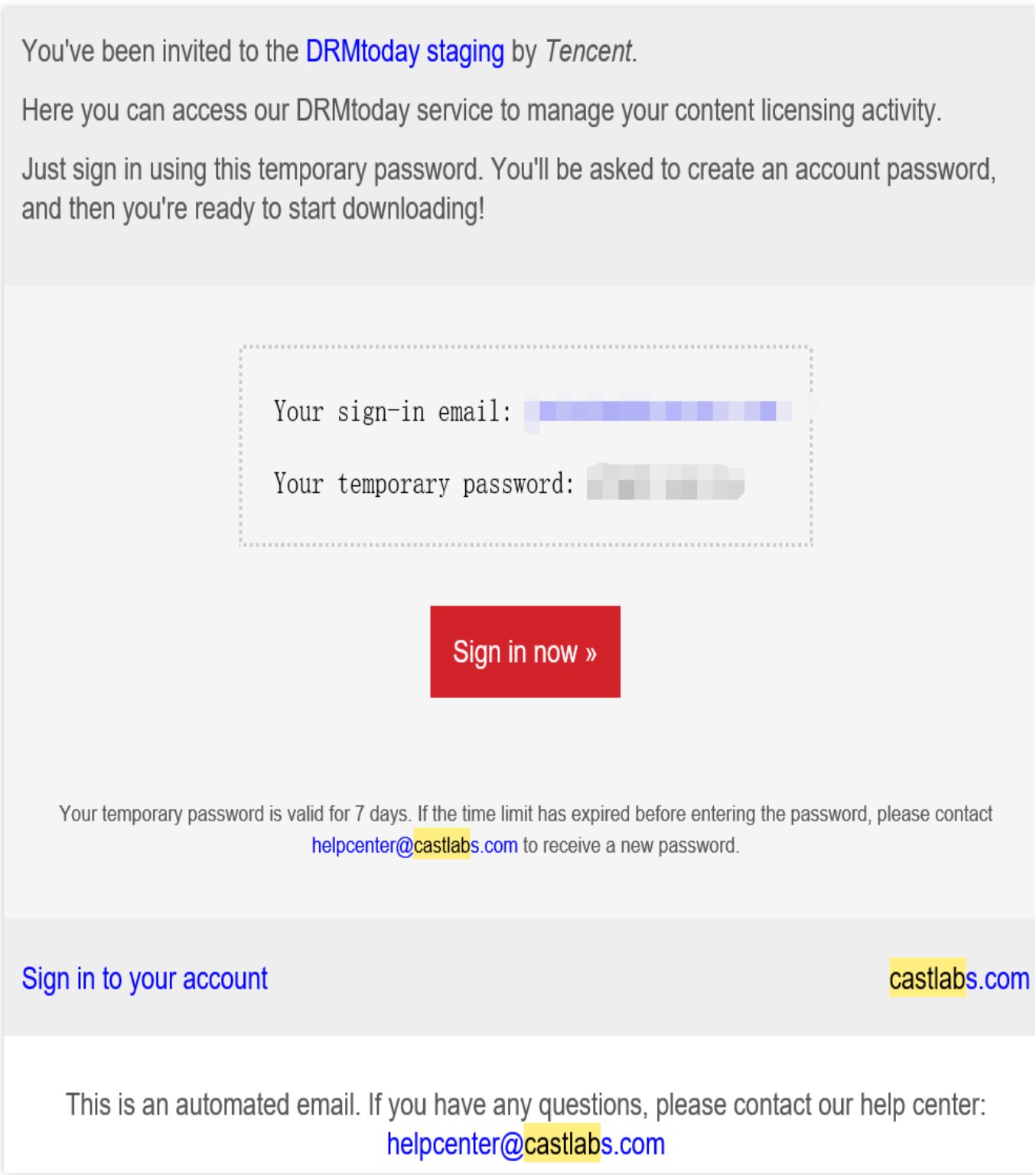
You'll receive an email shortly with account details to get started on your 30 day assessment period.
Our team validates trial requests, so it may take a business day for your account information to arrive.

If you have any questions please don't hesitate to contact us at: sales@castlabs.com

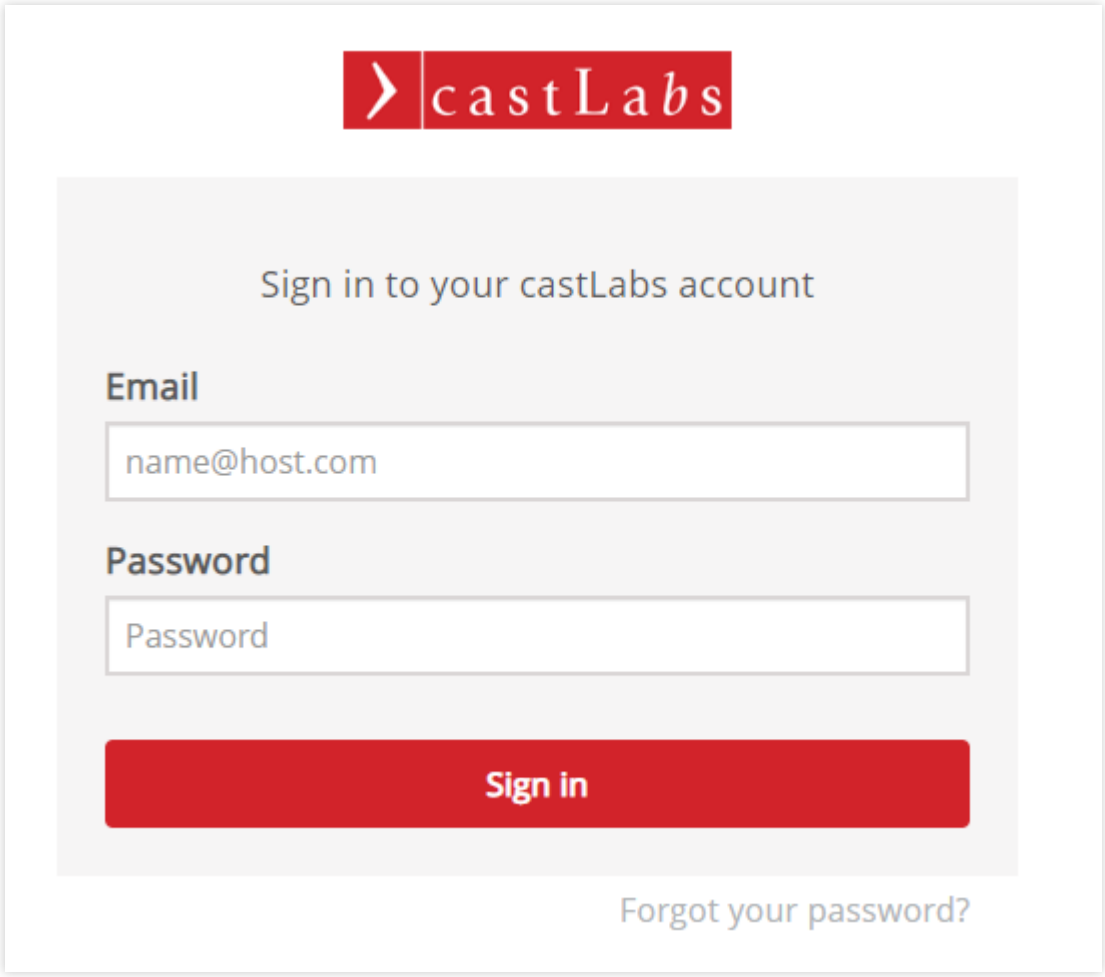
Below is a summary of the information you've submitted:

First name:
Last name:
E-mail:
Company:
Website:
Country where you are based:
Expected monthly user-base:
Streaming formats:
Streaming use cases:
Marketing communication opt-in:
How you heard about us:
Read and accepted the Privacy Policy:
Read and agreed to the Evaluation License Agreement:

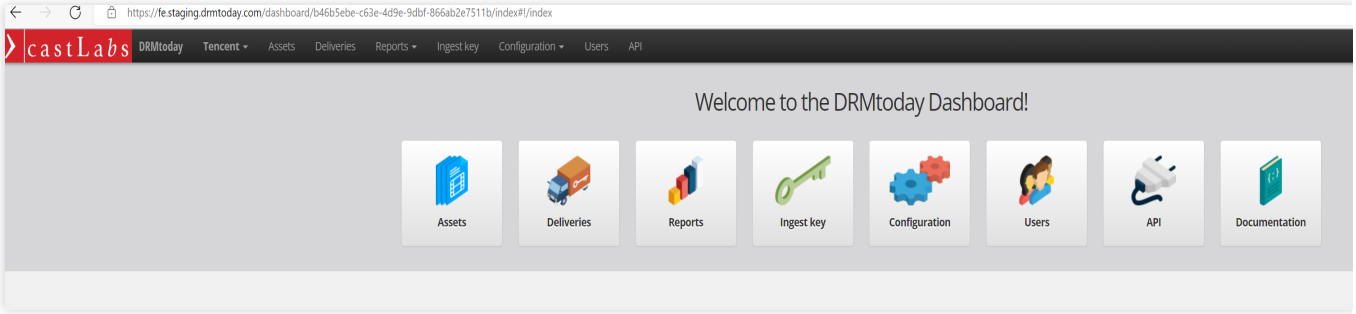
3. Shortly after that, DRMtoday will send you another email containing your account details.



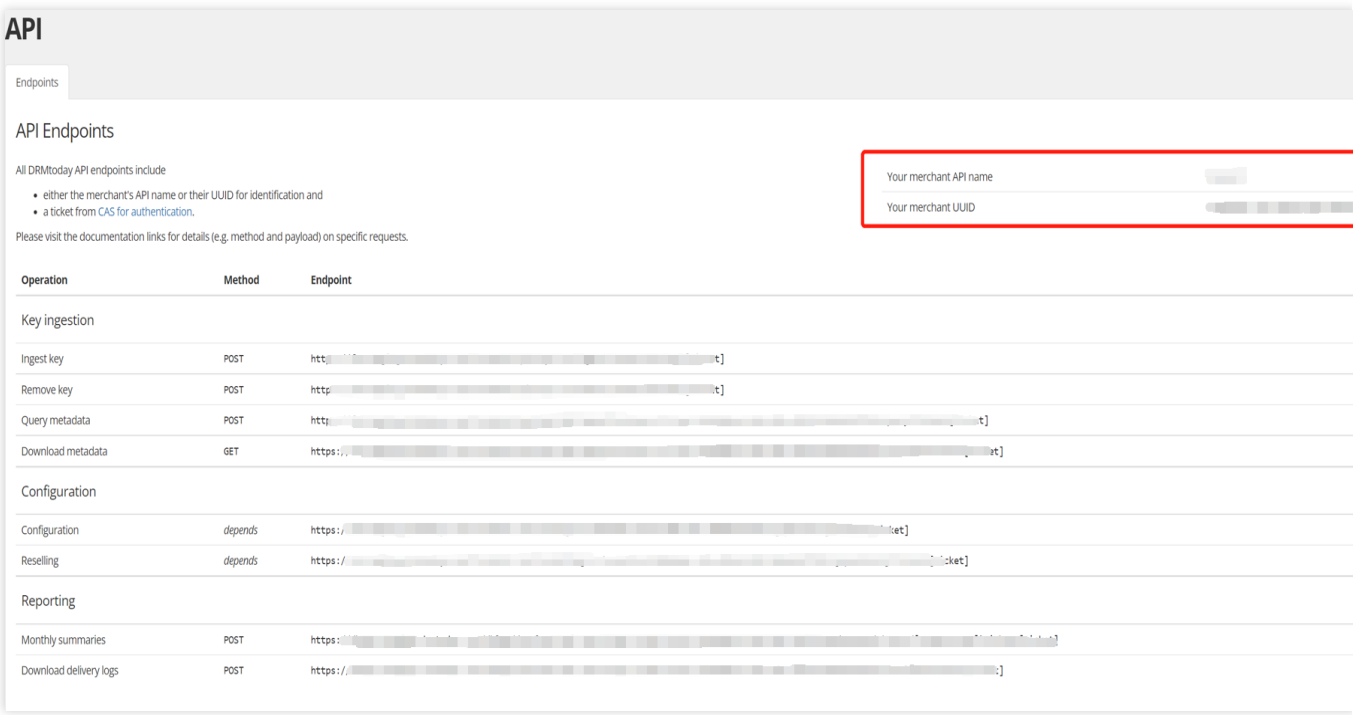
4. Visit the DRMtoday login page, enter your account, and create a password to log in.



5. You will enter the DRMtoday Dashboard.



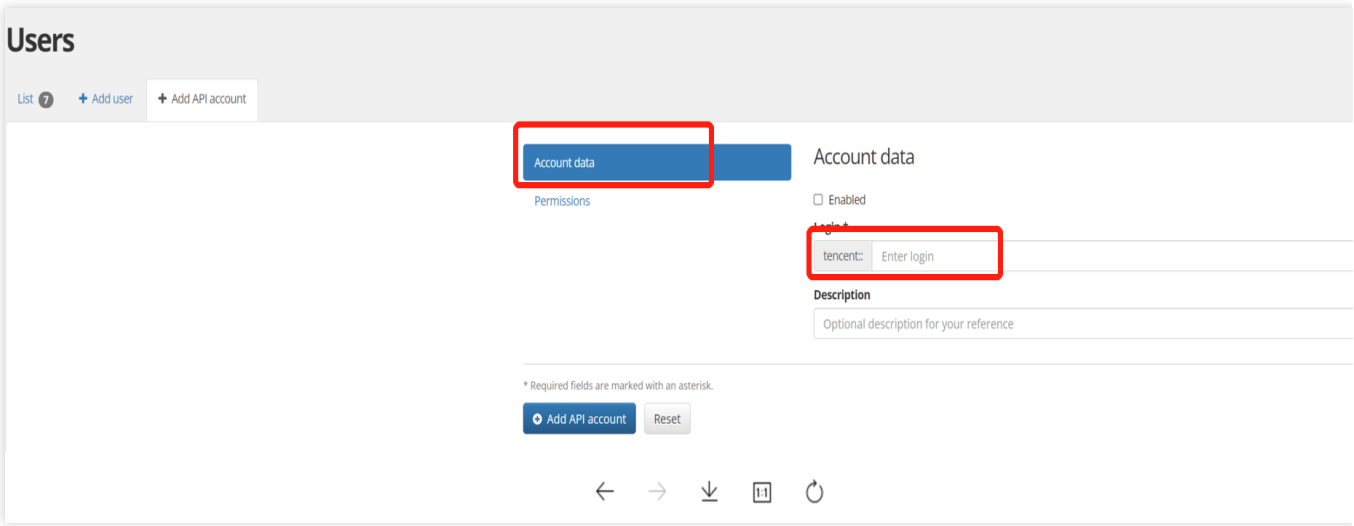
6. Click **API**. On the page below, note your merchant name and UUID.



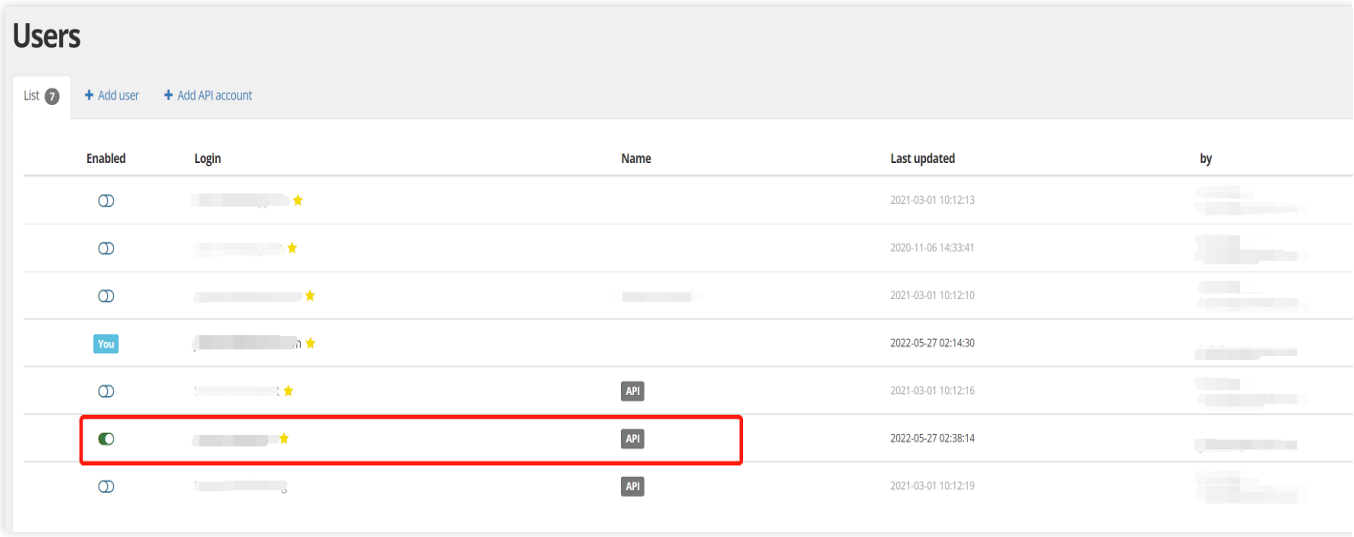
7. Go to the **Users** page. Add an API account, grant the permissions, and note the password.

Note:

The password will appear only once. Make sure you note your merchant API name and password.



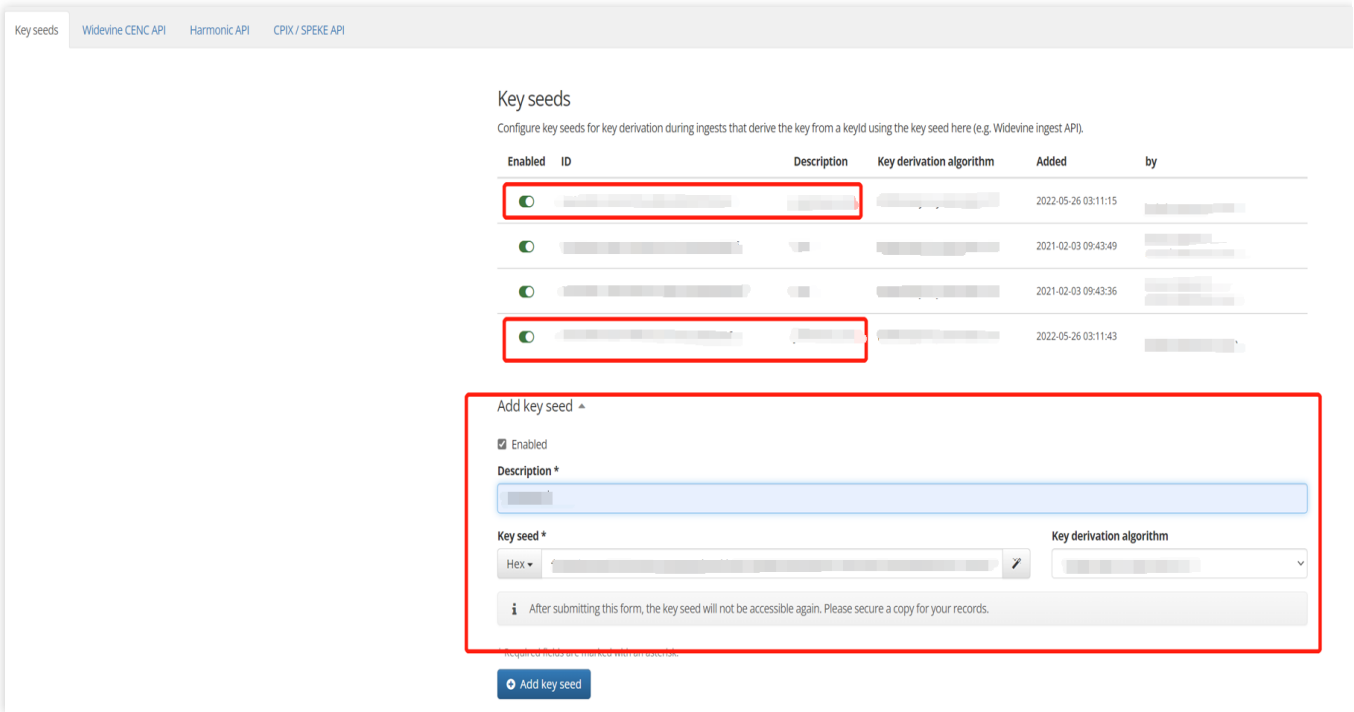
Enable the API account you created:



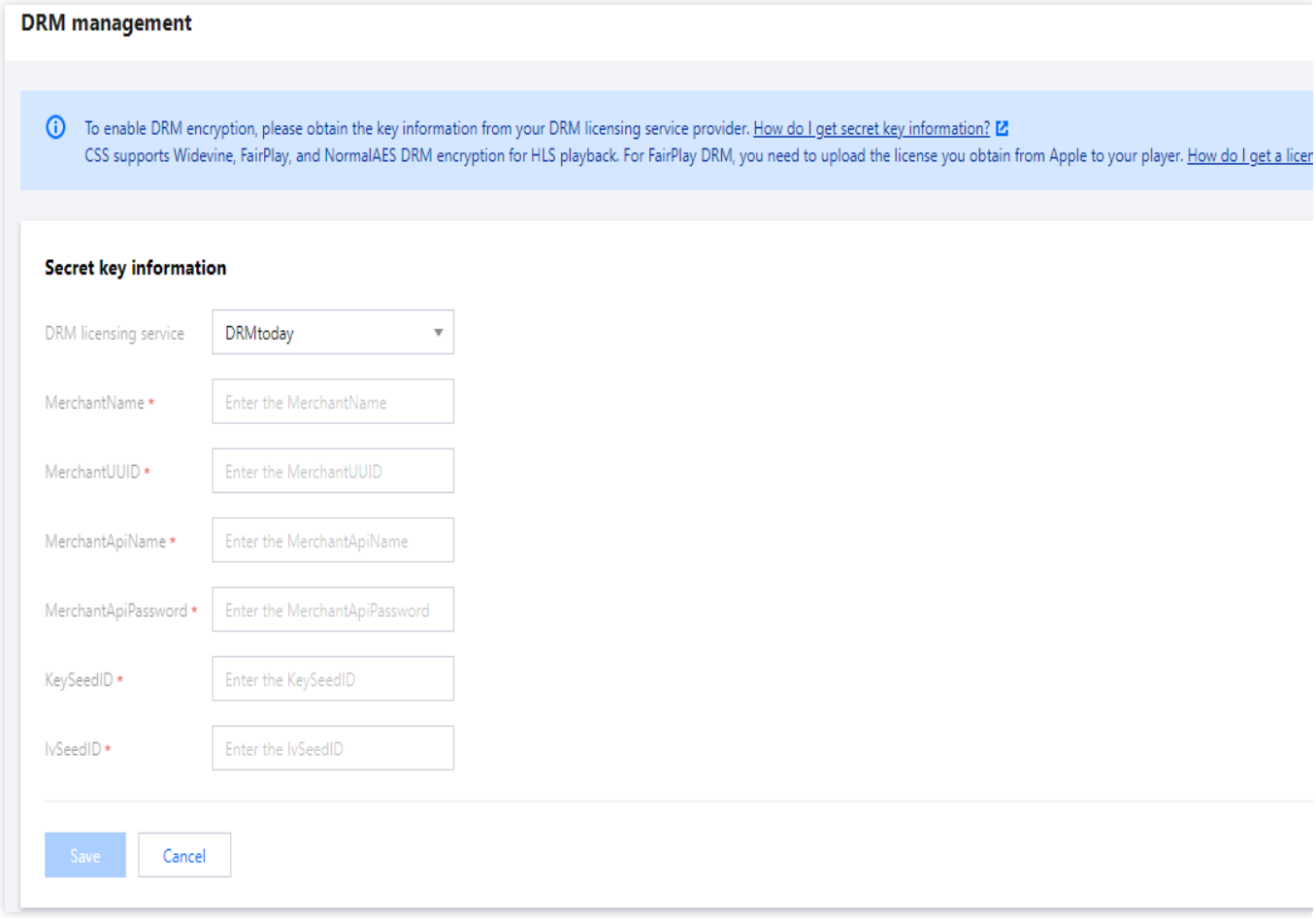
8. Go to **Configuration** > **Ingest Settings**. Add a key seed to generate the key (key seed ID) and IV (IV seed ID)

Note:

A key generated by a key seed can be viewed multiple times. You can provide it to your DRM encryption provider. For simple encryption with HMAC SHA512, you can use the key seed and key ID to generate an HMAC SHA512 string and use the first 16 characters of the string as the key or IV.



9. After obtaining the merchant name, merchant UUID, merchant API name, merchant API password, and key seed ID, and IV seed ID, enter the information in **DRM Management** of the CSS console.



Note:

If you encounter any problems while trying to obtain the above information, please submit a ticket. We will help you navigate the process.

Relay

Last updated：2025-04-18 15:32:47

If your live streaming source does not have the capability to push streams or if you want to stream on-demand videos, you can use the relay feature to quickly pull content from an existing live streaming source or video and then deliver it to the destination. You don't need to push streams yourself.

Prerequisites

You have activated CSS and logged in to the CSS console.
You have added a push domain name in the console.

Limits

You can create up to **200** relay tasks. If your relay business has a substantial volume and you require a larger task quota, contact us by submitting a service ticket, or seek assistance from our business manager.
The relay feature is charged based on the **duration of relay tasks**. For details, see Relay.
CSS is only responsible for pulling and relaying content. **Please make sure that your content is authorized and complies with relevant laws and regulations. In case of copyright infringement or violation of laws or regulations, CSS will suspend its services for you and reserves the right to seek legal remedies.**
The local relay mode became a paid feature starting from **00:00 on November 23, 2022**. To learn more, see Extended Features.
For relay, when pulling or pushing global streams, you need to set the task region to outside Chinese mainland.
You can use the relay recording function by binding a cloud streaming recording template, which will generate recording costs. The recording templates bound to the relay function only support templates that record the original stream content. To modify the recording template during a relay task, you need to halt the current task for 30 seconds before restarting it, only then can the new recording template take effect.
After the relay is bound to the transcoding template, the stream will first be pushed to CSS for transcoding, and then forwarded to the objective address of the task. The stream ID style of the push stream used for transcoding is "pp_relay task id", example: pp_12345678. Additional upstream push charges may be incurred. For the upstream push billing rules, please refer toUpstream Push Billing Instructions.

Creating a Task

1. Go to Relay, and click **Create Task**.

2. Enter the basic information:

Configuration Item	Description
Task Description	Describe the task.
Execution Time	By default, it is from `Current Time` to `Current Time + 24 Hours`. The optional range of execution time is any time within one year of the current time, but the duration cannot exceed 30 days. Assuming the current time is 11:34:28 on April 14, 2025, then: The optional time is from 11:34:28 on April 14, 2025 to 11:34:28 on May 14, 2025. The end time cannot exceed 11:34:28 on May 14, 2025.
Event Callback Notification	Enter a callback URL for receiving relay event notifications.

3. Provide the source information.

Region: Random (Chinese mainland), North China(Beijing), East China (Shanghai), South China (Guangzhou), Southeast Asia (Singapore), Southeast Asia (Bangkok), Northeast Asia(Tokyo), Northeast Asia (Seoul), Hong Kong/Macao/Taiwan (China) Hong Kong (China), West US(Silicon Valley),East US(Virginia),Europe(Frankfurt).
If you select **Random (Chinese mainland)**, the system will assign a region that is nearby.
4. For **Content Type**, you can select **Live streaming**, **Custom video path**, or **Image**.
4.1 **Live streaming**:
Enter a live streaming URL (**only one** is allowed).
You can select **Enable backup**.
In the event that the primary input source fails to retrieve content, an automatic switch to the backup input source will be initiated for content acquisition. If the backup input source's content type is live streaming, a manual switch back to the primary input source is required once it is restored. However, if the backup input source's content type is a custom video, the system will automatically revert to the primary input source upon completion of the current custom video playback cycle. The backup input source only supports the continuous loop playback of a single video.
Application scenarios: The backup source function is ideal for long-term live streaming tasks, preventing black screen viewing due to stream interruption, and providing backup sources and padding. For manual real-time switching of live

streaming scenarios, it is recommended to use the cloud director station function.

4.2 **Custom video path**:
You can enter **multiple** (max 30) source URLs.
Select **Repeat** to repeat the playback indefinitely or **Specified** to specify the number of times (1-100) to play the content.
If you enable local mode, sources in MP4 format will be cached to the local node before they are relayed. This ensures smoother and more reliable playback.

4.3 **Image**:
Upload an image or enter an image URL. You can click **Preview** to preview the image.
Images in JPEG, JPG, PNG, or BMP format are supported. If you enter an image URL, there is no limit on image size. If you upload an image, it cannot exceed 2 MB.
The file names of images to be uploaded only support letters, digits, and the following characters: `- ! _ . *`

Note:
The system will stop a relay task either when the playback count reaches the specified value or when the task reaches its end time.
In case of task modification:
If you change only the playback count, after the new value is applied, the count will start from 2.
If you change both the source URL and playback count, after the new configuration takes effect (whether immediately or after the current playback ends), the count will start from 1.
If you change the destination URL, the playback count will be reset.
Relaying a locally cached MP4 file will incur additional fees, which are based on the duration of the file relayed.
5. You can select **Watermark Configuration** ,**Transcoding Configuration**, and **Recording Configuration**. The configuration methods are as follows:
5.1 **Watermark Configuration:**
Click

to enable the watermark configuration. The PNG, JPG, and GIF watermark image formats are supported.

Set **Watermark Type**. You can select **Custom watermark URL** and **Upload image**.
For optimal visual effect, the watermark should be a transparent PNG image, with a file size less than 2 MB.
The file names of images to be uploaded only support letters, digits, and the following characters: `- ! _ . *`
Custom watermark URL
Upload image
Select **Custom watermark URL**, Enter the URL of the watermark image in the image address input field. By clicking on **Preview**, you can view the watermark in the preview section.

select **Upload image**, click **Select Image** Upload Watermark Image. The watermark image size supports full-window dimension stretching.

Configure the preview window size for watermark images:
Default dimensions: width 1920px, height 1080px.
Dimensional range: 360px to 4096px.
You can click the **Update** button on the right to perform automatic verification and synchronize the update of the watermark preview window.
Set the display position of the watermark image through the following methods.
Drag the image position on the watermark image configuration bar.
Configure the display position in the X-axis and Y-axis directions.

Note:
Enter the source information of the content. When the content type is image, the watermark configuration cannot be enabled.
Enabling the watermark function will generate transcoding costs.
When modifying the watermark, it takes effect immediately for live streaming source tasks, and for on-demand video source tasks, it takes effect starting from the next file. Modifying the watermark can cause playback to stutter. Usage scenario: It is recommended to use when relaying to a third-party origin server that does not have a watermark feature. For example, if you relay to CSS, you can use the live watermarking feature of CSS.
5.2 **Transcoding Configuration**:
Click

, select to enable the transcoding configuration, select a transcoding template, and click **Confirm**.

Note:

Enabling transcoding will incur live transcoding fees.

After the relay is bound to the transcoding template, the stream will first be pushed to CSS for transcoding, and then forwarded to the objective address of the task. The stream ID style of the push stream used for transcoding is "pp_relay task id", example: pp_12345678. Additional upstream push charges may be incurred. For the upstream push billing rules, please refer to Upstream Push Billing Instructions.

Turning on, off, or changing the transcoding template will take immediate effect. Modifications to the currently bound transcoding template in the pull task will only take effect after the task is restarted.

5.3 **Recording Configuration**

Click

to enable the recording configuration, select a recording configuration template, and click **Confirm**_.

Select a recording mode. You can select **Record and relay** or **Record only**.

Node:

Enabling recording will generate recording fees.

The recording templates bound to the relay function only support templates that record the original stream content. Templates for watermark streams and transcoding streams are not supported.

To modify the recording template during a relay task, you need to halt the current task for 30 seconds before restarting it, only then can the new recording template take effect.

If the recording template has been associated, it must first be unbound before being deleted. For unbinding procedures, refer to the unbinding recording configuration.

6. Enter a destination URL.
6.1 Click **Address Generator** to enter the URL generation page.
Click **Add** to add destination address 2.

6.2 Select an existing push domain, enter the `Appname`, `StreamName`, and expiration time, and click **Confirm** to generate a push URL, which will be auto-filled as **Destination Address**.

Note:
The URL expiration time must be later than the task end time. If you change the destination URL after the task starts, it will stop and restart.
7. Upon completing all configuration details, simply click **Save** to proceed.

Managing Tasks

Viewing Task Details

In the task list, find your task, and click its description/ID to view task details in the pop-up window.

Note:
You can click the buttons at the bottom of the pop-up window to **edit the task**, **switch sources**, **restart the task**, or **disable the task**.

Viewing Task Status

In the task list, find your task, and click its description/ID to view its execution status in the pop-up window.

Task Status	Field Value	Description
Not started	Inactive	The task has not started yet.
Valid	Active	The task has started and is executed as expected.

	Inactive	The task has started but is not executed as expected.
Disabled	Inactive	The task is disabled.
Expired	Inactive	The task has expired.

Querying Streaming Data

In the task list, select the successfully created relay task, and click **Streaming data** in the **Operation** column on the right to query the streaming data of the relay task. The event display information includes the event type, content type, time, source IP, target IP, and detailed information.

The streaming data query page of a relay task allows you to query the data of a single stream in the past seven days, including the video frame rate, video bit rate, audio frame rate, and audio bit rate.
The interval between the start and end time of the query should not exceed 3 hours.

Modifying a Task

1. In the task list, find the task you want to modify, and click **Edit**.

2. Modify the task information, and then click **Save**.
You cannot change the region or content type.
When modifying the task end time, make sure that the destination URL is valid until the task ends. Modifying the destination URL will cause the task to stop and restart.
If you change watermark settings for a live streaming source, the modifications will take effect immediately. For an on-demand video source, modifications to watermark settings will take effect starting from the next video. Modifying watermark settings may cause playback to stutter. We recommend you use the watermark feature for relay only if you relay to third-party sites that do not have watermarking capabilities. If you relay to CSS, you can use the live watermarking feature of CSS.
The recording templates bound to the relay function only support templates that record the original stream content. To modify the recording template during a relay task, you need to halt the current task for 30 seconds before restarting it, only then can the new recording template take effect.

3. In the pop-up window, check the information:
Suppose you modified the **start time, end time, and playback count** of a task. You would see the following information in the pop-up window:

If the source URLs for **Custom video path** are changed, you need to select whether to apply the change **After the current video ends** (default) or **Now**. After the changes take effect, relay will restart from the first source URL.

If **Destination Address** is changed, the system will remind you that after you click **Confirm**, the current relay task will **stop and restart**.

4. After checking, click **Confirm**.

Copying a Task

1. In the task list, find the relay task you want to copy, and click **Copy**. You will be directed to the task creation page.

2. The information of the copied task will be auto-filled. You can **modify** it as needed.
3. Click **Save** to create a new relay task.

Restarting a Task

Restarting a task will **not change its status**. An ongoing task will be **restarted from the beginning**. Perform the following to restart a task:
1. In the task list, find the relay task you want to restart, and click **Restart**.

2. In the pop-up window, click **Restart**.

Disabling a Task

If you disable a task, **the task will stop**. You can click **Enable** to start it again. Perform the following to disable a task:

1. In the task list, find the relay task you want to disable, and click **Disable**.

2. In the pop-up window, click **Disable**.

Enabling a Task

If you enable a task, **the task will start from the beginning**. Perform the following to enable a task:

1. In the task list, find the relay task you want to enable, and click **Enable**.

2. In the pop-up window, click **OK**.

Deleting a Task

Deleted tasks **cannot be recovered**. Perform the following to delete a task:

1. In the task list, find the relay task you want to delete, and click **Delete**.

2. In the pop-up window, click **Delete**.

Batch Operations

You can delete, disable, and enable **up to 10 relay tasks** at a time.

1. In the task list, select the relay tasks you want to delete, disable, or enable.
2. Click **Batch Operation**, and select **Enable**, **Disable** or **Delete**.

3. In the pop-up window, click **Enable**, **Disable** or **Delete**.

Auto-Deleting Expired Tasks

A task expires after its end time. If you have too many relay tasks, you may fail to create new ones. To avoid this, you can enable auto-delete for the system to delete expired tasks automatically at the specified time. Deleted tasks cannot be recovered.

1. Go to Relay, and click **Set** in the **Expired** area.

2. Click

to enable auto-delete.

3. Specify a period (1-24 hours) to retain expired tasks before they are deleted.

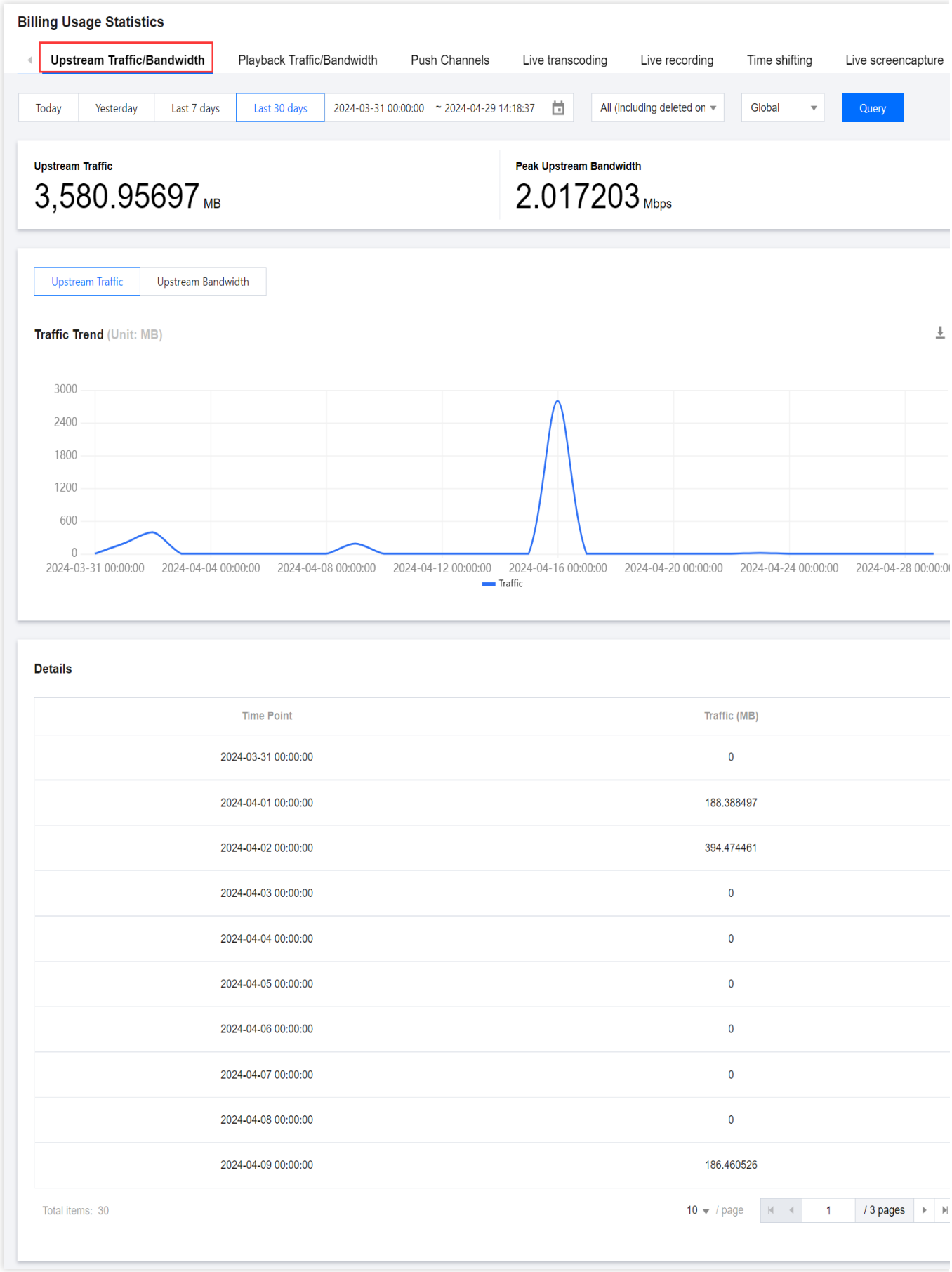
Billing Usage Statistics

Last updated：2024-09-12 14:07:24

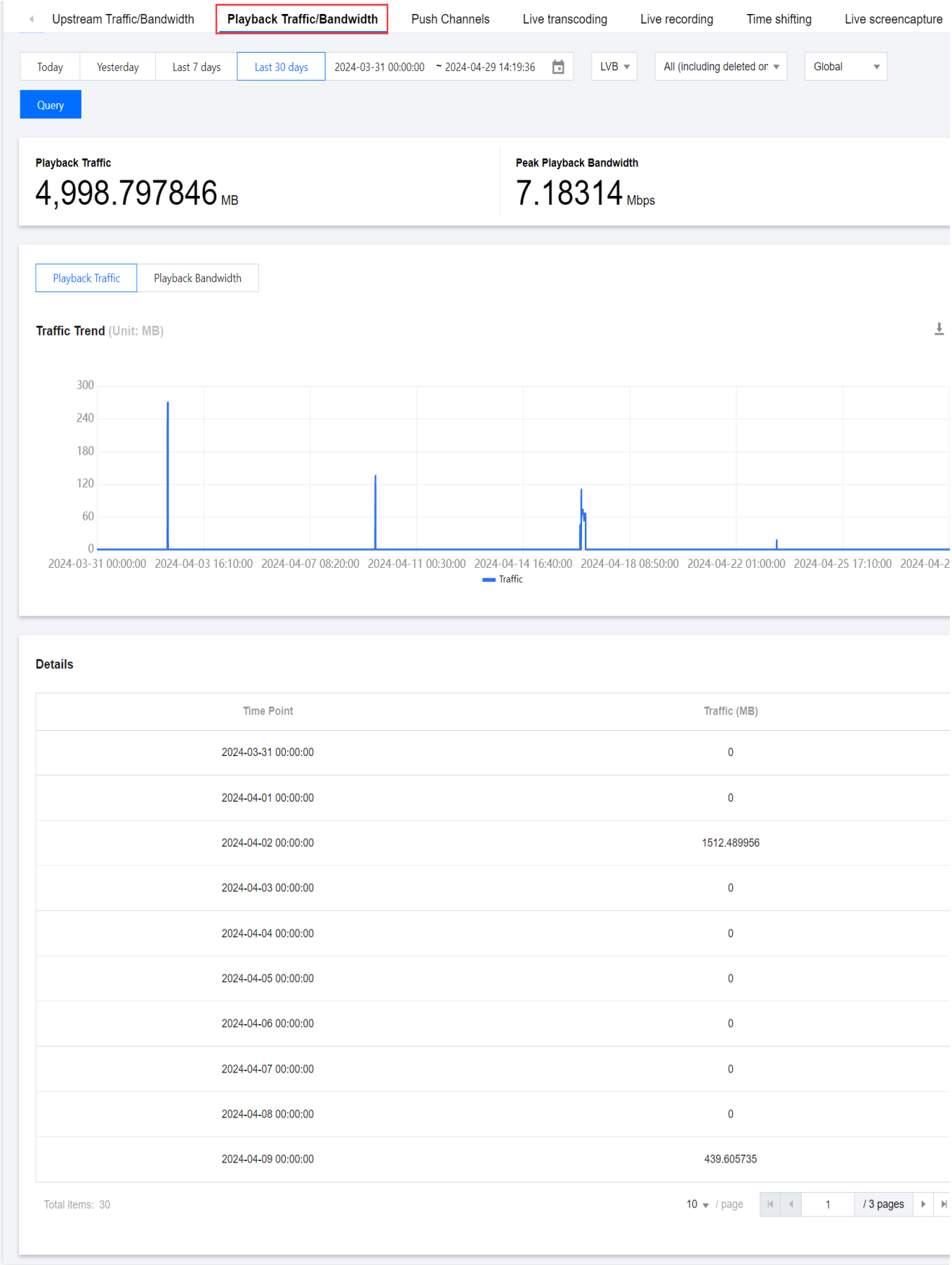
Billing usage statistics

The Tencent Cloud console provides a billing usage statistics query feature for Live Video Broadcasting (LVB) and Live Event Broadcasting (LEB). If you want to know the usage of services such as upstream traffic/bandwidth, playback traffic/bandwidth, push channels, live transcoding, live recording, time shifting, live screencapture, enhancement, content moderation, relay task duration, third-party relay, real-time log, and DRM encryption, you can view the relevant data in **Statistics** > Billing Usage Statistics in the Cloud Streaming Services (CSS) console. You can view data related to CSS service usage in the last month.

Upstream Traffic/Bandwidth
Playback Traffic/Bandwidth
Push Channels
Live transcoding
Live recording
Time shifting
Live screencapture
Enhancement
Content moderation
Relay task duration
Third-party relay
Real-time Log
DRM encryption



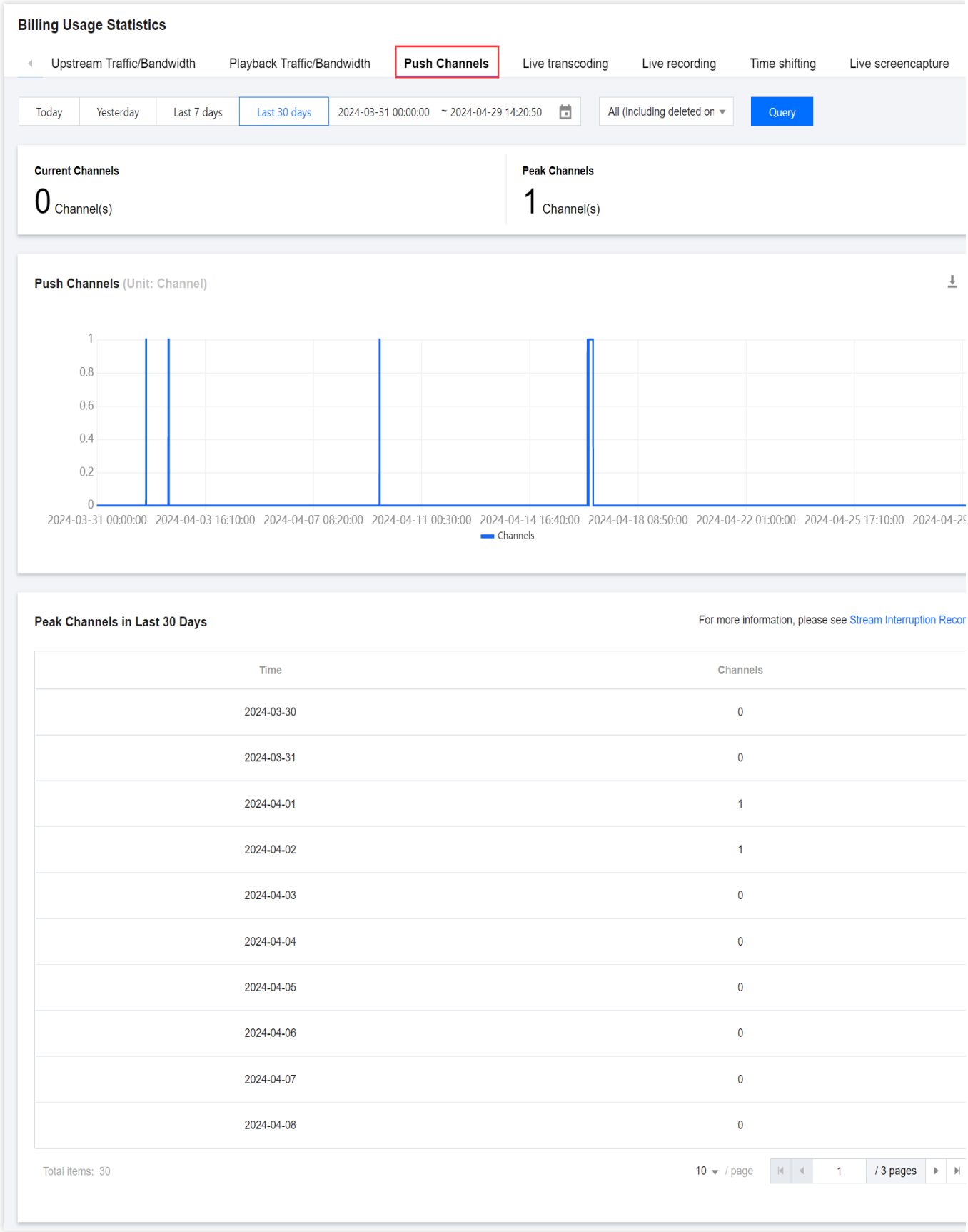
Billing Usage Statistics

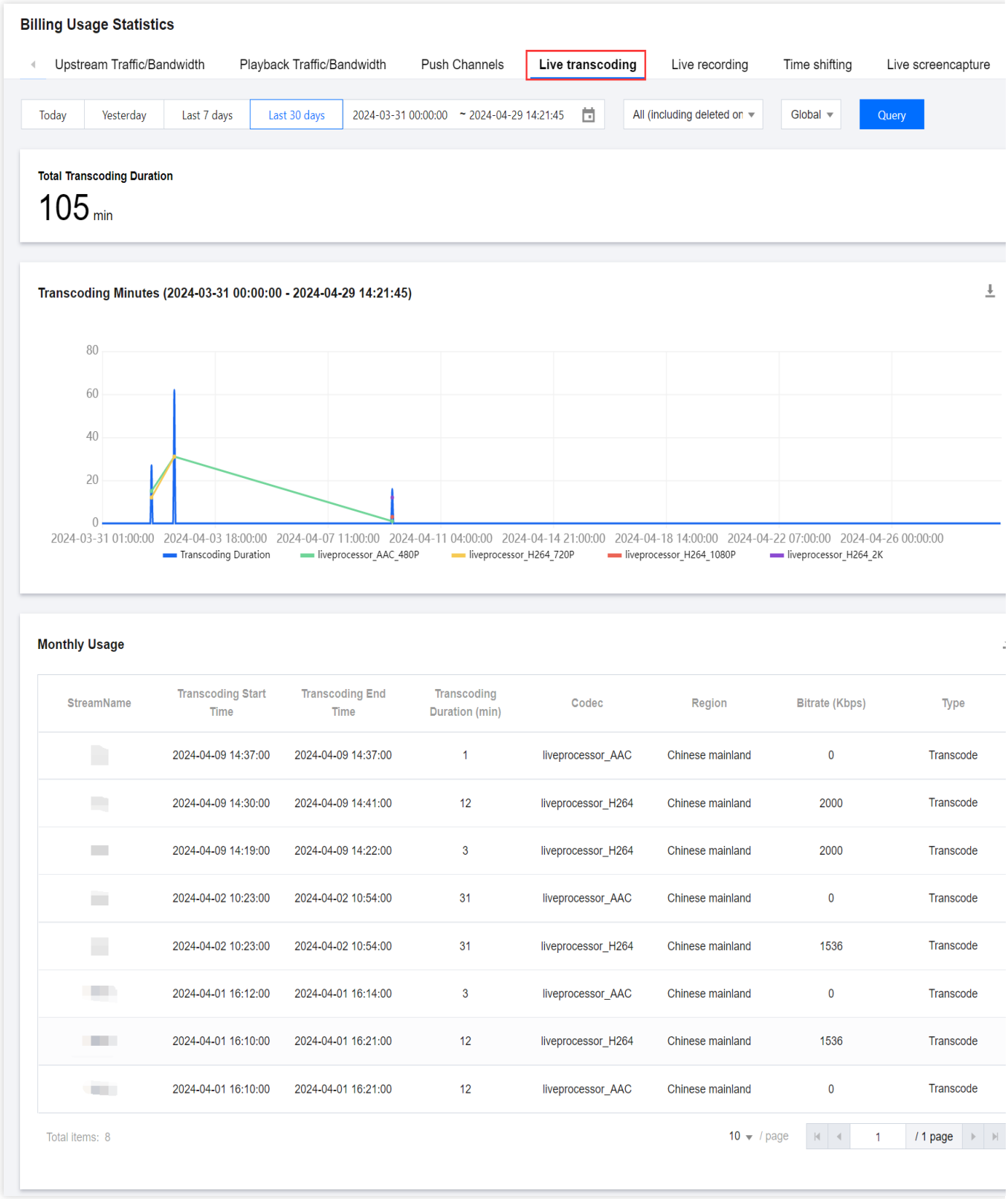


Details

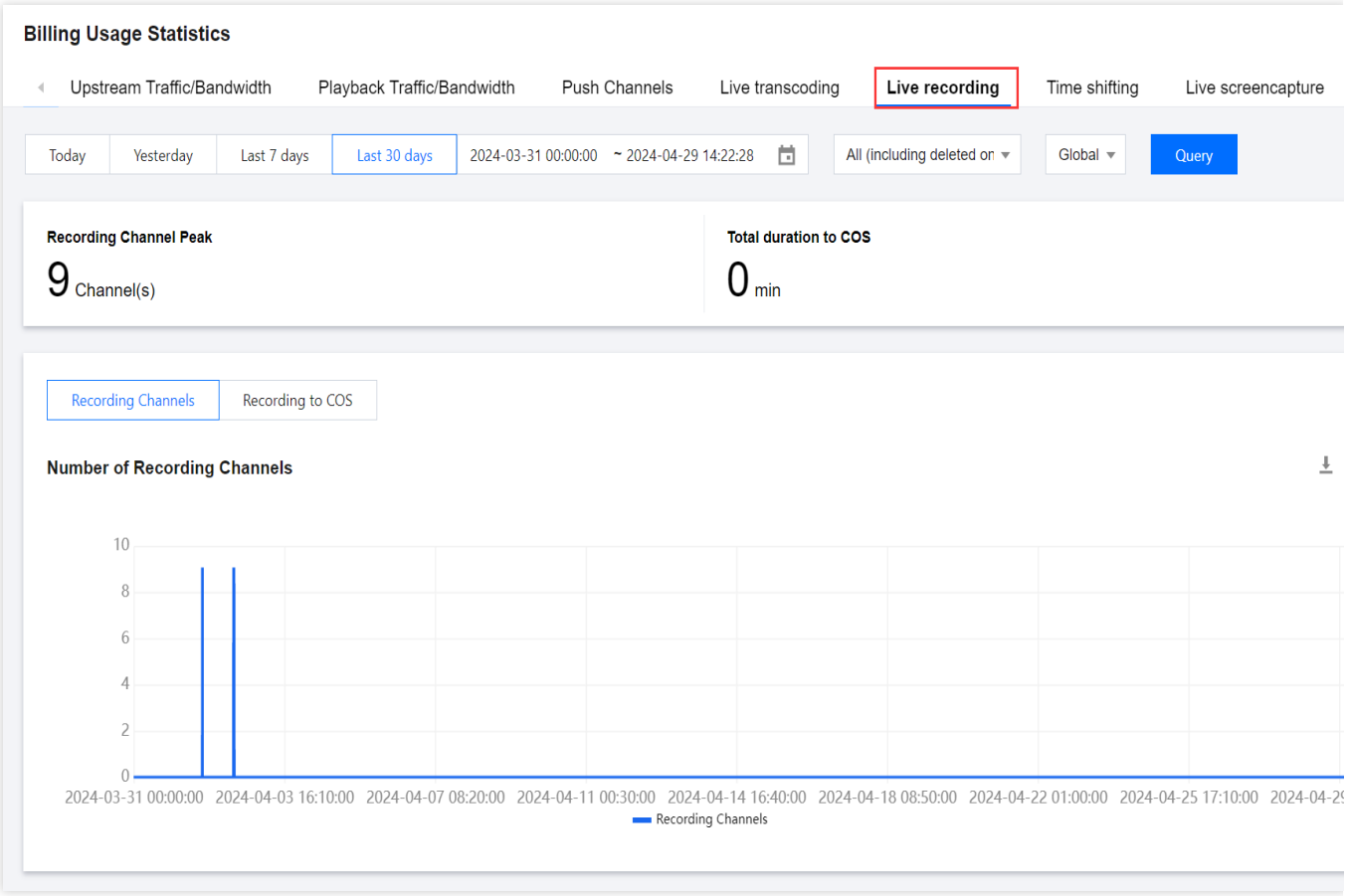
Time Point	Traffic (MB)
2024-03-31 00:00:00	0
2024-04-01 00:00:00	0
2024-04-02 00:00:00	1512.489956
2024-04-03 00:00:00	0
2024-04-04 00:00:00	0
2024-04-05 00:00:00	0
2024-04-06 00:00:00	0
2024-04-07 00:00:00	0
2024-04-08 00:00:00	0
2024-04-09 00:00:00	439.605735

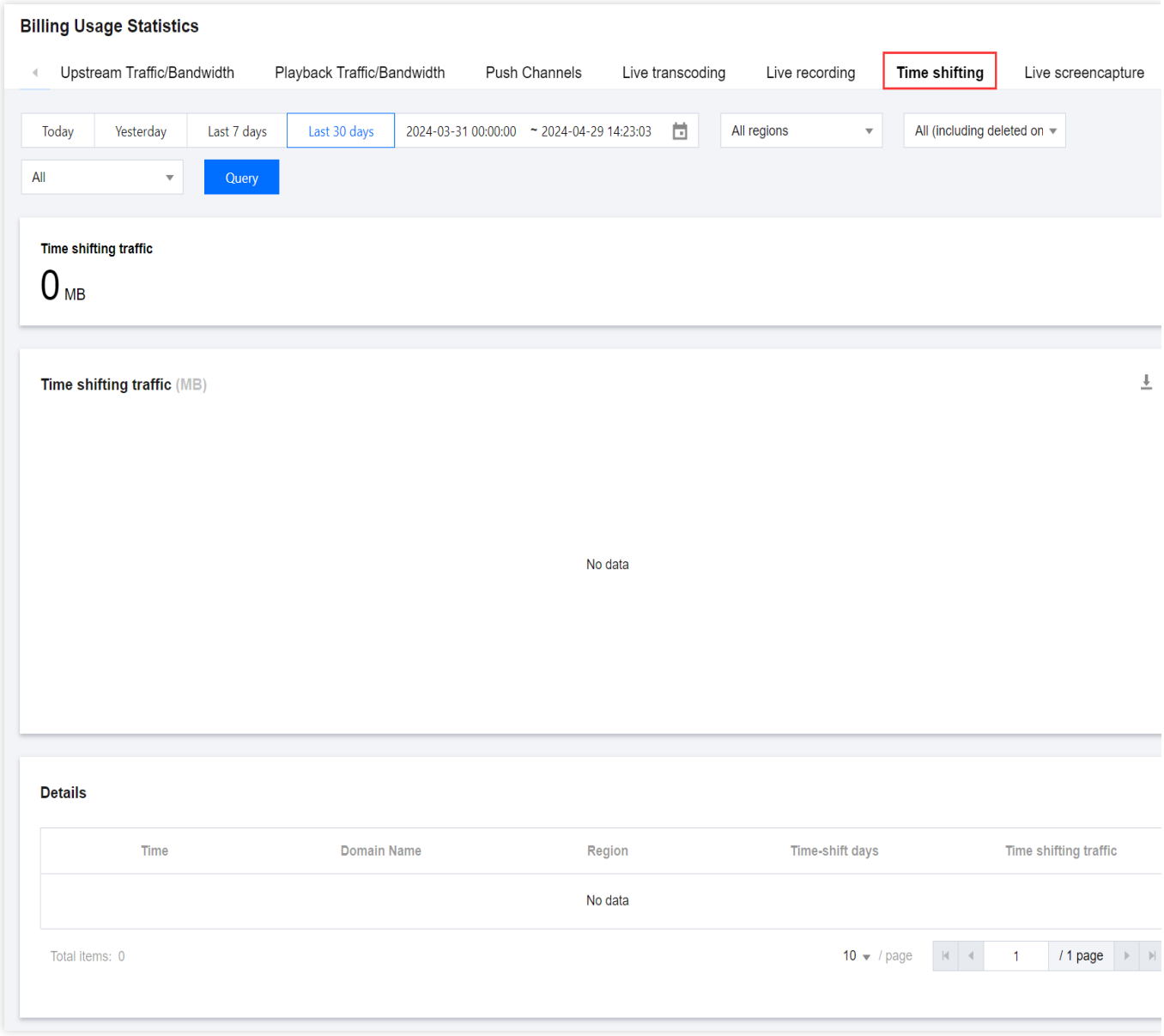
Total items: 30 10 / page 1 / 3 pages

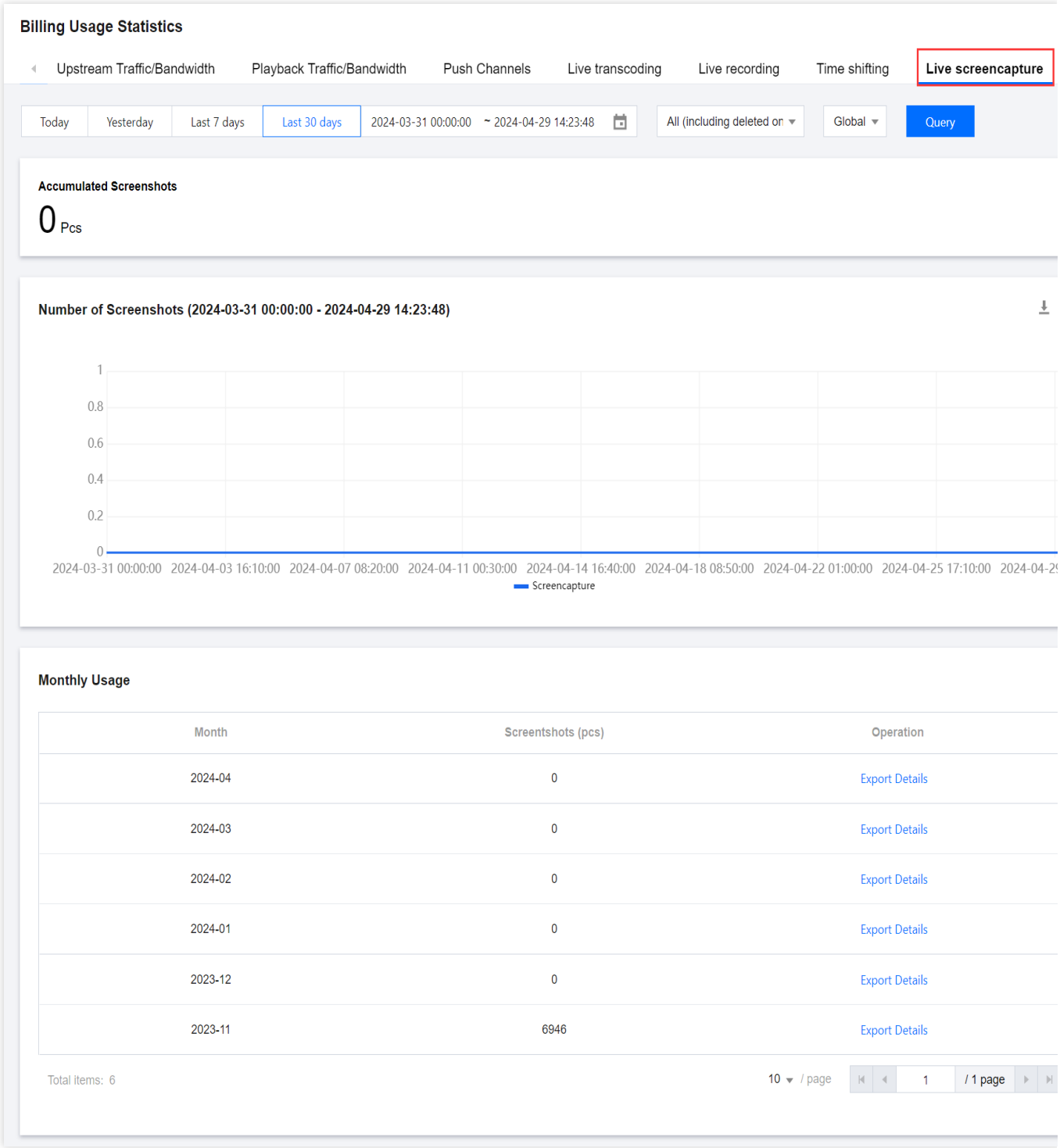

Billing Usage Statistics
Upstream Traffic/Bandwidth
Playback Traffic/Bandwidth
Push Channels
Live transcoding
Live recording
Time shifting
Live screencapture
Today
Yesterday
Last 7 days
Last 30 days
2024-03-31 00:00:00 ~ 2024-04-29 14:20:50
All (including deleted on
Query
Current Channels
0 Channel(s)
Peak Channels
1 Channel(s)
Push Channels (Unit: Channel)
1
0.8
0.6
0.4
0.2
0
2024-03-31 00:00:00
2024-04-03 16:10:00
2024-04-07 08:20:00
2024-04-11 00:30:00
2024-04-14 16:40:00
2024-04-18 08:50:00
2024-04-22 01:00:00
2024-04-25 17:10:00
Channels
Peak Channels in Last 30 Days
For more information, please see Stream Interruption Recor
Time
Channels
2024-03-30 0
2024-03-31 0
2024-04-01 1
2024-04-02 1
2024-04-03 0
2024-04-04 0
2024-04-05 0
2024-04-06 0
2024-04-07 0
2024-04-08 0
Total items: 30
10 / page
1
/ 3 pages

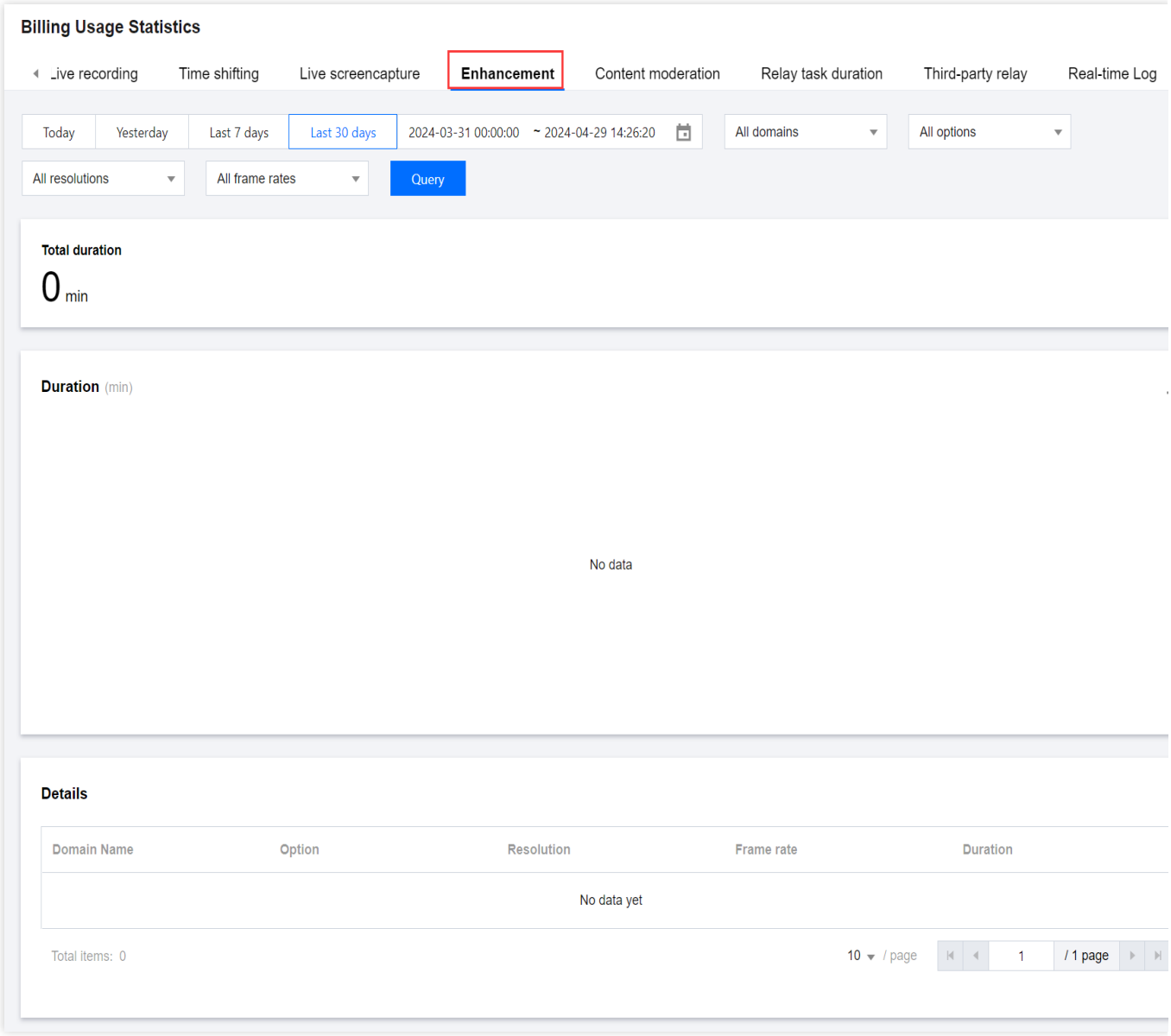


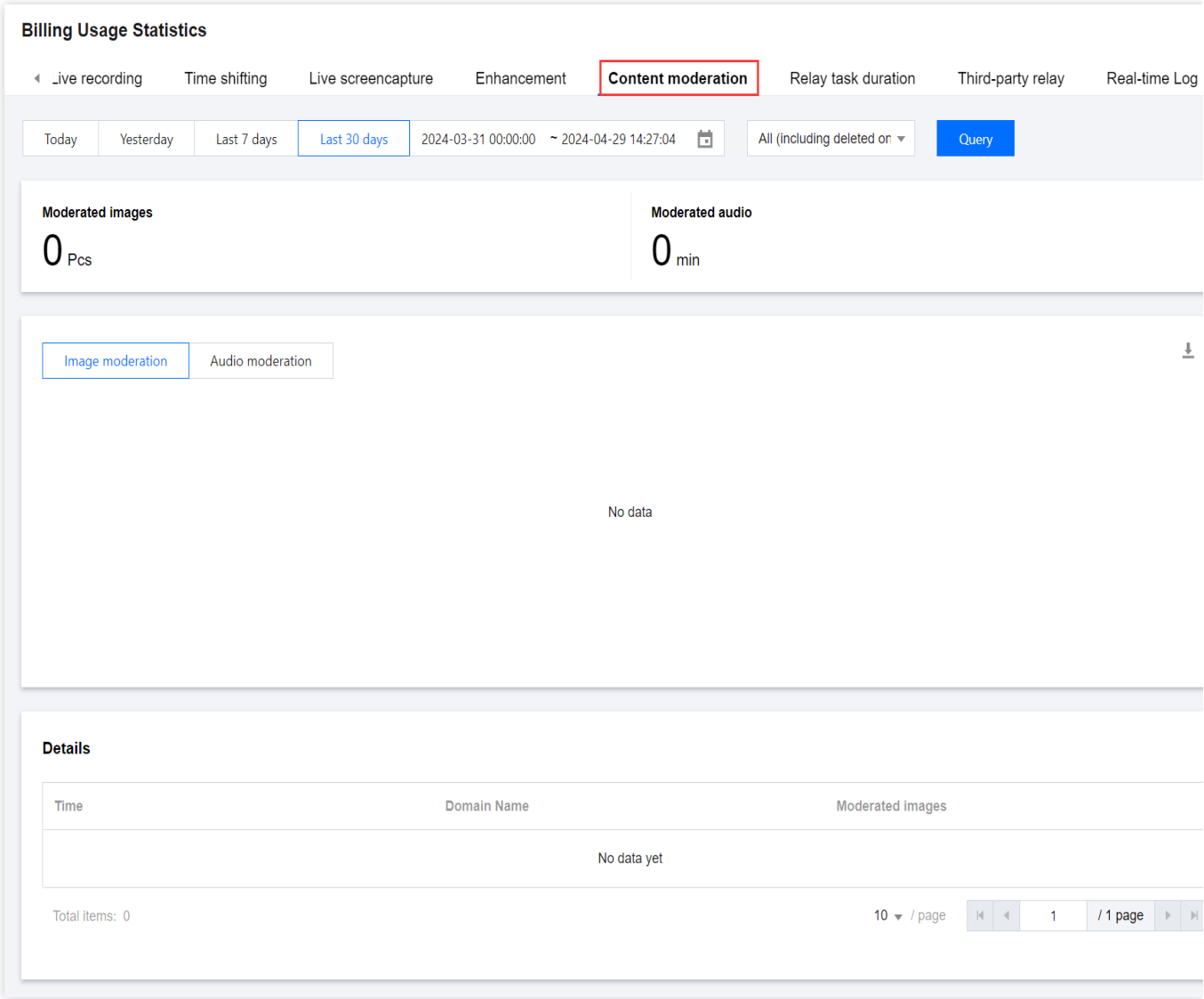
StreamName	Transcoding Start Time	Transcoding End Time	Transcoding Duration (min)	Codec	Region	Bitrate (Kbps)	Type
	2024-04-09 14:37:00	2024-04-09 14:37:00	1	liveprocessor_AAC	Chinese mainland	0	Transcode
	2024-04-09 14:30:00	2024-04-09 14:41:00	12	liveprocessor_H264	Chinese mainland	2000	Transcode
	2024-04-09 14:19:00	2024-04-09 14:22:00	3	liveprocessor_H264	Chinese mainland	2000	Transcode
	2024-04-02 10:23:00	2024-04-02 10:54:00	31	liveprocessor_AAC	Chinese mainland	0	Transcode
	2024-04-02 10:23:00	2024-04-02 10:54:00	31	liveprocessor_H264	Chinese mainland	1536	Transcode
	2024-04-01 16:12:00	2024-04-01 16:14:00	3	liveprocessor_AAC	Chinese mainland	0	Transcode
	2024-04-01 16:10:00	2024-04-01 16:21:00	12	liveprocessor_H264	Chinese mainland	1536	Transcode
	2024-04-01 16:10:00	2024-04-01 16:21:00	12	liveprocessor_AAC	Chinese mainland	0	Transcode

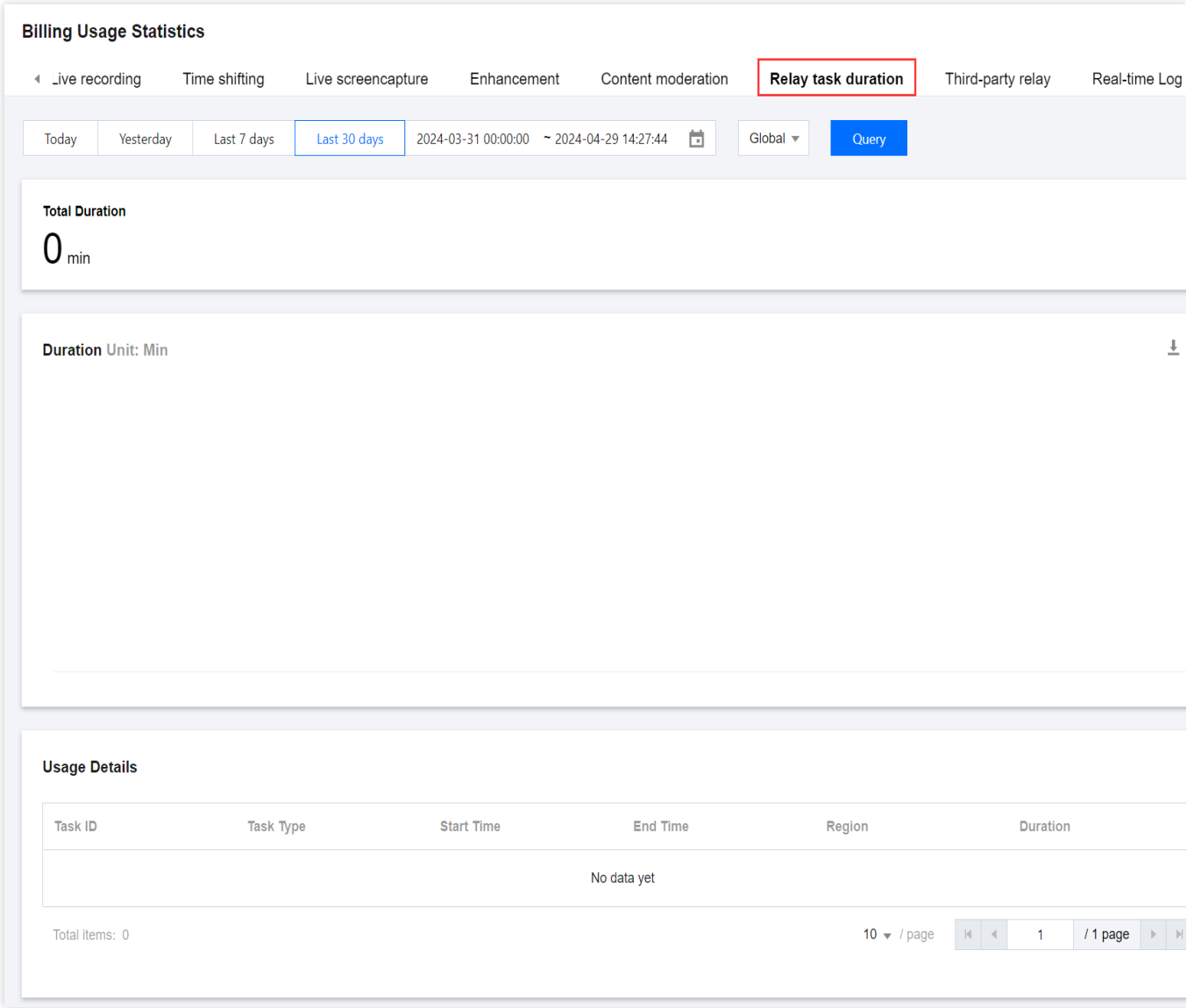

Billing Usage Statistics
Upstream Traffic/Bandwidth
Playback Traffic/Bandwidth
Push Channels
Live transcoding
Live recording
Time shifting
Live screencapture
Today
Yesterday
Last 7 days
Last 30 days
2024-03-31 00:00:00 ~ 2024-04-29 14:22:28
All (including deleted or
Global
Query
Recording Channel Peak
9 Channel(s)
Total duration to COS
0 min
Recording Channels
Recording to COS
Number of Recording Channels
10
8
6
4
2
0
2024-03-31 00:00:00
2024-04-03 16:10:00
2024-04-07 08:20:00
2024-04-11 00:30:00
2024-04-14 16:40:00
2024-04-18 08:50:00
2024-04-22 01:00:00
2024-04-25 17:10:00
Recording Channels

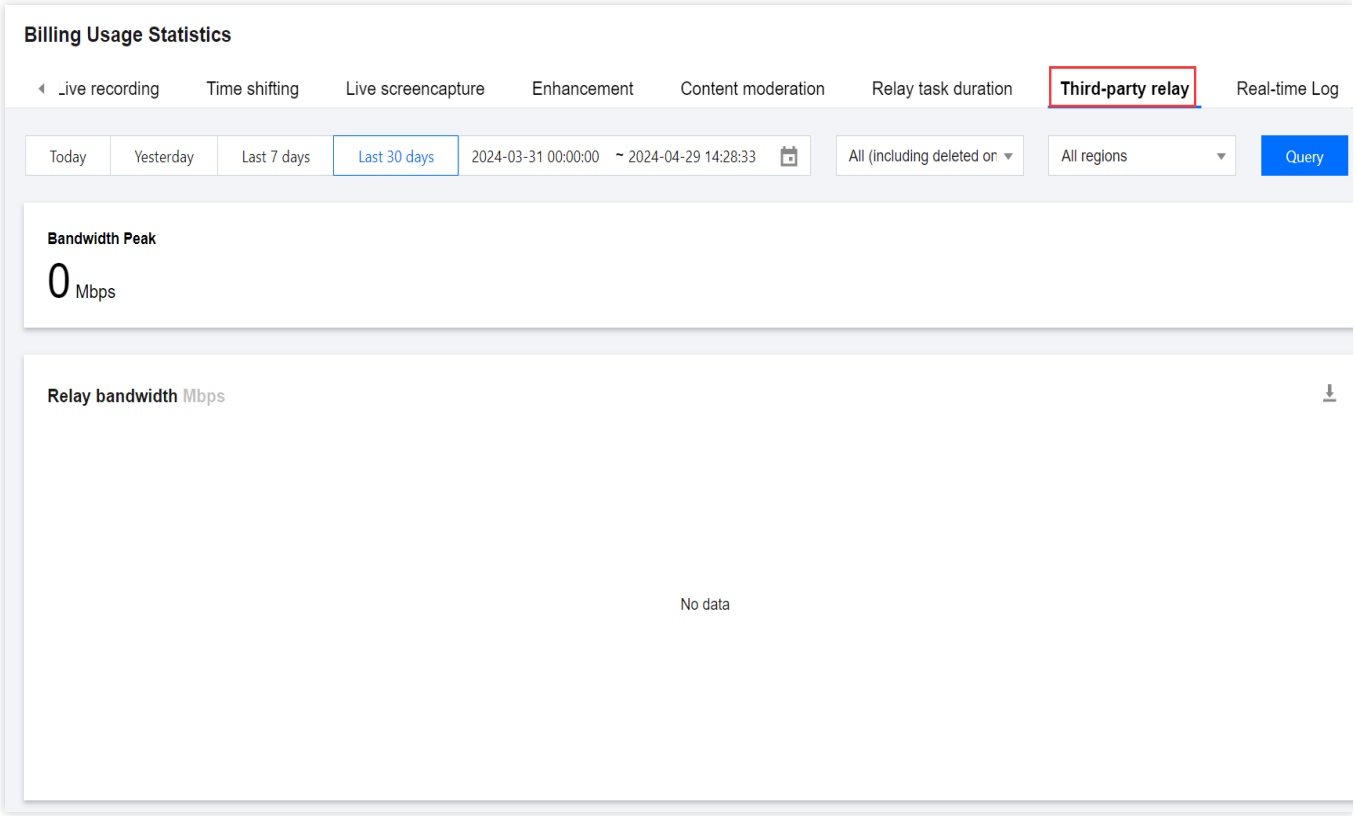

Billing Usage Statistics
Upstream Traffic/Bandwidth
Playback Traffic/Bandwidth
Push Channels
Live transcoding
Live recording
Time shifting
Live screencapture
Today
Yesterday
Last 7 days
Last 30 days
2024-03-31 00:00:00 ~ 2024-04-29 14:23:03
All regions
All (including deleted on
All
Query
Time shifting traffic
0 MB
Time shifting traffic (MB)
No data
Details
Time
Domain Name
Region
Time-shift days
Time shifting traffic
No data
Total items: 0
10 / page
1
/ 1 page

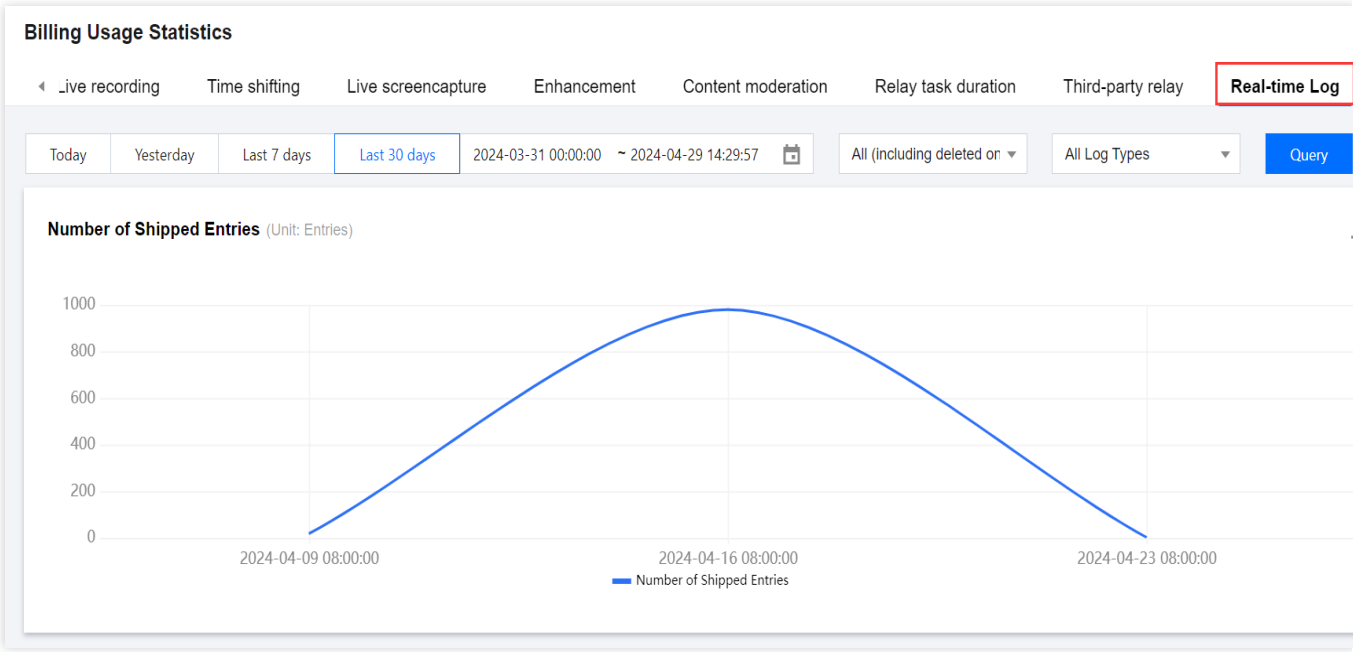

Billing Usage Statistics
Upstream Traffic/Bandwidth
Playback Traffic/Bandwidth
Push Channels
Live transcoding
Live recording
Time shifting
Live screencapture
Today
Yesterday
Last 7 days
Last 30 days
2024-03-31 00:00:00 ~ 2024-04-29 14:23:48
All (including deleted or
Global
Query
Accumulated Screenshots
0 Pcs
Number of Screenshots (2024-03-31 00:00:00 - 2024-04-29 14:23:48)
1
0.8
0.6
0.4
0.2
0
2024-03-31 00:00:00
2024-04-03 16:10:00
2024-04-07 08:20:00
2024-04-11 00:30:00
2024-04-14 16:40:00
2024-04-18 08:50:00
2024-04-22 01:00:00
2024-04-25 17:10:00
Screencapture
Monthly Usage
Month
Screentshots (pcs)
Operation
2024-04
0
Export Details
2024-03
0
Export Details
2024-02
0
Export Details
2024-01
0
Export Details
2023-12
0
Export Details
2023-11
6946
Export Details
Total items: 6
10 / page
1
/ 1 page

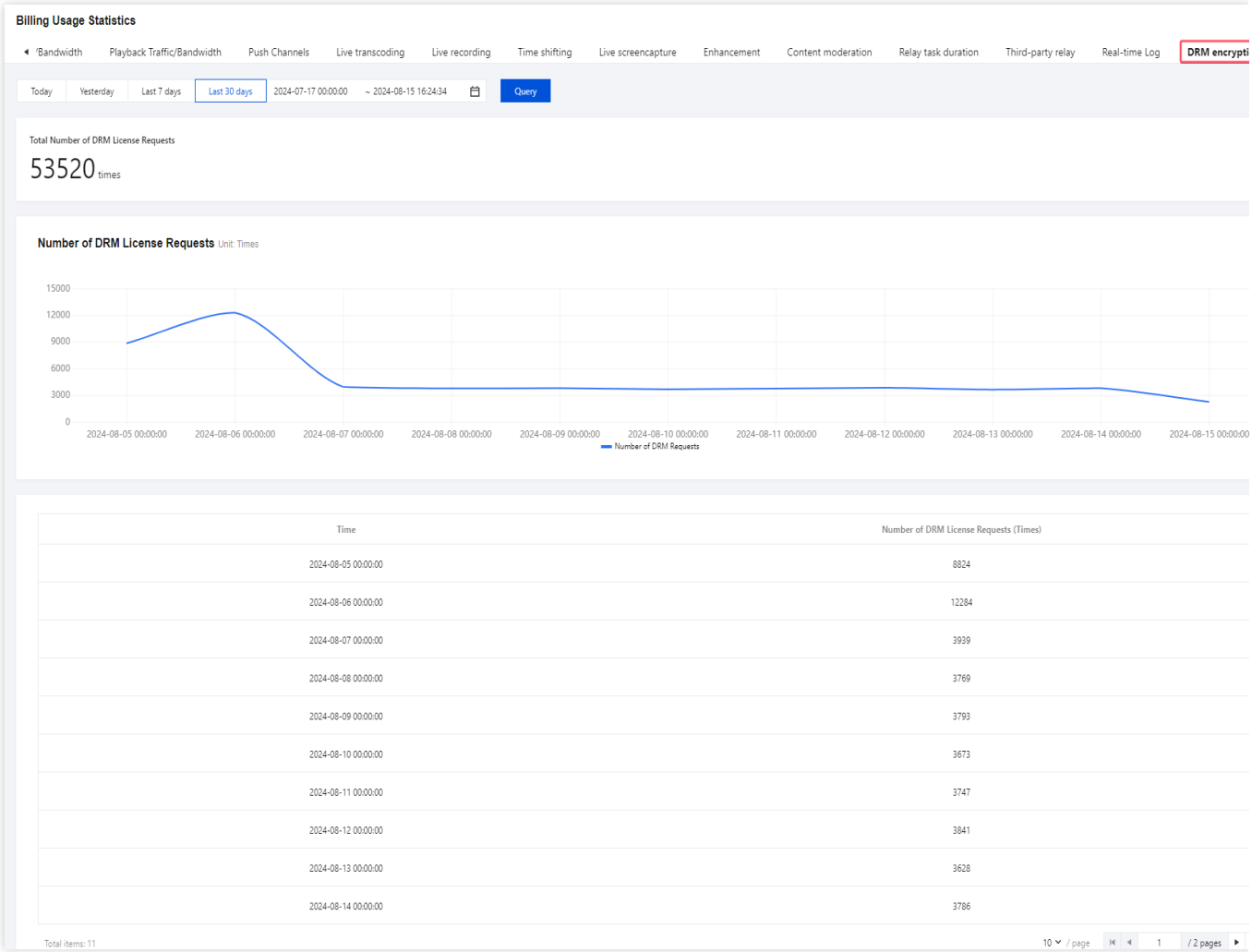

Billing Usage Statistics
ive recording
Time shifting
Live screencapture
Enhancement
Content moderation
Relay task duration
Third-party relay
Real-time Log
Today
Yesterday
Last 7 days
Last 30 days
2024-03-31 00:00:00 ~ 2024-04-29 14:26:20
All domains
All options
All resolutions
All frame rates
Query
Total duration
0 min
Duration (min)
No data
Details
Domain Name
Option
Resolution
Frame rate
Duration
No data yet
Total items: 0
10 / page
1
/ 1 page


Billing Usage Statistics
ive recording
Time shifting
Live screencapture
Enhancement
Content moderation
Relay task duration
Third-party relay
Real-time Log
Today
Yesterday
Last 7 days
Last 30 days
2024-03-31 00:00:00 ~ 2024-04-29 14:27:04
All (including deleted or
Query
Moderated images
0 Pcs
Moderated audio
0 min
Image moderation
Audio moderation
No data
Details
Time
Domain Name
Moderated images
No data yet
Total items: 0
10 / page
1
/ 1 page


Billing Usage Statistics
ive recording
Time shifting
Live screencapture
Enhancement
Content moderation
Relay task duration
Third-party relay
Real-time Log
Today
Yesterday
Last 7 days
Last 30 days
2024-03-31 00:00:00 ~ 2024-04-29 14:27:44
Global
Query
Total Duration
0 min
Duration Unit: Min
Usage Details
Task ID
Task Type
Start Time
End Time
Region
Duration
No data yet
Total items: 0
10 / page
1
/ 1 page


Billing Usage Statistics
Live recording
Time shifting
Live screencapture
Enhancement
Content moderation
Relay task duration
Third-party relay
Real-time Log
Today
Yesterday
Last 7 days
Last 30 days
2024-03-31 00:00:00 ~ 2024-04-29 14:28:33
All (including deleted or
All regions
Query
Bandwidth Peak
0 Mbps
Relay bandwidth Mbps
No data


Billing Usage Statistics
Live recording
Time shifting
Live screencapture
Enhancement
Content moderation
Relay task duration
Third-party relay
Real-time Log
Today
Yesterday
Last 7 days
Last 30 days
2024-03-31 00:00:00 ~ 2024-04-29 14:29:57
All (including deleted or
All Log Types
Query
Number of Shipped Entries (Unit: Entries)
1000
800
600
400
200
0
2024-04-09 08:00:00
2024-04-16 08:00:00
2024-04-23 08:00:00
Number of Shipped Entries



Billing Details

Billable Service	Statistical Item	Description
Upstream traffic/bandwidth	Upstream traffic	Upstream traffic consumed for push during the selected time range
	Peak upstream bandwidth	Peak bandwidth used for push during the selected time range
	Upstream traffic/bandwidth line chart	Upstream traffic/bandwidth usage on a 5-minute basis
	Details	Hourly upstream traffic/bandwidth consumption over the last 30 days
Playback traffic/bandwidth	Playback traffic	Downstream traffic consumed for playback during the selected time range
	Peak playback bandwidth	Peak bandwidth used for playback during the selected time range

	Playback traffic/bandwidth line chart	Downstream traffic/bandwidth usage on a 5-minute basis. You can choose to view the usage of LVB or LEB.
	Details	Hourly playback traffic/bandwidth consumption over the last 30 days
Push channels	Current channels	Current number of push channels
	Peak channels	Maximum number of push channels
	Push channel line chart	Number of push channels on a 5-minute basis
	Peak channels in last 30 days	Highest number of channels per day in the last 30 days
Live transcoding	Total transcoding duration	Total transcoding duration during the selected time range
	Transcoding duration line chart	Transcoding durations on a 5-minute basis
	Monthly usage	Transcoding detail information of stream dimension in the last 30 days
Live recording	Recording channel peak	Highest number of concurrent recording channels during the selected time range
	Total duration to COS	The total duration of recording shipping to COS during the query period
	Recording channel peak/Total duration to COS line chart	Highest number of concurrent recording channels on a 5-minute basis/Cumulative data on the duration of recording shipping to COS
Time shifting	Time shifting traffic	Time shifting write volume during the query period
	Time shifting traffic line chart	Cumulative data of time shifting write volume on a 5-minute basis
	Details	Time shifting write volume by domain name and time shifting day
Live screencapture	Accumulated screenshots	Total number of screenshots taken during the selected time range
	Screenshot number line chart	Number of screenshots on a 5-minute basis
	Monthly usage	Total number of screenshots each month in the last six months
Enhancement	Total duration	Total enhancement duration during the query period

	Duration line chart	Enhancement duration data on a 5-minute basis
	Details	Live streaming enhancement consumption data in the last 30 days
Content moderation	Moderated images	Total number of images generated by image moderation during the query period
	Moderated audio	Total duration generated by audio moderation during the query period
	Image moderation/Audio moderation line chart	Cumulative data of image moderation/audio moderation on a 5-minute basis
	Details	Content moderation records in the last 30 days
Relay task duration	Total duration	Total duration of relay tasks during the selected time range
	Duration line chart	Cumulative task duration data on a 5-minute basis
	Usage details	Detailed information such as task start time and end time by task dimension
Third-party relay	Bandwidth peak	Peak bandwidth of the relay service during the query period
	Relay bandwidth line chart	Peak bandwidth of the relay service on a 5-minute basis
Real-time log	Number of shipped entries	Total number of shipped entries for push logs/playback logs during the query period
DRM encryption	Total number of DRM license requests	Total number of DRM license requests in the last 30 days
	DRM license request line chart	Number of DRM license requests every 5 minutes

Monitoring
Operation Analysis

Last updated：2025-05-15 17:02:09

The CSS console provides the **Operation Analysis** page where you can view data related to **Live Playback**, **User distribution**, **Top playbacks**, **Device Statistics**, and **Origin Server**.

Note:
For the **Live Playback** and **User distribution** tabs, data is based on the user's location IP.
The **Origin Server** tab does not support querying data before February 18, 2022.
Data for outside the Chinese mainland is aggregated instead of ISP-specific.

Live Playback

Under the **Live Playback** tab, you can view data on bandwidth peak, total traffic, total requests, and concurrent connection peak. It supports querying data at the domain name granularity and allows you to select regions and ISPs. You can query data for the last three months, and the maximum time span for each query is one month.

Statistical Item	Description
Bandwidth Peak	Peak bandwidth data generated by downstream playback of live streaming.
Total Traffic	Total traffic data generated by downstream playback of live streaming.
Total Requests	Total number of requests between the player and CSS platform during live streaming.
Concurrent Connection Peak	Peak concurrent connection data between players and the CSS platform during live streaming.

User Distribution

Under the **User distribution** tab, you can view the geographic location, traffic, and request data of live streaming users. It supports querying data at the domain name granularity and allows you to select regions and ISPs. You can query data for the last three months, and the maximum time span for each query is one month. The data is classified by **Greater region** and **Region** and sorted by the ratio of traffic in this region to the total traffic of all regions in the list.

When querying data in the Chinese mainland, the **Greater region** includes North China, Northwest China, Northeast China, East China, Central China, Southwest China, South China, and Other. The **Region** are specific province under each **Greater region**.
When querying data outside of the Chinese mainland, the **Greater region** includes Asia Pacific Region 1, Asia Pacific Region 2, Asia Pacific Region 3, North America, Europe, South America, Middle East, Africa, and Other. The **Region** is specific country or region under each **Greater region**.

Statistical Item	Description
Traffic (MB)	Total traffic of each region.
Traffic/Current list	Ratio of traffic in this region to the total traffic of all regions in the list.
Traffic/Total	Ratio of traffic in this region to all other regions within or outside Chinese mainland. For example, when the user query data within Chinese mainland, this statistical item indicates the ratio of traffic in this region to the total traffic of the Chinese mainland.
Requests	Total number of requests for each region.
Regional requests/Current list	Ratio of requests in this region to the total requests of all regions in the list.
Regional requests/Total	Ratio of requests in this region to all other regions within or outside the Chinese mainland. For example, when the user query data within Chinese mainland, this statistical item indicates the ratio of requests in this region to the total requests of the Chinese mainland.

To view the traffic and bandwidth trends for one or more regions, you can select the desired regions and click on **Traffic Trend** and **Bandwidth Trend**.

Taking the example of selecting multiple regions simultaneously, the displayed traffic trend chart is as follows:

Taking the example of selecting multiple regions simultaneously, the displayed bandwidth trend chart is as follows:

Top Playbacks

The Playback Ranking feature offers display and query capabilities for **TOP 100 streams**, **TOP 100 client IPs**, **TOP 100 URL**, and **TOP 100 Referer**, assisting you in understanding the popularity of live streams and the distribution of viewers. Additionally, this feature supports the query of various data indicators such as ranking, traffic, traffic ratio, frequency, and frequency ratio. It also supports data queries at the domain level (playback) and allows for the selection of regions and the query of data from the most recent three months, The maximum time span supported for each query is one day.

Key Features

Top 100 streams: This feature allows you to query and view the top 100 live streams with the highest viewership, including the ranking, traffic, and traffic proportion.

Top 100 client IPs: This feature allows you to query and view the top 100 client IP addresses that watch the most live broadcasts, helping you understand the audience distribution.

TOP 100 URL: You can inquire and display the top 100 URLs (request paths) ranked by frequency, including information such as ranking, domain, URL, frequency, and frequency ratio. This facilitates your understanding of the audience's access to different URLs.

TOP 100 Referer: You can inquire and display the top 100 Referers (request sources) ranked by frequency, including information such as ranking, domain, Referer, and frequency ratio. This facilitates your understanding of the audience's access situation from different Referers.

Note:

The top-ranking data of streams, IP, URL, and Referer on the current page is only used for operation analysis, and the specific result of the data analysis is subject to the actual log data.

Statistical Item	Description
Top 100 streams: Traffic/Current list TOP 100 Streams - Proportional Traffic Distribution	Ratio of the traffic of this stream to the total traffic of all streams in the list.
Top 100 client IPs: Traffic/Current list	Ratio of the traffic of this IP address to the total traffic of all IP addresses in the list.
Top 100 URL - Frequency Ratio	Ratio of the traffic of this stream to the total traffic of all streams in the list.
Top 100 Referer - Frequency Ratio	Ratio of the traffic of this stream to the total traffic of all streams in the list.

Device Statistics

The Device Statistics feature provides queries and displays for device type, browser type, and operating system type. It supports data queries (playback) at the domain name granularity level and allows the selection of regions. It supports queries for data from the past 3 months.

Statistics Item	Description
Device Type	**Device types** include: Tablet, Mobile, Desktop, TV, and Other.
Browser Type	**Browser types** include: Empty, Chrome, Safari, Opera, QQBrowser, LBBrowser, MaxthonBrowser, SouGouBrowser, BIDUBrowser, TaoBrowser, UBrowser, IE, Microsoft Edge, Bot, and Other.
Operating System Type	**Operating system types** include: Empty, Android, IOS, Mac OS, Windows, Linux, Chromium OS, NetBSD, Bot, and Other.

Origin Server

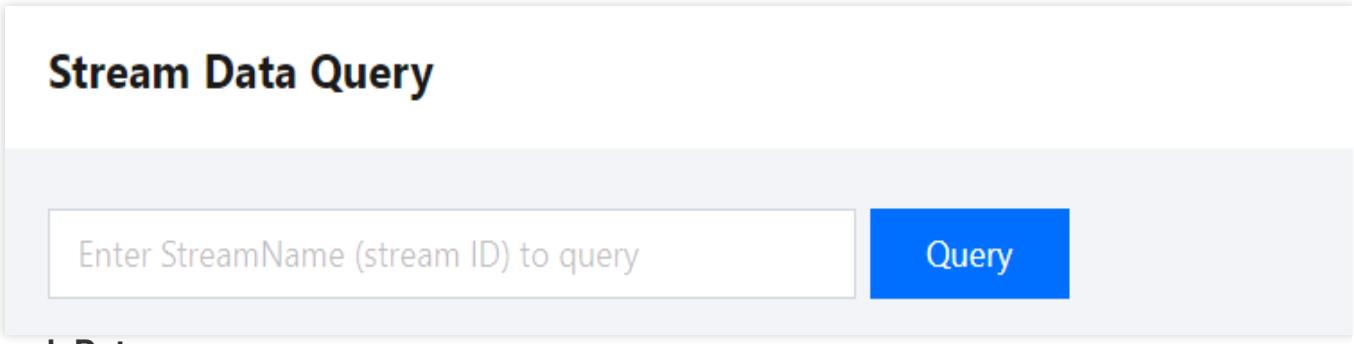
The **Origin Server** tab provides the traffic and peak bandwidth from origin server. It supports querying data at the domain name granularity and allows you to select regions and ISPs. You can query data for the last three months, and the maximum time span for each query is one month.

Statistical Item	Description
Total traffic	Traffic data from the origin server.
Peak bandwidth	Peak bandwidth data from the origin server.

Stream Data Query

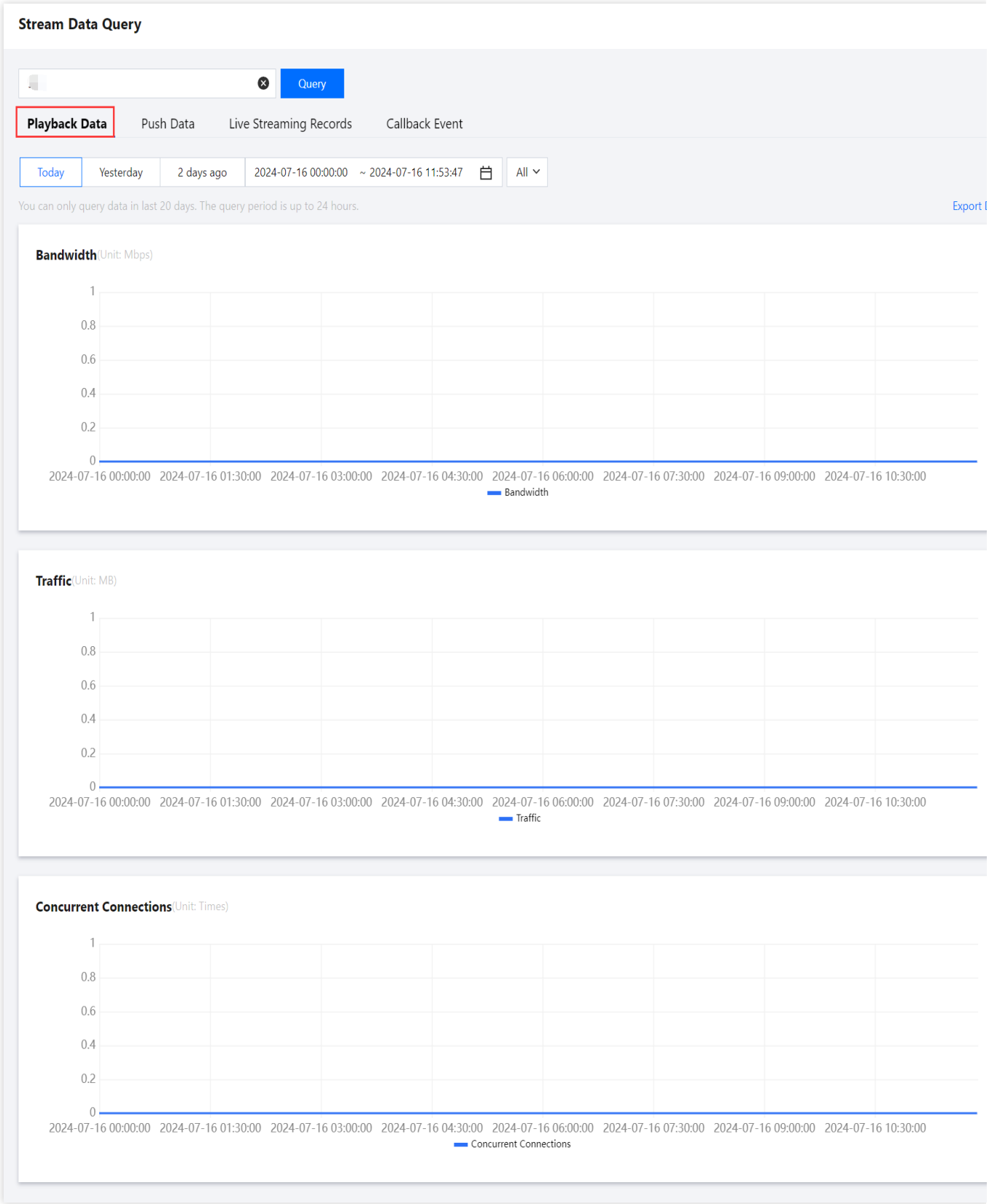
Last updated：2024-10-24 15:12:20

Log in to the CSS console, select Stream Data Query on the left sidebar, and enter a stream name to view its playback data, push data, live streaming records, and callback events.



Playback Data

Under the **Playback Data** tab, you can view data on bandwidth, traffic, and concurrent connections from the last 20 days. The maximum query period is 24 hours.



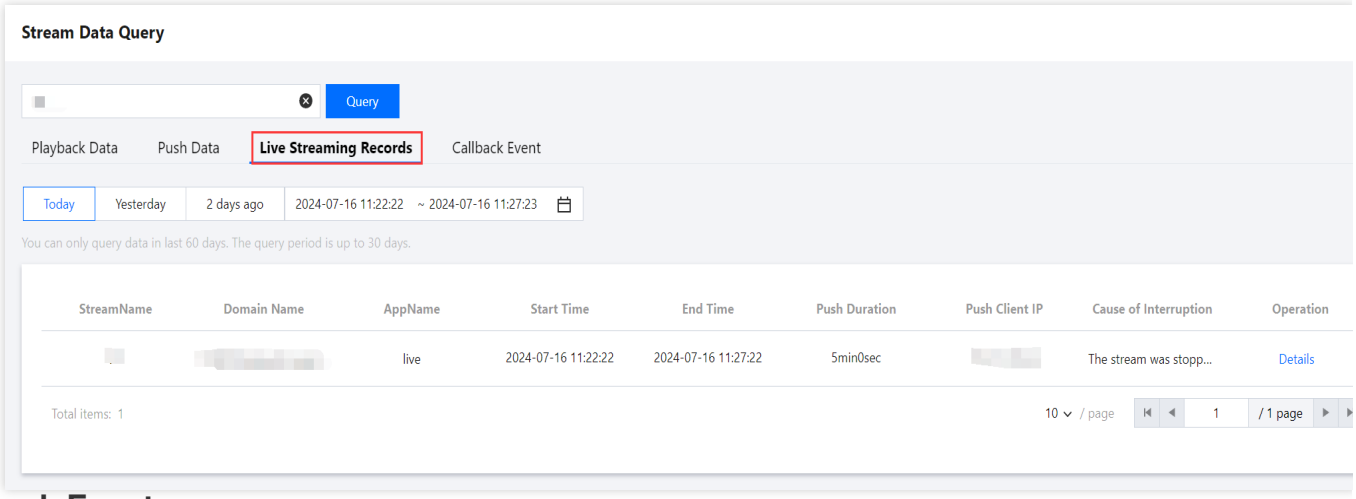
Push Data

Under the **Push Data** tab, you can query data of a single stream, including the traffic, bandwidth, video frame rate, video bitrate, audio frame rate, and audio bitrate. It supports queries for the past 7 days, with the query period less than 3 hours. Streams pushed again from the same IP address will be displayed with curves of different colors.

After entering a stream name, select **Push Data** to view the push data.

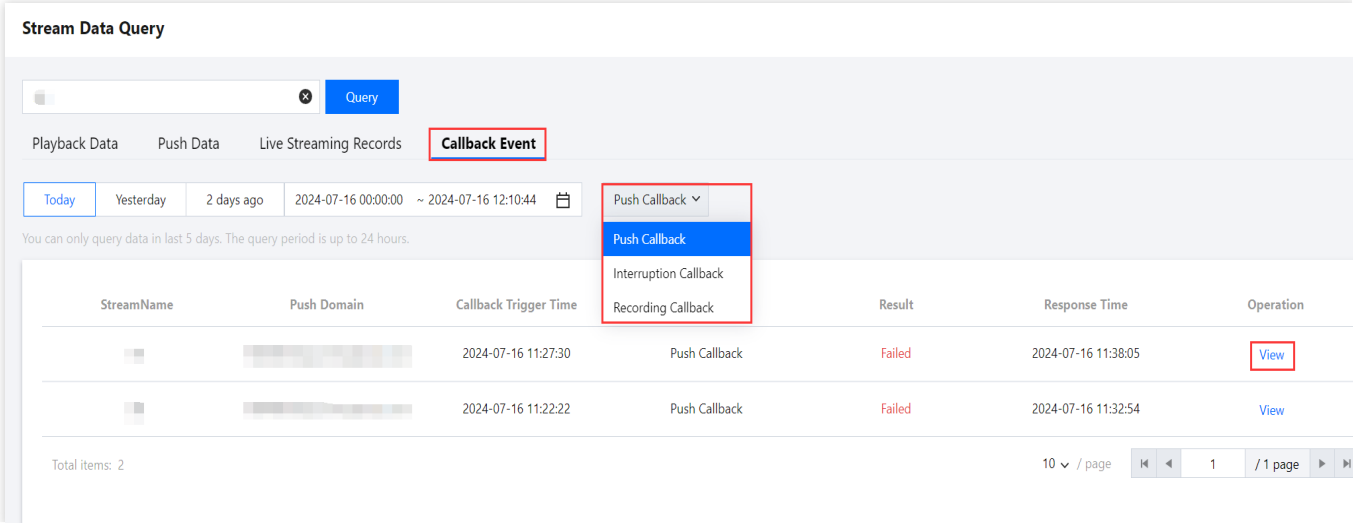
Live Streaming Records

Under the **Live Streaming Records** tab, you can view live streaming information including the name of a stream, its push domain name, live streaming application name, start time, end time, push duration, and push client ID from the last 60 days. You can also click **Details** to view push data. The maximum query period is 30 days.



Callback Event

Under the **Callback Event** tab, you can view the stream name, push domain, callback trigger time, response time, and the result of a push, interruption, or recording callback in the last five days. You can also click **View** to view the content of a callback. The maximum query period is 24 hours.



Errors

Last updated：2025-03-31 17:56:38

Tencent Cloud Streaming Services (CSS) supports the errors feature, allowing you to quickly check errors that occur during the live streaming process. Moreover, you can understand the status of these streams by viewing the primary and backup stream events.

Prerequisites

You have logged in to the CSS Console.

Note

You can configure the push errors event callback in the Live Callback settings. When an event occurs within the live streaming service, the message will be notified through a unified callback of the event message.

Push Errors Query

1. Select **Monitoring** > Errors on the left sidebar.
2. On the errors page, querying by stream ID is supported. You can query the push errors in the last 7 days, and the data within the query period is less than 3 hours.

Primary/Backup Streams Query

1. Select **Monitoring** > Errors from the left sidebar to enter the Primary/Backup Streams page.
2. On the Primary/Backup Streams page, querying by stream ID is supported. You can query the primary/backup streams in the past 7 days, and the data within the query period is less than 3 hours.

Error Types

Below is a list of errors that may occur during live streaming.

Number	Error Type
1	The video timestamp moved backwards
2	The audio timestamp moved backwards
3	The video timestamp increased notably
4	The audio timestamp increased notably
5	Chunk size too big
6	Two consecutive video frames arrived late
7	Two consecutive audio frames arrived late
8	The video codec changed
9	The audio codec changed
10	No codec header before a video frame arrived
11	No codec header before an audio frame arrived
12	Video header parsing failure
13	Large Chunk Size
14	Low video frame rate
15	Large timestamp interval of audio frames
16	Large GOp Size
17	Uncommon audio/video encoding and decoding formats

Stream Interruption Records

Last updated：2024-06-19 17:01:34

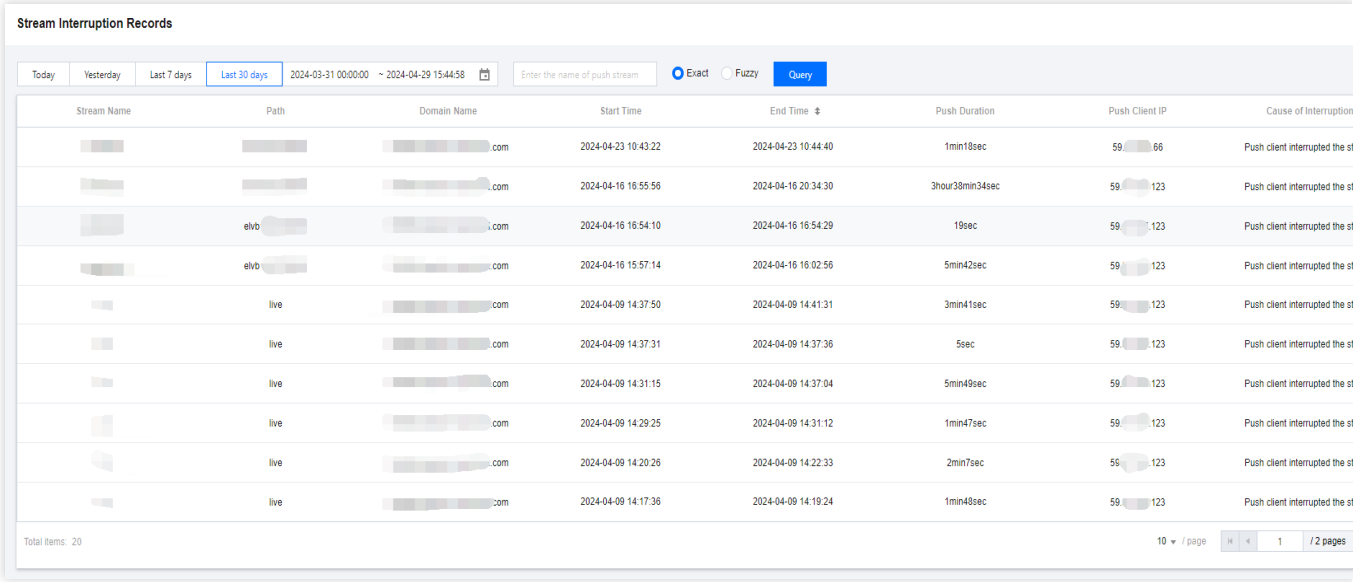
You can view records of live push interruptions and their causes in the CSS console.

Prerequisites

You have logged in to the CSS console.
There is a live stream whose push was interrupted under your account.

Directions

1. In the console, select **Monitoring** > Stream Interruption Records on the left sidebar.
2. Our platform supports querying stream interruption records for the past 30 days through the use of stream names, offering both exact and fuzzy search capabilities. Users can access detailed information including the stream name, path, domain name, start time, end time, push duration, push client IP, and cause of interruption.



On the **Stream Interruption Records** page:
Path is the value of `AppName` in the push URL.
Stream Name is the value of `StreamName` in the push URL.

Causes of Stream Interruption

The table below lists the possible causes of stream interruption and their error codes:

errcode	sub_errcode	errmsg
0	0	Unknown reason.
1	0	The push client stopped the stream.
2	0	The push client stopped the stream.
3	0	The push client stopped the stream.
4	0	The push client stopped the stream.
5	0	CSS system internal error.
6	0	RTMP content error.
7	0	Exceeded the maximum size allowed for a single RTMP frame.
8	0	The system stopped the stream because no data was generated for a long time.
9	0	CSS system internal error.
10	0	The proxy layer received an interruption command.
11	0	CSS system internal error.
12	0	Network error for the push client.
13	0	Network error for the push client.
14	0	Network error for the push client.
15	0	Network error for the push client.
16	0	Network error for the push client.
17	0	Network error for the push client.
18	100	CSS system internal error.
18	101	CSS system internal error.
18	102	CSS system internal error.
18	103	CSS system internal error.

18	104	CSS system internal error.
18	200	Failed to get the user information for the push URL.
18	201	Your CSS services have been suspended.
18	202	Your CSS services have been suspended due to overdue payments. Please top up your account balance.
18	203	Your CSS services have been suspended.
18	300	Push using an IP address is not allowed.
18	301	Unable to identify the push domain name.
18	302	Invalid push domain name.
18	303	The push domain name is disabled.
18	304	The push application is disabled.
18	305	The stream is disabled.
18	306	Channel mode is used, but there isn't a push channel.
18	307	Channel mode is used, but the current push channel is disabled.
18	308	The push name contains unallowed characters.
18	309	The push application name contains unallowed characters.
18	400	The push client's IP address is on the blocklist.
18	401	The push client's IP address is not on the allowlist.
18	500	The expiration time parameter is missing from the push URL.
18	501	The push URL has expired.
18	502	The authentication parameter is missing from the push URL.
18	503	Authentication failed.
18	600	Reached the maximum number of streams that can be pushed.
18	601	Reached the maximum number of streams that can be pushed using this stream name.
18	602	The priority of this stream is lower than another stream.

19	0	Third-party authentication failed.
20	0	The system stopped the stream because no data was generated for a long time.
21	100	The stream was stopped at your request.
21	101	The stream was disabled at your request.
21	102	A new push URL replaced the current one.
21	103	A new push URL replaced the current one that has no data.
22	0	Unknown reason.
23	0	RTMP content error.
24	0	CSS system internal error.
25	0	Unknown reason.
26	0	Unknown reason.
27	0	Unknown reason.
28	0	Unknown reason.
29	0	Unknown reason.
30	0	Unknown reason.
31	0	Unknown reason.
32	0	Unknown reason.
33	0	RTMP AMF error.
34	0	Unknown reason.
35	0	The push client stopped the stream.
36	0	Unknown reason.
37	0	SRS stopped the stream because it was not played.
38	0	CSS system internal error.
39	0	Exceeded the maximum frame size allowed for push.

Log Service
Real-Time Log Analysis

Last updated：2025-05-07 10:04:31

Real-time log analysis enables quick retrieval, analysis, and storage of log data through the real-time collection and delivery of CSS access logs to Tencent Cloud Log Service (CLS). This enables you to mine log data for data-driven operations and management, allowing for the rapid and accurate development of operational strategies.

Note:

Real-time log analysis now fully supports shipping logs to Cloud Log Service. This document will guide you on how to use the real-time log feature.

Notes

Log data is collected in real-time, with log search and reporting data stabilizing after three minutes.

Currently, reporting analysis is only available for playback logs. If you have other log management needs, visit Cloud Log Service.

After enabling the log delivery feature, ensure that your CLS service is in normal operation, as the suspension of CLS will prevent the delivery of logs.

The bandwidth or traffic data recorded in logs is the application layer (HTTP protocol) return data. Due to mechanisms like TCP header consumption and failed retransmissions, it is smaller than the bandwidth or traffic consumption calculated at the TCP layer.

Operation Instructions

Creating a log topic

1. Go to the CSS console and select **Monitoring** > **Cloud Log Service** > Real-time log analysis to enter the real-time log analysis page.

2. If this is your first time using this feature, you need to use your CSS service role to grant authorization. After authorization, you need to agree to the service agreement and click **Start**. The system will automatically activate the CLS product and open the real-time log analysis management page.

3. Choose a region and click the link on the page to create a new logset.

Note:

The region includes Guangzhou and Singapore. Log topics created under the logset in the Guangzhou region can only deliver logs within the Chinese mainland. In contrast, log topics created under the logset in the Singapore region can

only deliver logs globally, including to Hong Kong (China), Macao (China), and Taiwan (China).

4. Click **Confirm** to create a new logset.

5. After successfully creating a logset, click **Create Log Topic** to enter the log topic creation page. The newly created log topic will by default be in the process of delivering logs to CLS.

Modifying a log topic

1. Enter the log topic list in real-time log analysis and click **Manage** in the operation column of the log topic you need to modify.

2. Enter the log topic editing page to modify the log topic information.

Analyzing a log report

Only log topics of the log type provide report analysis. There are four types of data on the page: **Basic Data Analysis, Resource Distribution Analysis, Exception Diagnosis Analysis,** and **User Analysis**.
1. Enter the log topic list in **Real-time Log Analysis** and click **Report** on the right side of the log topic you want to view.

2. Enter the log report page to view report data; you can separately view **Basic Data**, **Resource Distribution**, **Exception Diagnosis**, and **User Analysis**.
Basic Data
Resource Distribution

Exception Diagnosis
User Analysis

Log Search

Log search supports multiple types of retrieval and analysis methods, as well as various forms of chart analysis. For detailed information, see Log Search and Analysis.
Log search is performed based on log topics. Select the log topic you need to search for and click Search to enter the log search page.

Stop shipping a log topic to CLS

1. Enter the log topic list in Real-time Log Analysis and click **Stop** on the right of the log topic you wish to stop shipping.

2. In the pop-up window, click Confirm to stop shipping. The status of the corresponding log topic will change to "stop shipping", and logs will no longer be shipped to CLS.

Deleting a log topic

Note：
Once a log topic is deleted, it cannot be recovered. Please proceed with caution.
If you delete a log topic, you will stop pushing log data of the related domain, the corresponding log topic in CLS will also be deleted, and all shipped logs will be cleared. Meanwhile, you will no longer be able to use the report associated with that topic.

1. Enter the log topic list in **Real-time Log Analysis** and click **Delete** on the right side of the log topic you wish to remove.

2. In the pop-up window, confirm whether to delete the log topic and click **OK** to proceed.

Log Fields

Push logs

Order	Log Field	Description
1	time	Request time
2	client_ip	Client IP
3	host	Accessed domain name
4	url	URL
5	size	Stream push byte size
6	country_id	Country ID
7	prov	Province
8	isp	ISP
9	streamname	Stream ID
10	node_ip	Node IP
11	server_region	Server region
12	server_country	Server country

Playback logs

Order	Log Field	Description

1	type	Playback type: lvb represents Live Video Broadcasting and leb represents Live Event Broadcasting
2	time	Request time
3	client_ip	Client IP
4	host	Accessed domain name
5	url	URL
6	size	Byte size of this access request
7	country_id	Country ID
8	prov	Province
9	isp	ISP
10	http_code	HTTP status code
11	referer	Referer information
12	process_time	Processing duration (in milliseconds)
13	ua	User-Agent information
14	range	Range parameter
15	method	HTTP Method
16	streamname	Stream ID
17	hit	Cache hit/miss
18	node_ip	Node IP (This field may be empty for the IP addresses of certain CDN cluster nodes cannot be obtained.)
19	server_region	Server region
20	server_country	Server country
21	connect_fd	Connection port number
22	lost_rate	The packet loss rate, only valid for type=leb
23	rtt	Round-trip time, only valid for type=leb

Note:

The special status codes in the log are as follows:

0: Connection established.

4: Request timed out, authentication timed out, or response timed out.

5: Origin server disconnected or stream terminated.

6: Client disconnected.

Country (Region) Mapping:

```
**China：1**, **Bahrain：2**, **South Korea：3**, **Lebanon：4**, **Nepal：5**,
**Thailand：6**, **Pakistan：7**, **United Arab Emirates：8**, **Bhutan：9**,
**Oman：10**, **Azerbaijan：11**, **North Korea：12**, **Philippines：13**,
**Cambodia：14**, **Qatar：15**, **Kyrgyzstan：16**, **Maldives：17**,
**Malaysia：18**, **Saudi Arabia：20**, **Cyprus：21**, **Brunei：22**, **Laos：
23**, **Japan：24**, **Turkmenistan：25**, **Turkey：26**, **Kazakhstan：27**,
**Palestine：28**, **Tajikistan：29**, **Tajikistan：30**, **Kuwait：31**,
**Syria：32**, **India：33**, **Indonesia：34**, **Armenia：35**, **Afghanistan：
36**, **Afghanistan：37**, **Sri Lanka：38**, **Iraq：39**, **Vietnam：40**,
**Iran：41**, **Yemen：42**, **Jordan：43**, **Myanmar：44**, **Sikkim：45**,
**Bangladesh：46**, **Bangladesh：47**, **Israel：48**, **Egypt：49**, **Burkina
Faso：50**, **Madagascar：51**, **Algeria：52**, **Burundi：53**, **Equatorial
Guinea：54**, **Togo：55**, **Angola：56**, **Ethiopia：57**, **Nigeria：58**,
**South Africa：59**, **Senegal：60**, **Cape Verde：61**, **The Democratic
Republic of Sao Tome and Principe：62**, **Swaziland：63**, **Niger：64**,
**Mauritius：65**, **Guinea-Bissau：66**, **Eritrea：67**, **Tanzania：68**,
**Sudan：69**, **Guinea：70**, **Côte d'Ivoire：71**, **Chad：72**, **Comoros：
73**, **Sierra Leone：74**, **Central African Republic：75**, **Zambia：76**,
**Uganda：77**, **Mauritania：78**, **Libya：79**, **Cameroon：80**, **Djibouti：
81**, **Liberia：82**, **Zimbabwe：83**, **Congo：84**, **Mali：85**, **Lesotho：
86**, **Gabon：87**, **Morocco：88**, **Gambia, The：89**, **Ghana：90**,
**Kenya：91**, **Malawi：92**, **Namibia：93**, **Seychelles：94**, **Botswana：
95**, **Mozambique：96**, **Benin：97**, **Rwanda：98**, **Somali：99**,
**Tunisia：100**, **Ivory coast：101**, **France：102**, **Albania：103**,
**Dublin：104**, **Estonia：105**, **Andorra：106**, **Monaco：107**,
**Luxembourg：108**, **Spain：109**, **Sweden：110**, **Macedonia：111**,
**Italy：112**, **San Marino：113**, **Hungary：114**, **The Socialist Federal
Republic of Yugoslavia：115**, **Greece：116**, **Switzerland：117**, **Moldova：
118**, **Lithuania：119**, **Latvia：120**, **Vatican City State：121**,
**Iceland：122**, **Poland：123**, **United Kingdom：124**, **Liechtenstein：
125**, **Slovakia：126**, **Netherlands：127**, **Ukraine：128**, **Portugal：
129**, **Malta：130**, **Belgium：132**, **Croatia：133**, **Finland：134**,
**Bulgaria：135**, **Germany：136**, **Czech Republic：137**, **Romania：138**,
**Norway：139**, **Slovenia：140**, **Austria：141**, **Belarus：142**,
**Denmark：143**, **Bosnia and Herzegovina：144**, **Ireland：145**,
**Argentina：146**, **Paraguay：147**, **Brazil：148**, **Bolivia：149**,
**Venezuela：150**, **Chile：151**, **Uruguay：152**, **Suriname：153**, **Peru：
154**, **Colombia：155**, **Ecuador：156**, **Guyana：157**, **Dominican
Republic：158**, **Bahamas：160**, **Panama：161**, **Nicaragua：162**,
```

```
**Barbados：163**, **Jamaica：164**, **Haiti：165**, **Mexico：166**,
**Guatemala：167**, **Cuba：168**, **Honduras：169**, **Grenada：170**, **Costa
Rica：171**, **Dominica：172**, **Saint Christopher and Nevis：173**, **United
States：174**, **Saint Vincent and the Grenadines：175**, **Trinidad and Tobago：
176**, **Antigua and Barbuda：177**, **Dominica：178**, **Belize：179**, **El
Salvador：180**, **Canada：181**, **Saint Lucia：182**, **Australia：183**,
**Nauru：184**, **Palau：185**, **Papua New Guinea：186**, **Samoa：187**,
**Fiji：188**, **Solomon Islands：189**, **Kiribati：190**, **Micronesia：191**,
**Tuvalu：192**, **New Zealand：193**, **Tonga：194**, **Marshall Islands：195**,
**Vanuatu：196**, **Mongolia：197**。
```

Provincial Mapping:

```
**Beijing：1**, **Tianjin：2**, **Hebei：3**, **Shanxi：4**, **Inner Mongoria：
5**, **Jiangsu：6**, **Anhui：7**, **Shandong：8**, **Liaoning：9**, **Jilin：
10**, **Heilongjiang：11**, **Shanghai：12**, **Zhejiang：13**, **Jiangxi：14**,
**Fujian：15**, **Hubei：16**, **Hunan：17**, **Henan：18**, **Guangdong：19**,
**Guangxi：20**, **Hainan：21**, **Chongqing：22**, **Sichuan：23**, **Guizhou：
24**, **Yunnan：25**, **Xizang：26**, **Shaanxi：27**, **Gansu：28**, **Ningxia：
29**, **Qinghai：30**, **Xinjiang：31**, **China Hongkong：32**, **China Macao：
33**, **China Taiwan：34**。
```

Carrier Mapping:

```
**China Telecom：1**, **China Netcom：2**, **Cernet：3**, **China Mobile：4**,
**China Unicom：5**, **China Railcom：6**, **Great Wall Broadband Network：7**,
**Telecom：8**, **PCCW：9**, **Oriental Cable：10**, **Hutchison
Telecommunications：11**, **City Telecom：12**, **Gehua：13**, **Founder
Broadband：14**, **Tianwei：15**, **Hong Kong Cable：16**, **SmarTone：17**,
**University：18**, **Consulting Networking：19**, ** CITIC Pacific：20**, **New
World Telecommunications：21**, **Hengtong International：22**, **Wharf
Telecommunication：23**, ** Pacnet：24**, **First Line：25**, **Connectivity
Advantage：26**, **Keying Telecom：27**, **CNLink Networks：28**, **New Network：
29**, **SunnyVision：30**, **Chunghwa Telecom：31**, **New Electricity：32**,
**First：33**, **Hong Kong Information Technology：34**, **Nanling：35**,
**Alibaba：36**, **Tencent：37**, **Dr.Peng：38**, **Radio And Television：40**,
**Hong Kong Broadband：41**, ** Technology Network：42**, **WangSu：43**,
**akamai：44**, **Zhejiang Huashu：45**。
```

Server Region and Country (Region) Mapping:

Region	Country (region)
China	China
Asia Pacific	China Hongkong

1	China Macao
	Singapore
	Vietnam
	Thailand
Asia Pacific 2	China Taiwan
	Japan
	Malaysia
	Indonesia
	South Korea
Asia Pacific 3	Philippines
	India
	Australia
Middle East	Saudi Arabia
	United Arab Emirates
	Turkey
North America	United States
	Canada
Europe	United Kingdom
	Germany
	France
	Italy
	Ireland
	Spain
South America	Brazil
Africa	South Africa

Definitions

Logset

A logset classifies log topics and metric topics and can contain multiple log topics and metric topics. A logset itself does not store any log data, it only facilitates user management of topics. CSS logsets have the following basic attribute information:
Region: The region to which a logset belongs.
Note：
Guangzhou and Singapore regions are currently supported.
Logset Name: The name of a logset.
Retention period: The default retention period for data in the log set is 30 days.
Creation time: Logset creation time.

Log Topic

A log topic is a basic unit for log data collection, storage, retrieval, and analysis on the CLS platform. The vast amounts of logs collected are managed by log topic, including the configuration of the collection rules and storage time, log search and analysis, and log download, consumption, and delivery.
Log topic features include:
Collect logs to log topics.
Store and manage logs based on log topics.
Search and analyze logs by log topics.
Ship logs to other platforms based on log topics.
Download and consume logs from log topics.
Note：
The information above is excerpted from the CLS product documentation. For more details, see Log Topic and Logset and refer to the CLS documentation for accurate information.

Toolkit
Web Push

Last updated：2024-07-22 16:36:54

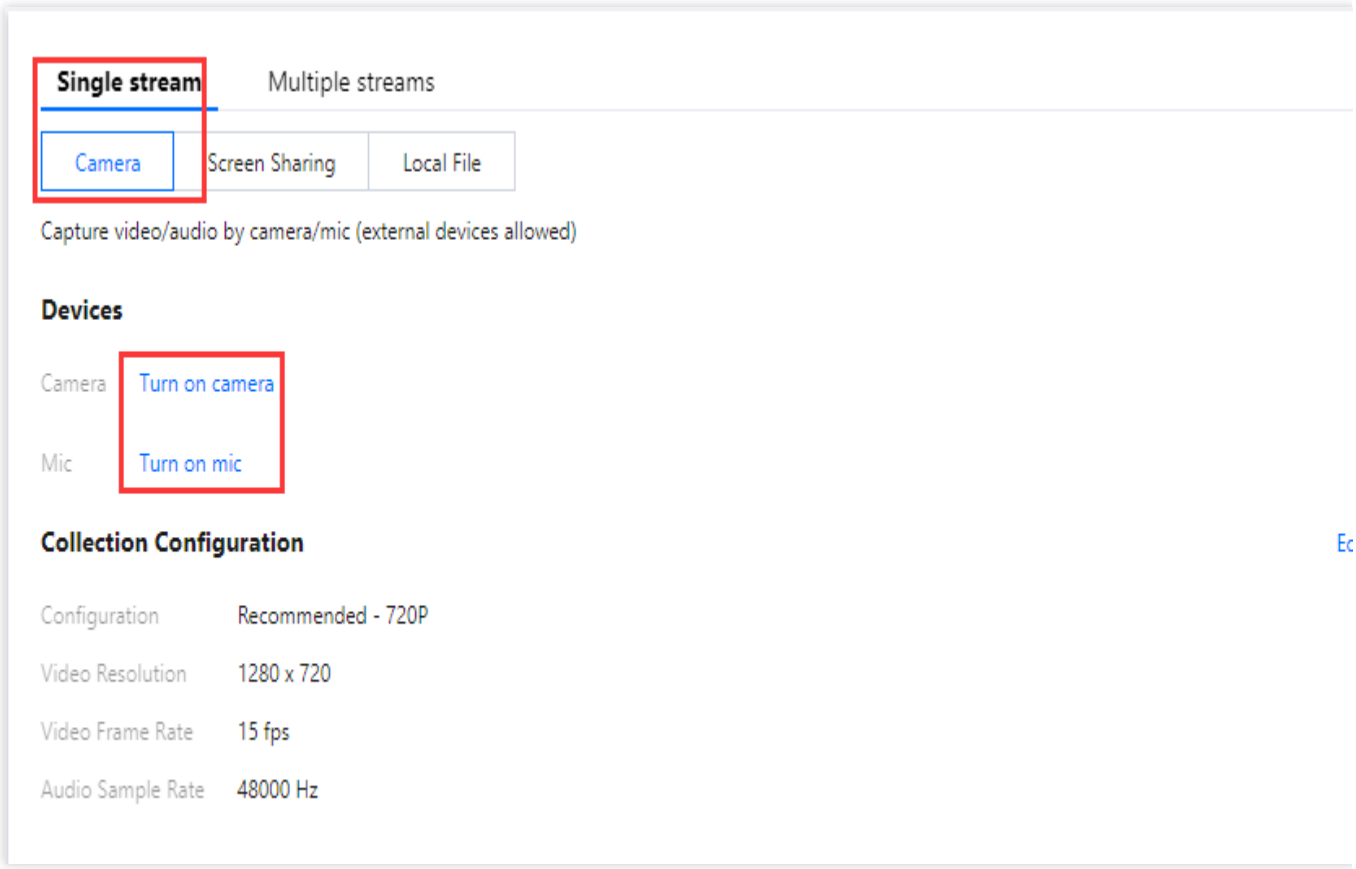
CSS allows you to push streams over the web. You can generate a push URL quickly and push streams from the camera or screen or push a local file to test CSS features.

Prerequisites

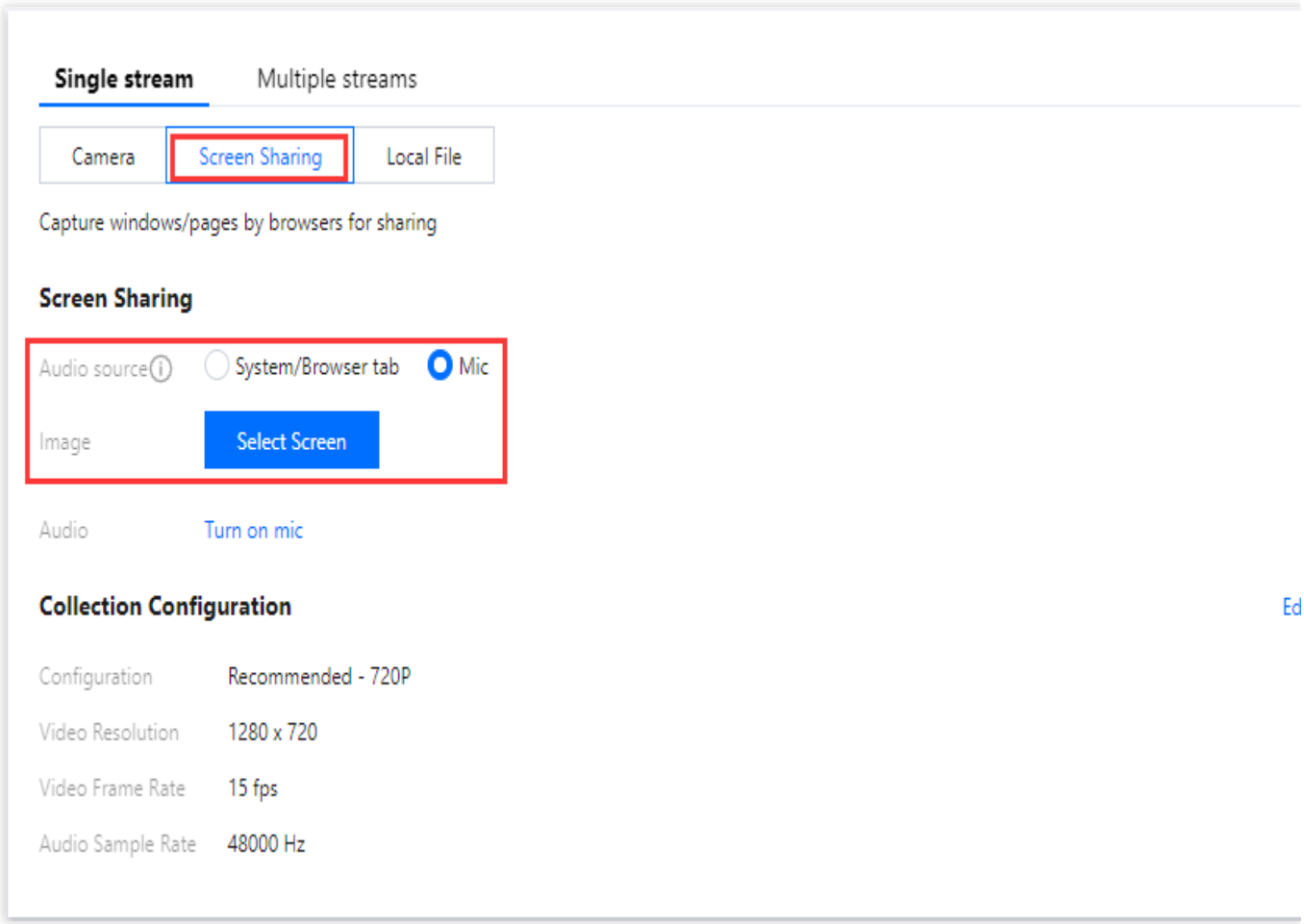
You have logged in to the CSS console.
You have added a push domain name.
Your device has a camera installed and your browser allows Flash to access the camera.

Single stream

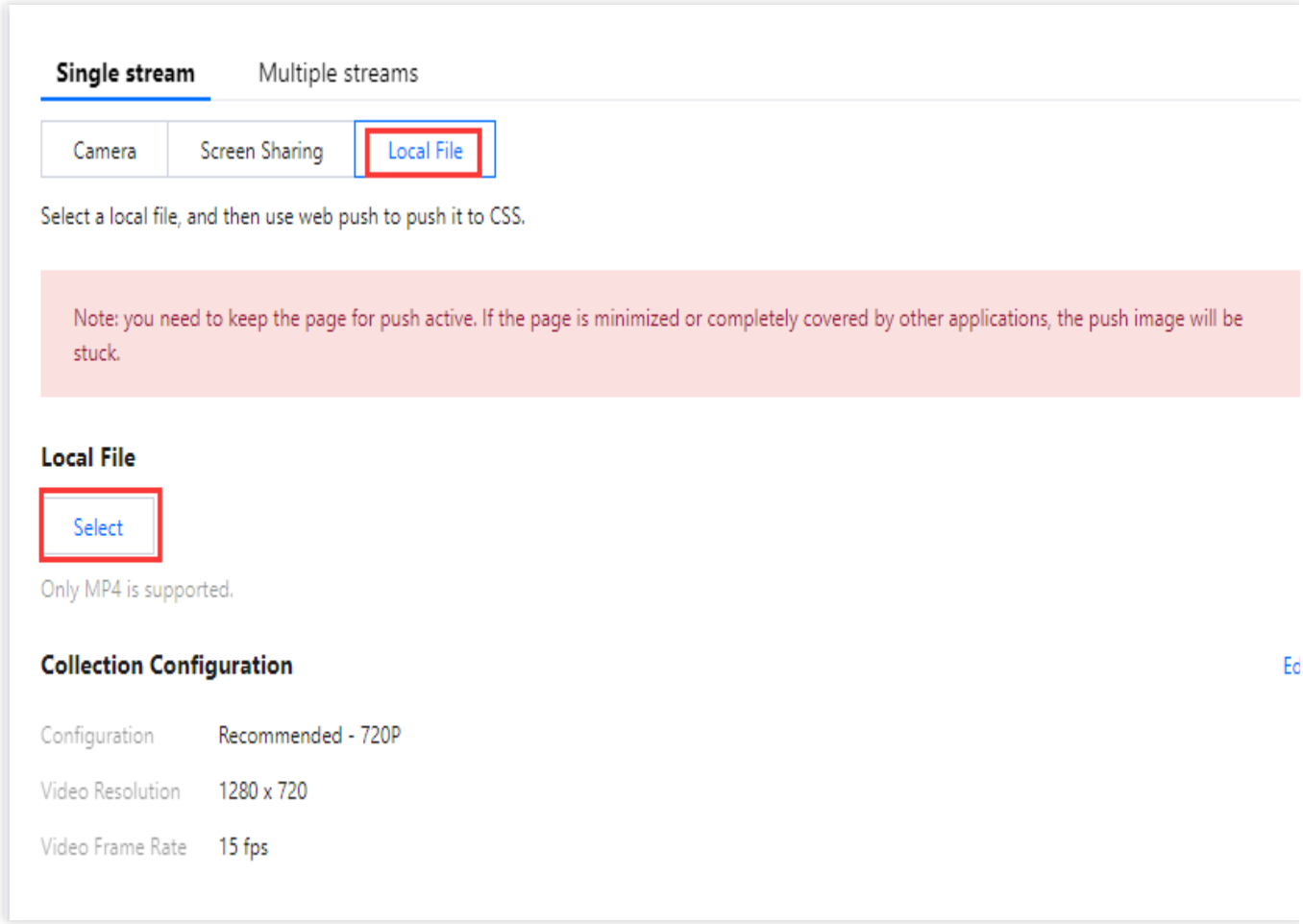
1. Log in to the CSS console and select **Web Push**.Click on **Single stream**.
2. **Select the capturing source**, which can be camera, screen, or local file.
Camera
Screen Sharing
Local File
Capture and publish audio/video from the camera/mic (which can be a peripheral device). Click **Turn On** for **Camera**/**Mic**. You need to grant your browser access to the camera/mic if it is the first time you perform this action.



Capture and publish streams from the screen. Click **Select Screen** to select a screen/window/browser tab to publish.



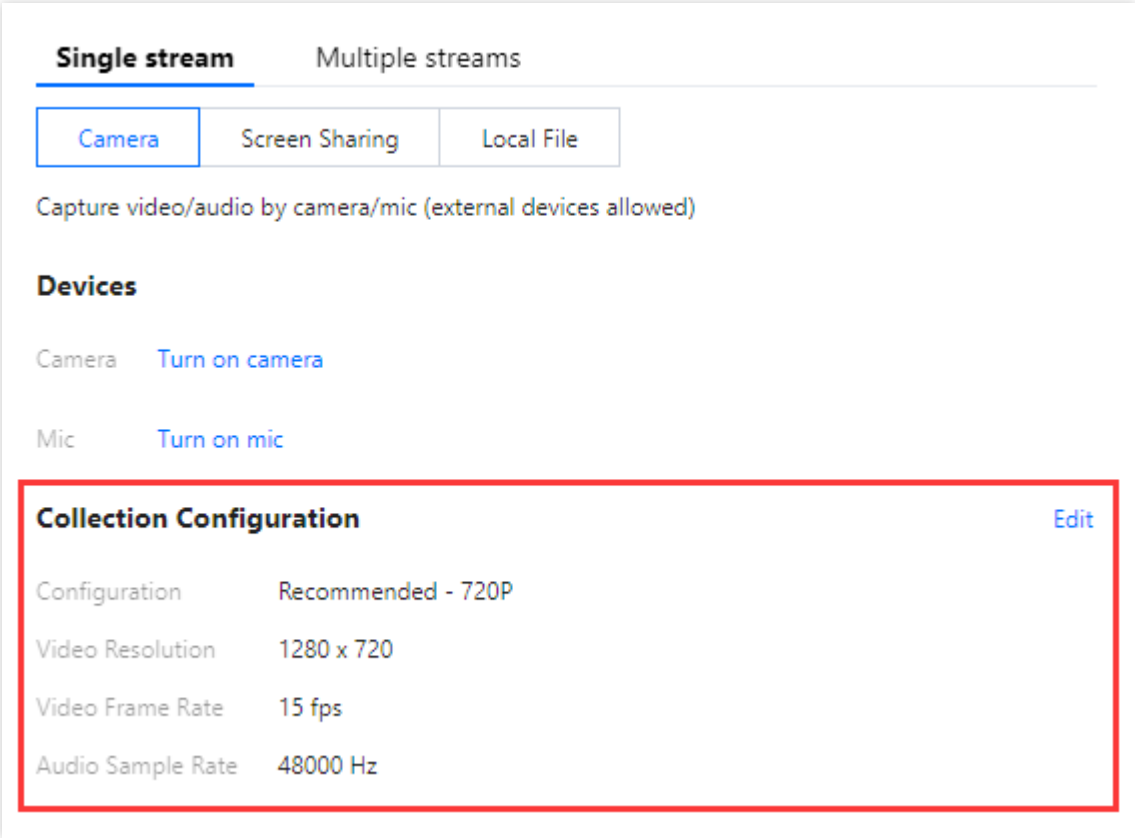
Publish a local file using the web push tool to CSS. Click **Select** to select a file to publish. Currently, you can publish only files in MP4 format.



Note：

You cannot change the capturing source after enabling camera preview or selecting screen content to share. To switch the source, disable camera preview or cancel screen sharing first.

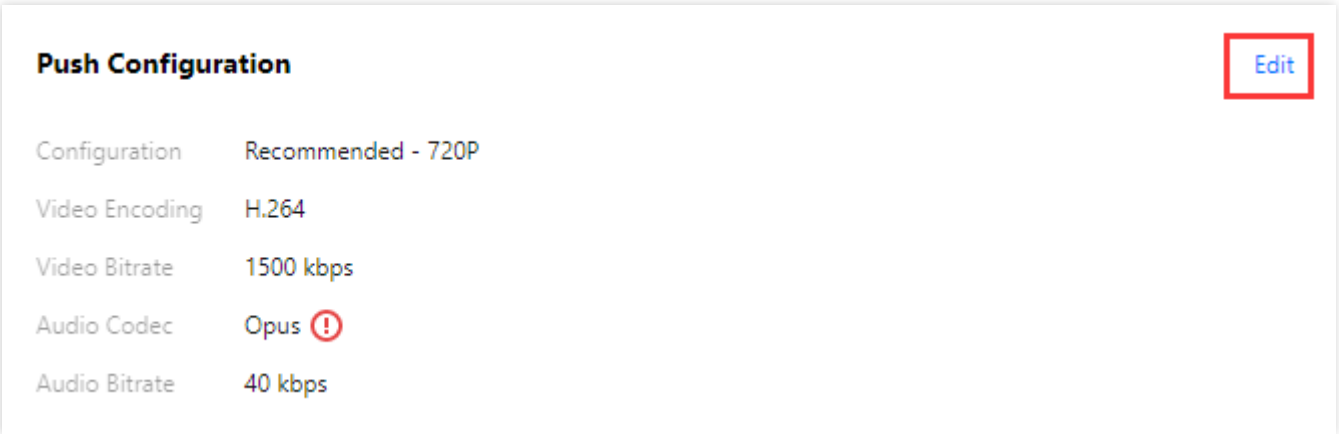
3. **Configure capturing data**. The defaults are recommended settings, which vary with resolution. You can click **Edit** and select **Custom** to customize capturing data. **For camera and screen sharing, the settings include resolution, video frame rate, and audio sample rate, while for local files, only the former two are applicable.**



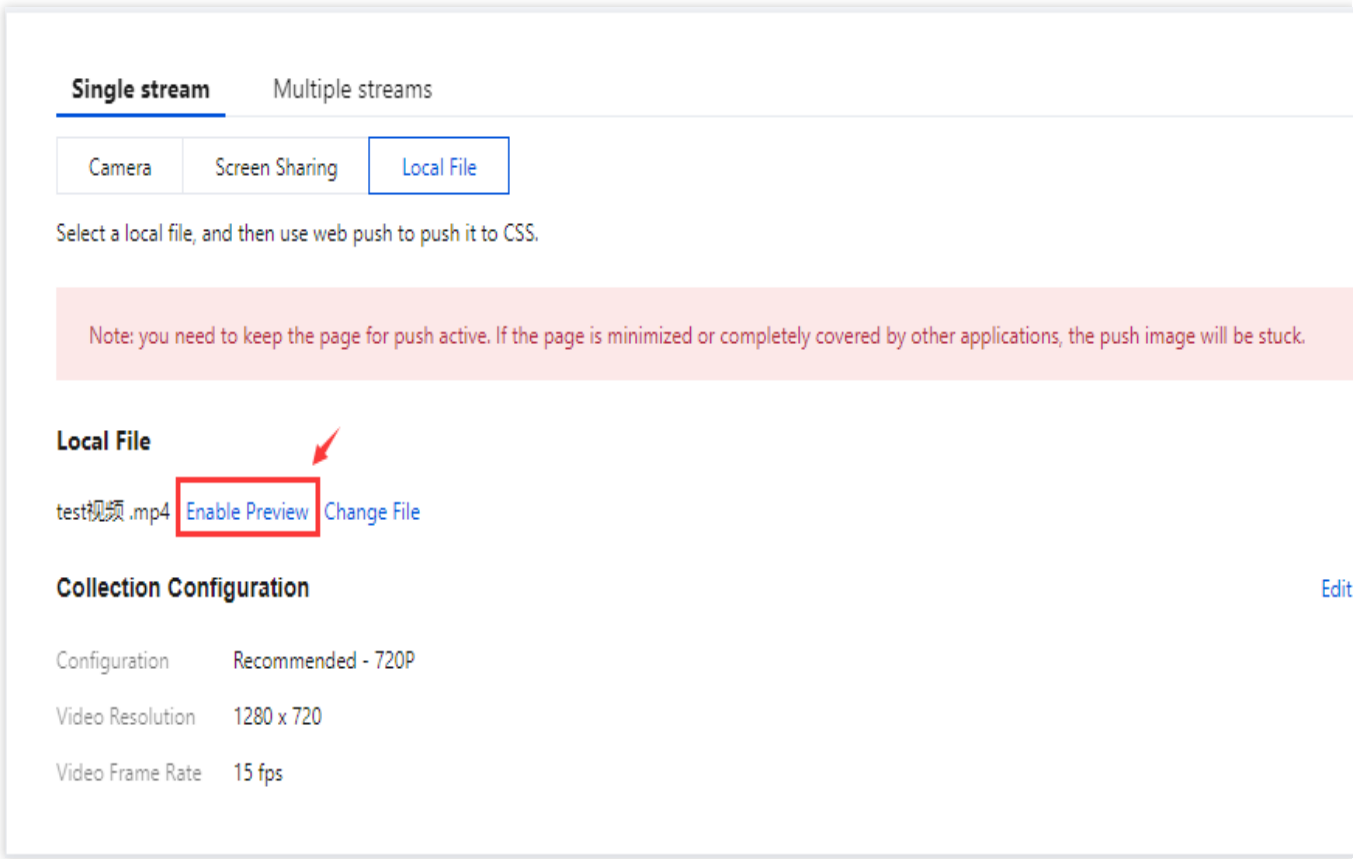
4. **Configure push data**. The defaults are recommended settings (the recommended video bitrate varies with resolution, and the audio bitrate is fixed). You can click **Edit** and select **Custom** to customize video and audio bitrates.

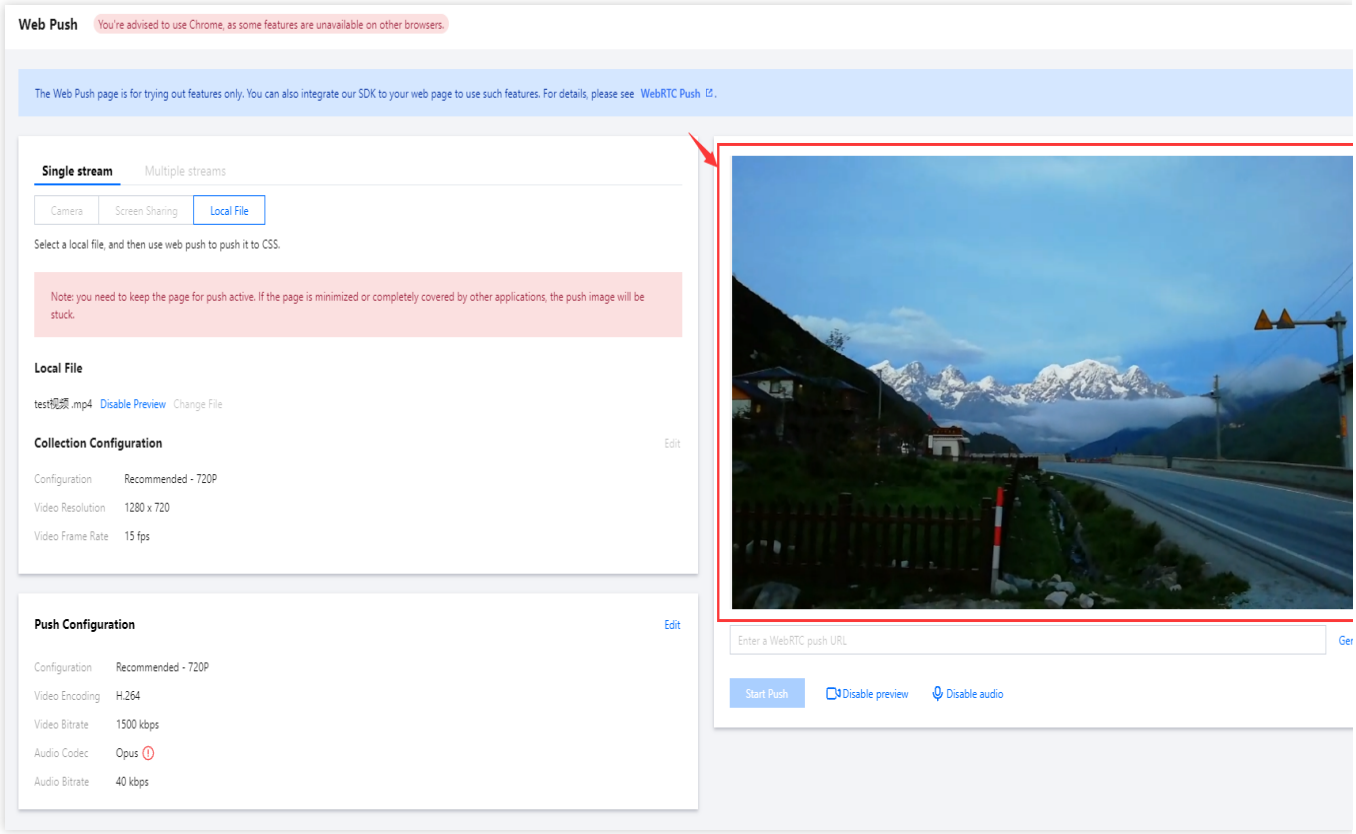
Note：

WebRTC push uses the Opus audio codec, and you are advised to play the streams pushed using LEB WebRTC URLs. If you use a standard live streaming protocol (RTMP, FLV, or HLS), the system will automatically convert the streams to AAC, which will incur transcoding fees. For details, see the billing document.

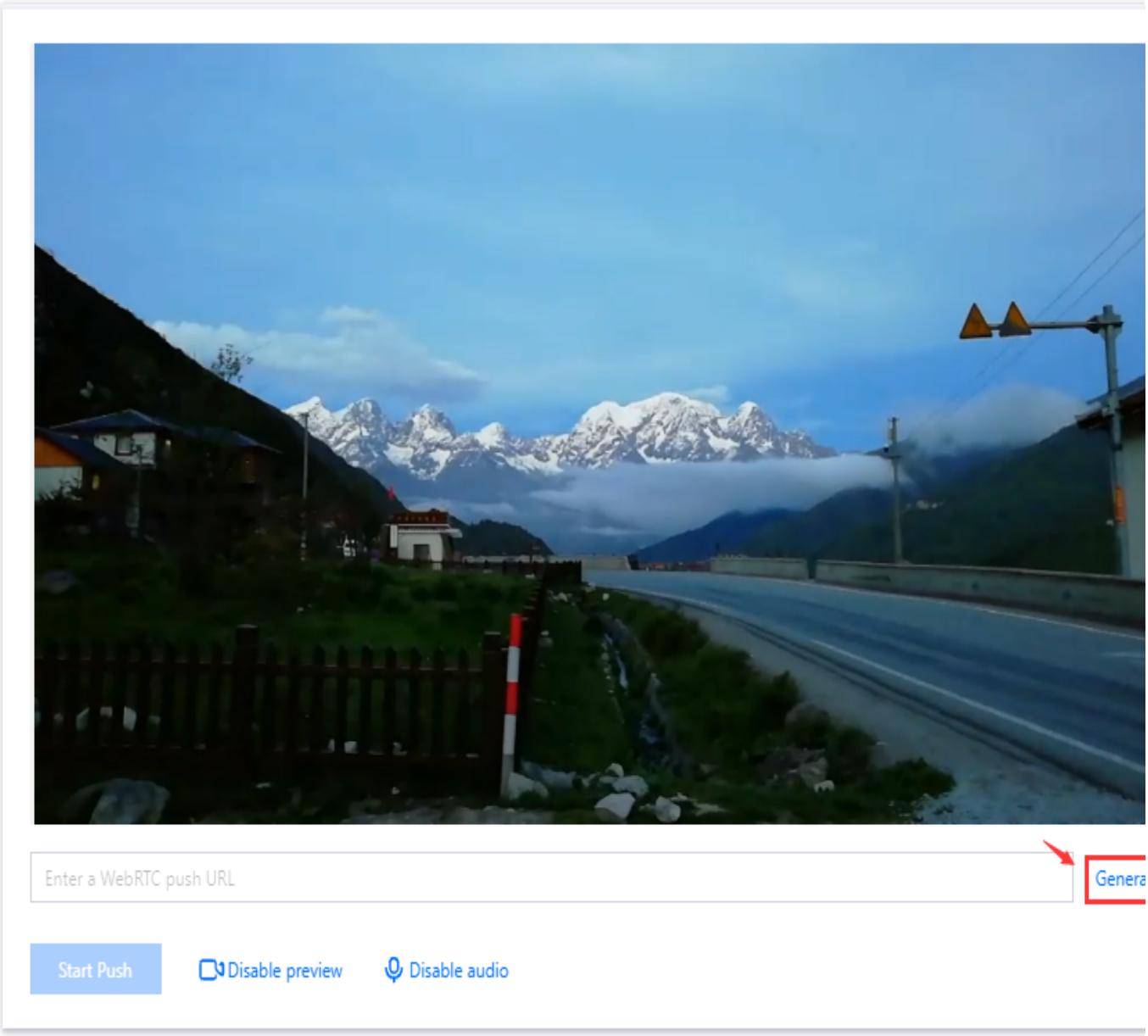


5. **Preview streams**. After completing the above steps, you can enable preview to preview the stream on the right.


Single stream
Multiple streams
Camera
Screen Sharing
Local File
Select a local file, and then use web push to push it to CSS.
Note: you need to keep the page for push active. If the page is minimized or completely covered by other applications, the push image will be stuck.
Local File
test视频 .mp4
Enable Preview
Change File
Collection Configuration
Edit
Configuration
Recommended - 720P
Video Resolution
1280 x 720
Video Frame Rate
15 fps



6. Enter a WebRTC push URL or click **Generate** and complete the following configuration:



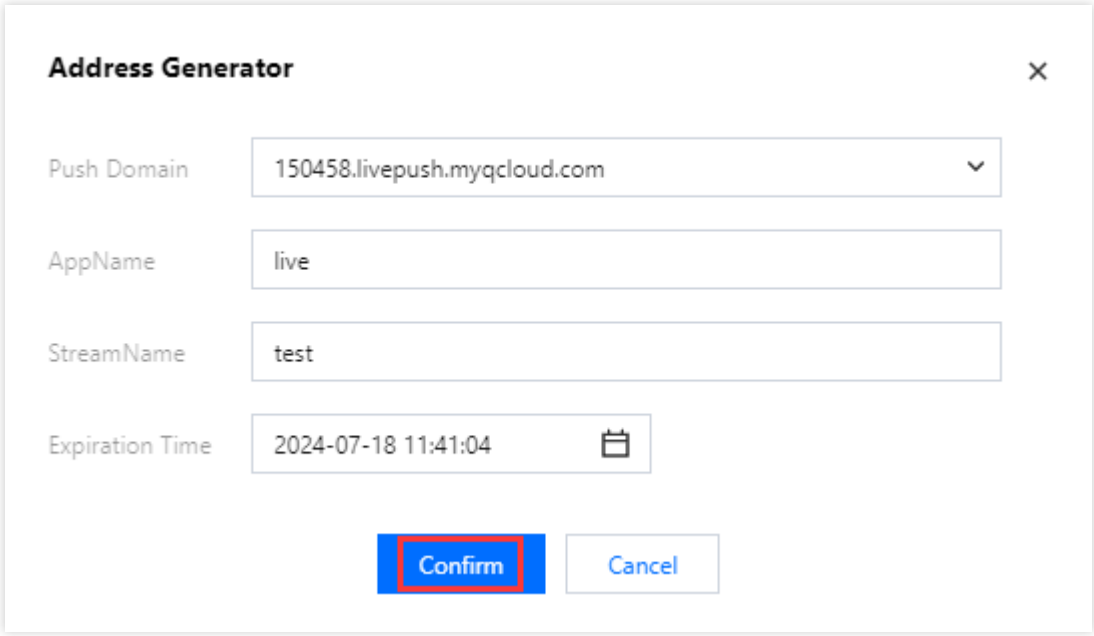
6.1 Select your push domain.

6.2 Enter a unique `AppName` for an application to distinguish it from other applications under the same domain name. `AppName` is `live` by default.

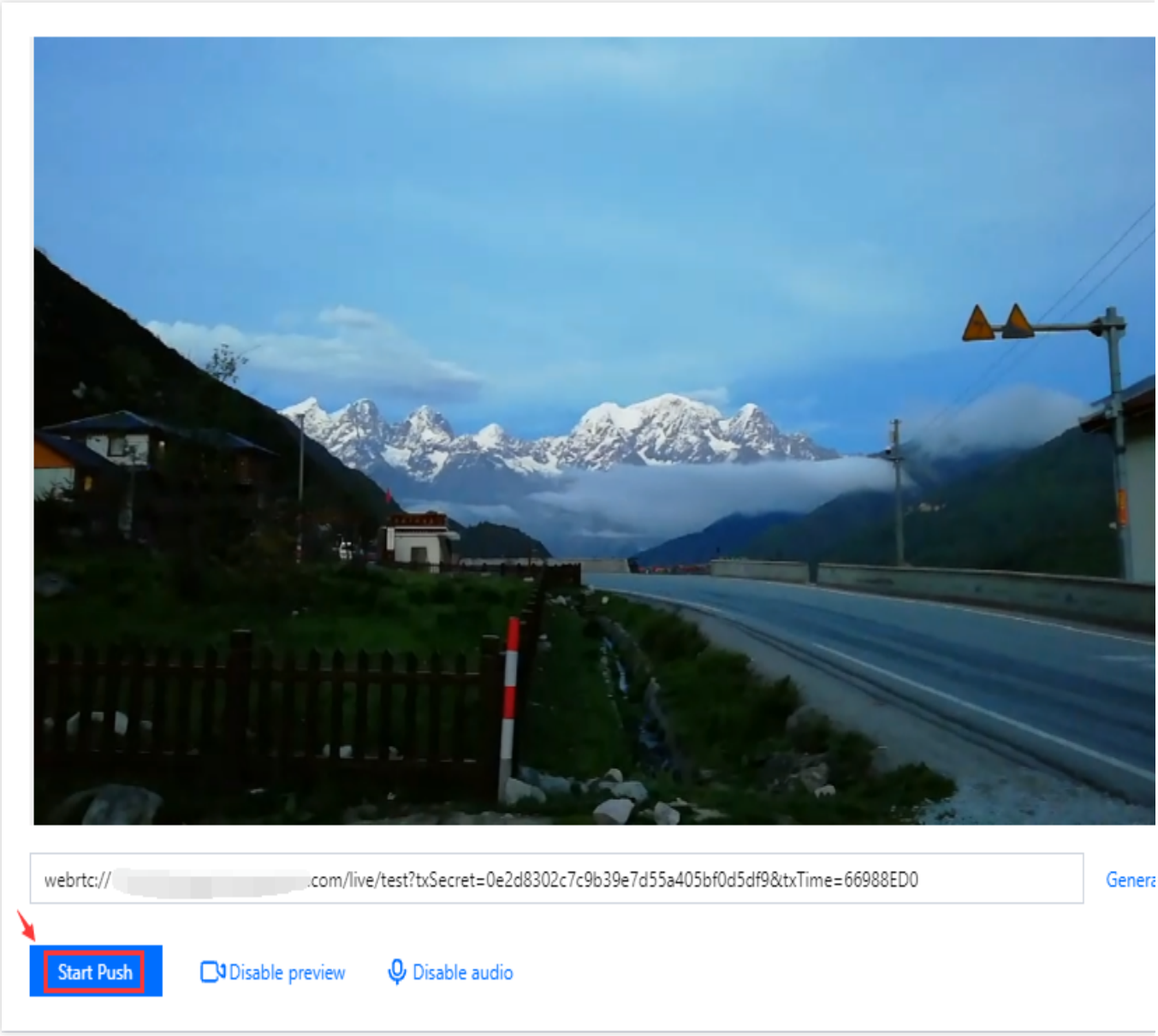
6.3 Enter a custom `StreamName`, such as `test`.

6.4 Select an expiration time, such as `2024-07-18 11:41:04`.

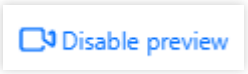
6.5 Click **Confirm**, and a push URL is auto-generated.



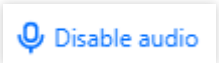
7. Click **Start Push** to start streaming.



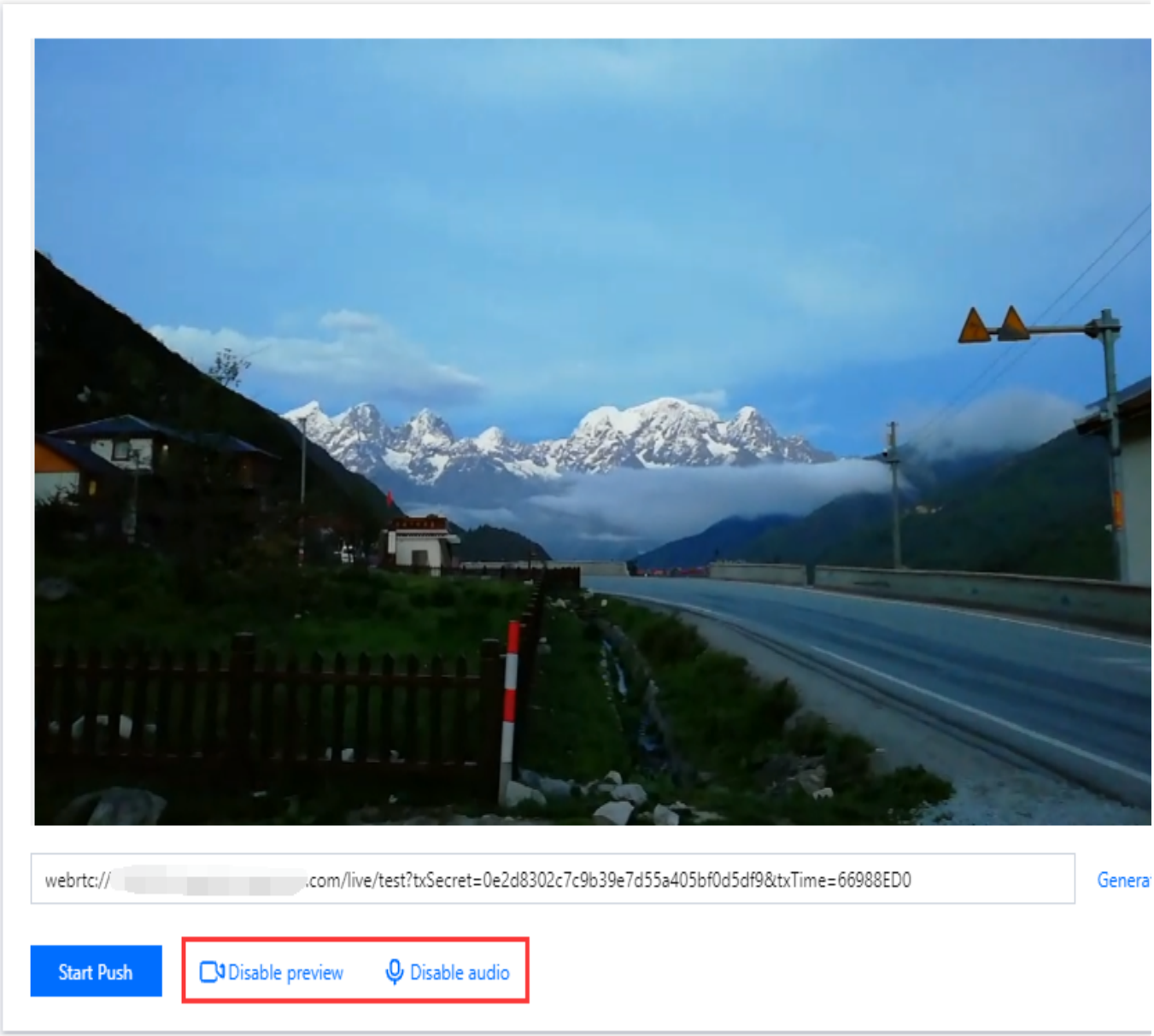
7.1 To enable/disable video or audio, click



or



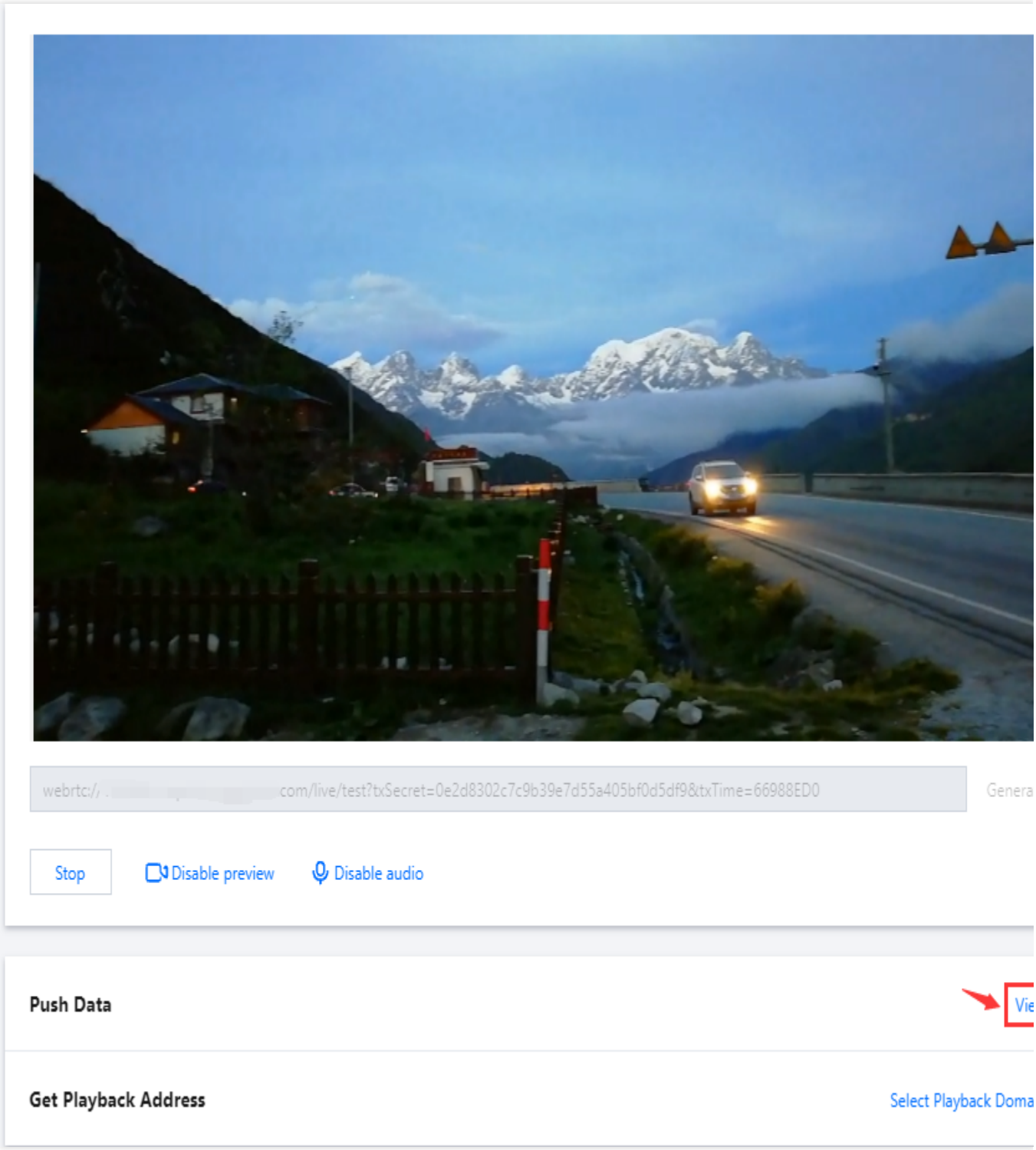
. After you disable video/audio, data capturing will continue and push will still succeed, but the stream cannot be previewed and will have no video or audio.



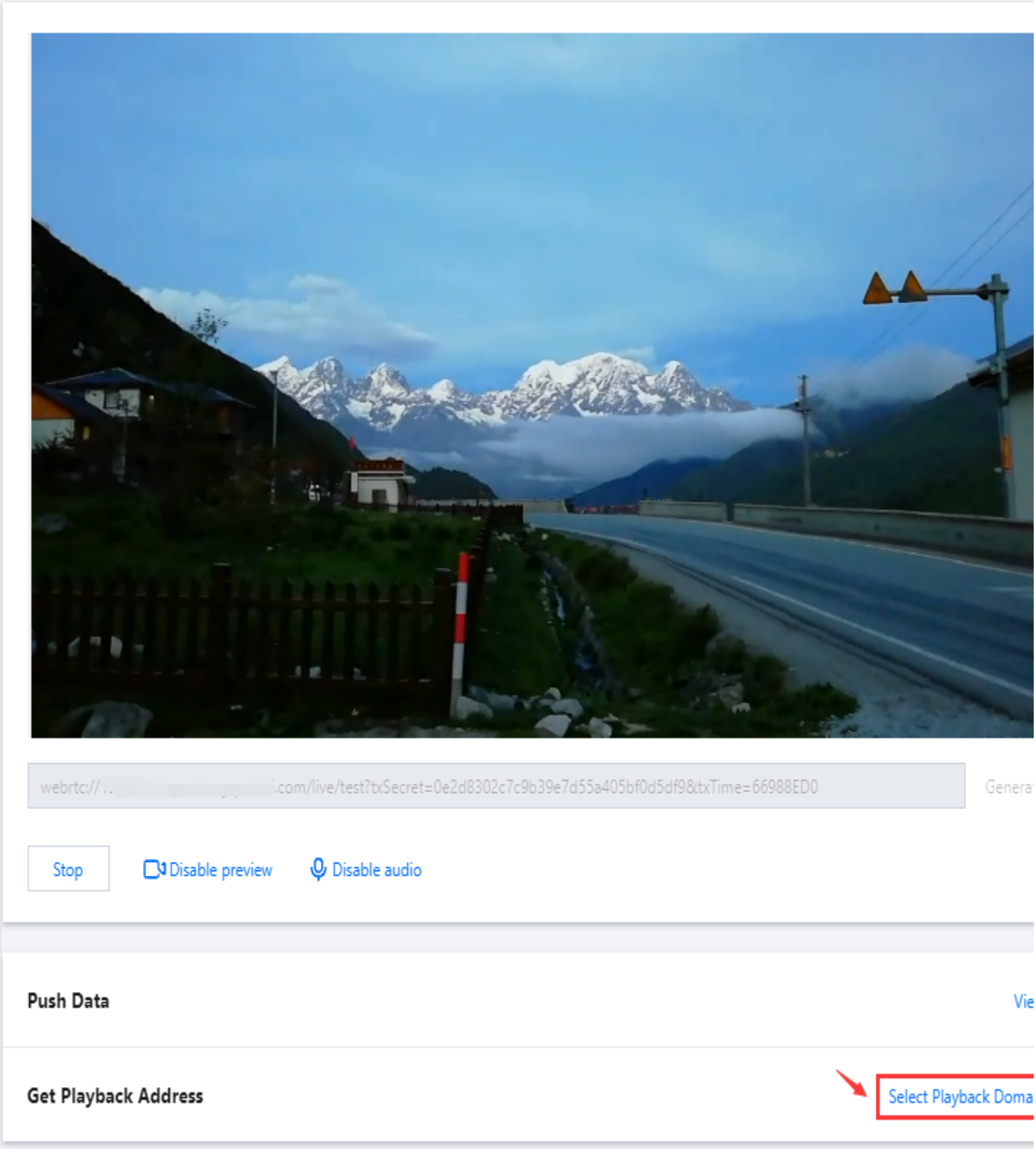
Note：

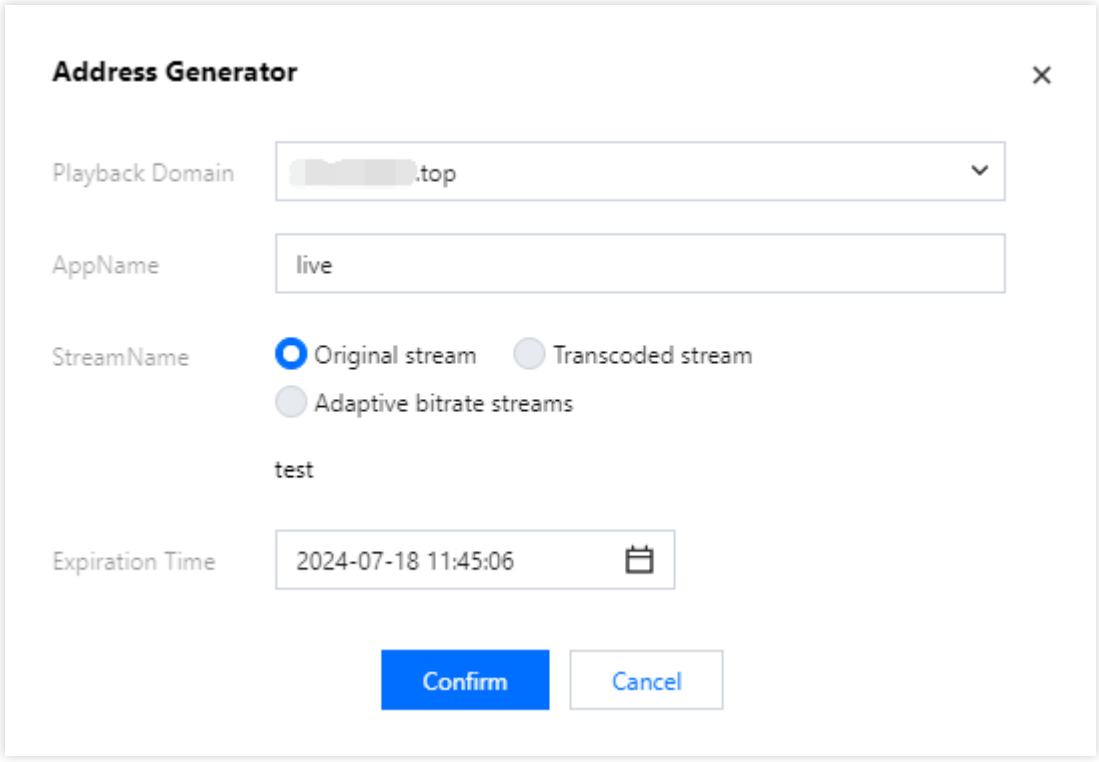
You cannot enable or disable preview after push succeeds, and you may incur bandwidth/traffic costs or the costs of other value-added services for pushing streams.

8. After push succeeds, click **View** below the preview to view streaming statistics. You cannot obtain statistics or playback URLs for push URLs not under your account. Please use a push domain under your account to generate push URLs or relay streams to your account.

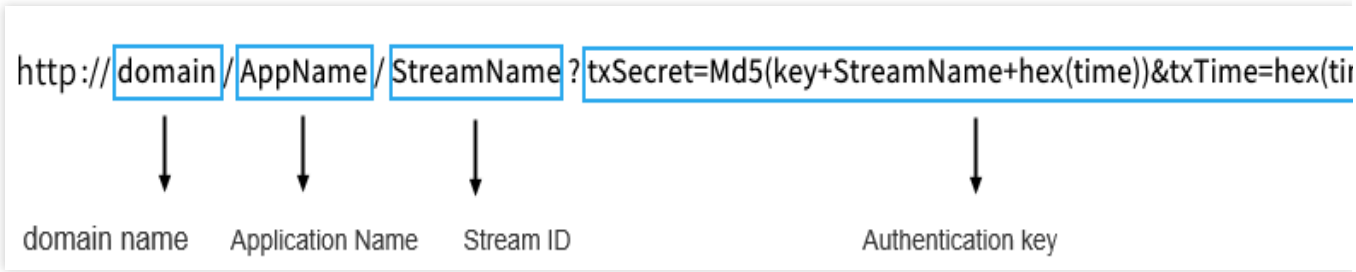


9. If you have added a playback domain in **Domain Management**, you can **select the domain** to generate a playback URL. If you need to generate a playback address with transcoding or adaptive transcoding configuration, you must first bind the playback domain to a transcoding template or adaptive transcoding template to generate a transcoded stream or adaptive transcoded stream.


webrtc://
.com/live/test?txSecret=0e2d8302c7c9b39e7d55a405bf0d5df9&txTime=66988ED0
Stop
Disable preview
Disable audio
Push Data
Vie
Get Playback Address
Select Playback Doma



A playback URL is made up of four parts, as shown below:



Supported protocols include RTMP, FLV, HLS, and UDP. You can also click the QR code icon and scan the QR code using the TCToolkit app to obtain the playback URL.

Note：

If HTTPS is enabled for the playback domain selected, the FLV and HLS URLs generated will start with https.

Multiple streams

Enter configuration

1. Log in to the CSS console and select **Web Push**.Click on **Multiple streams**.

2. In the input configuration, click **Add**. Choose the capture method. You can select from three capture methods: camera capture, screen sharing capture, and local file capture. You can also add text configuration for multi-stream mixed live streaming. **Up to 10 input sources can be added**.

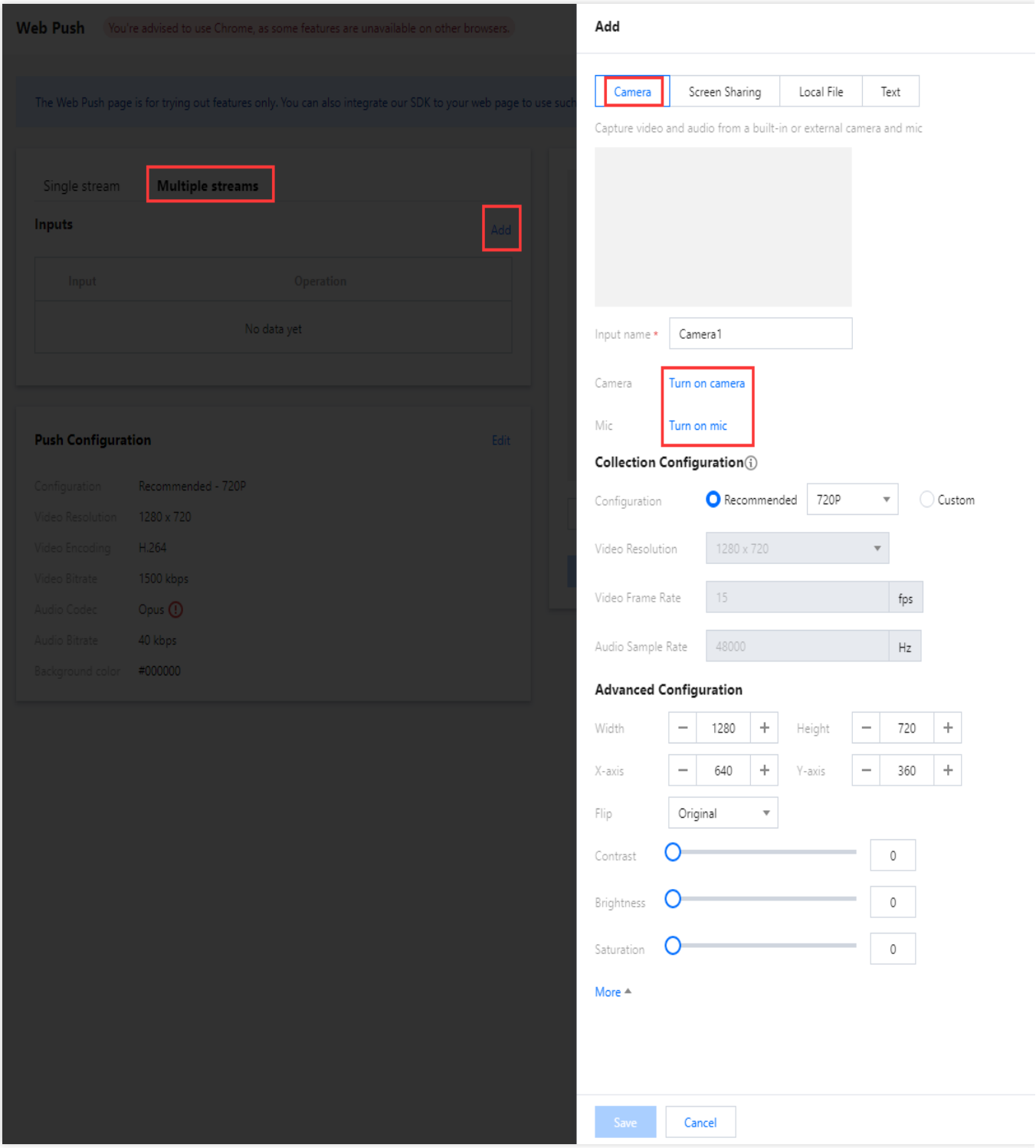
Camera

Screen Sharing

Local File

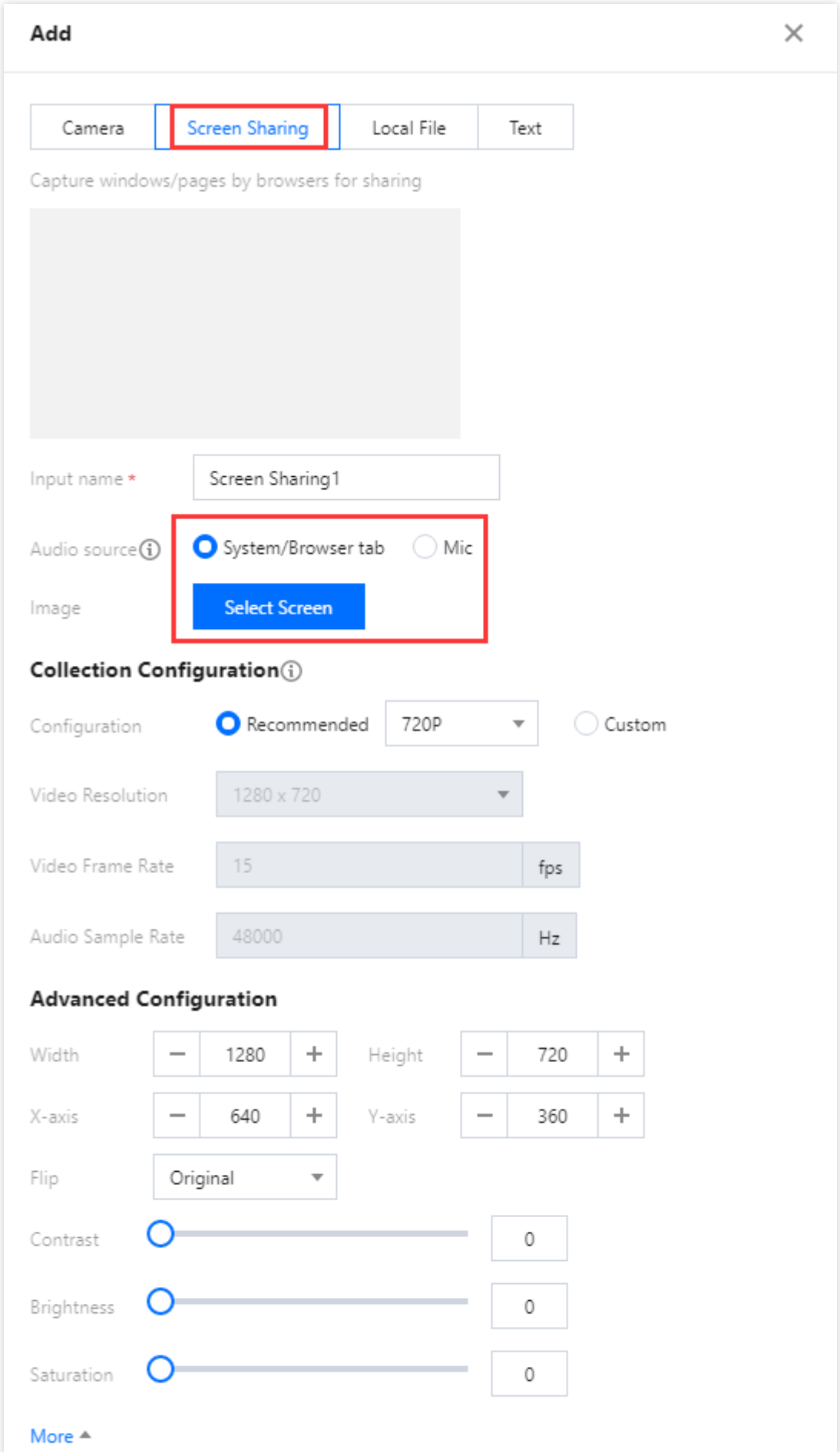
Text

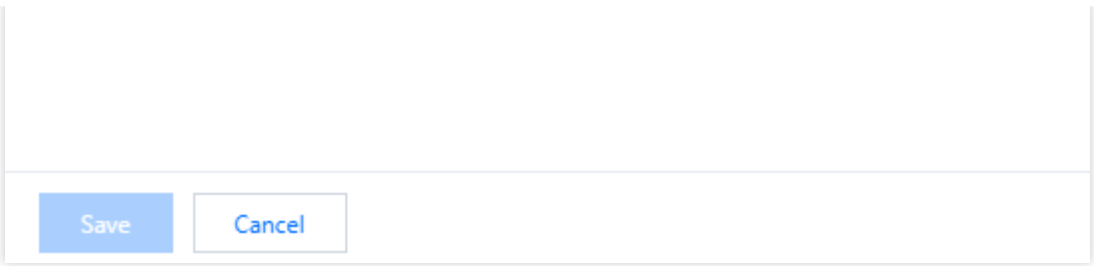
Camera capture is the process of capturing video and audio through a camera/microphone (external devices are supported). Click **Enable Camera**/ **Enable Microphone**, and the first time you enable it, you'll need to grant the browser permission to use the camera and microphone.



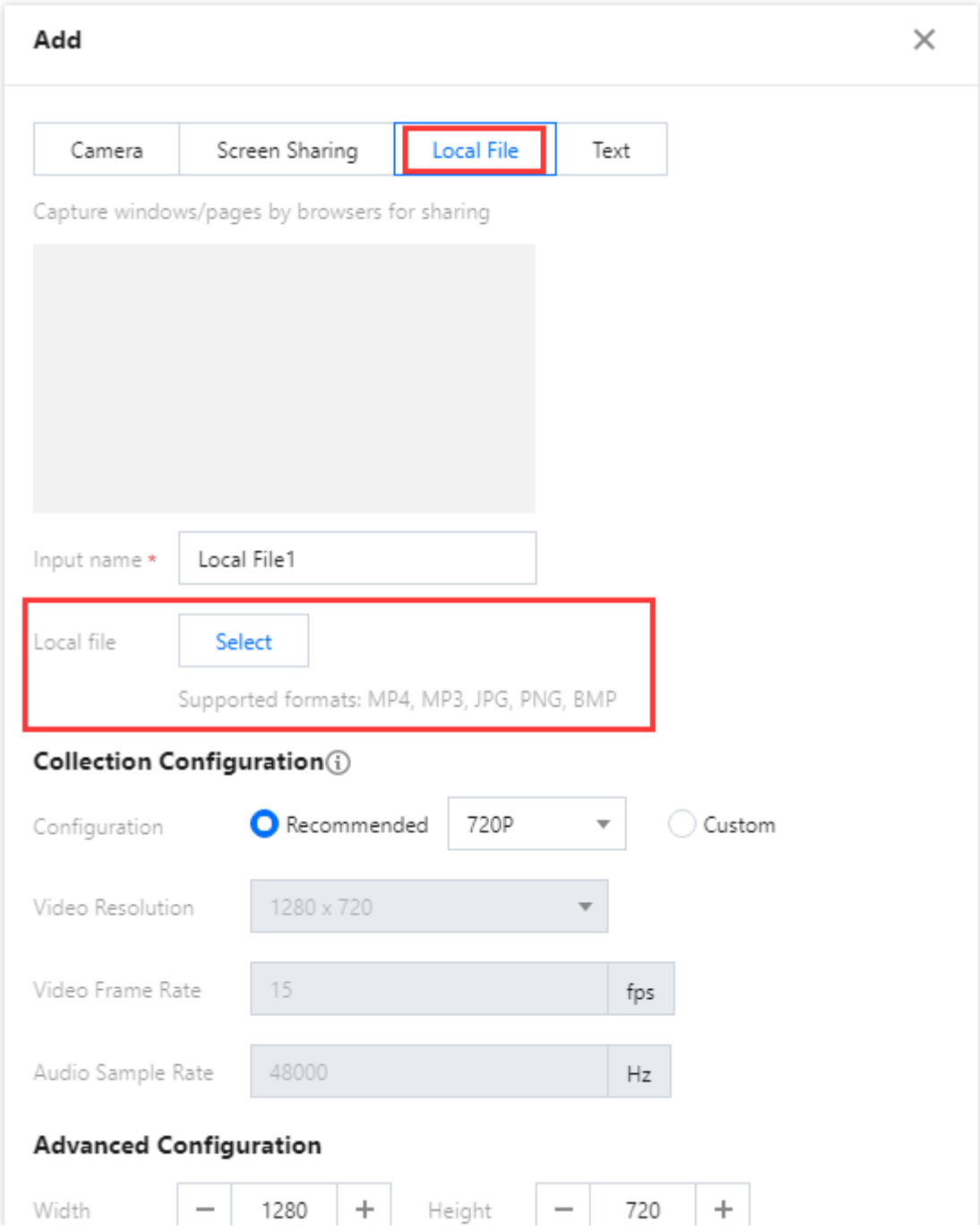
Screen sharing capture is the process of capturing a specific window or interface through the browser for sharing. Click **Select Screen Sharing** and choose the content to share, which can be the entire screen, a specific window, or a browser tab. You need to select the screen to share before you can save it.

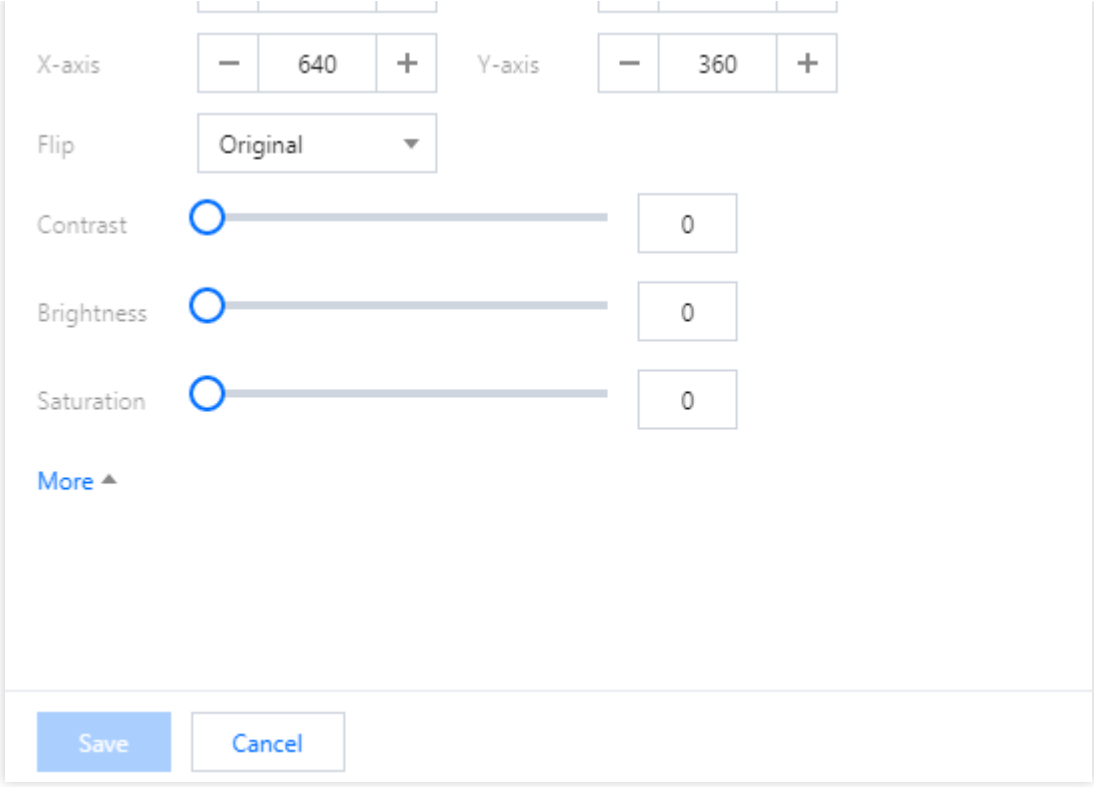
Screen sharing capture supports selecting audio sources. Currently, only Chrome 74+ and Edge 79+ support capturing sound. On Windows systems, you can capture the entire system's sound, while on Linux and Mac, you can only capture the sound from a browser tab.


Add
Camera
Screen Sharing
Local File
Text
Capture windows/pages by browsers for sharing
Input name *
Screen Sharing1
Audio source
System/Browser tab
Mic
Image
Select Screen
Collection Configuration
Configuration
Recommended
720P
Custom
Video Resolution
1280 x 720
Video Frame Rate
15
fps
Audio Sample Rate
48000
Hz
Advanced Configuration
Width
1280
Height
720
X-axis
640
Y-axis
360
Flip
Original
Contrast
0
Brightness
0
Saturation
0
More



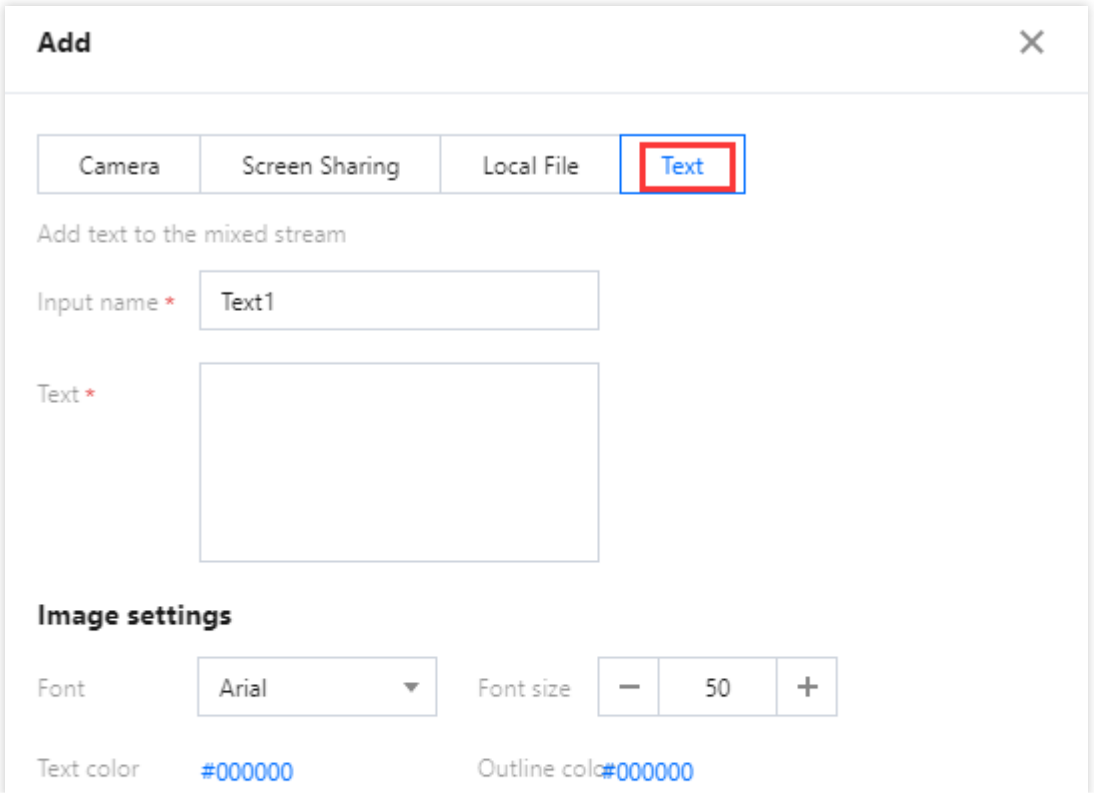
Local file capture is the process of capturing images from a specified local file and then pushing it to the cloud live streaming service using a Web-based push tool. Click **Select Local File** to choose the content to be pushed. Currently, MP4, MP3, JPG, PNG, and BMP file formats are supported. Click **Enable Preview** to save the settings.

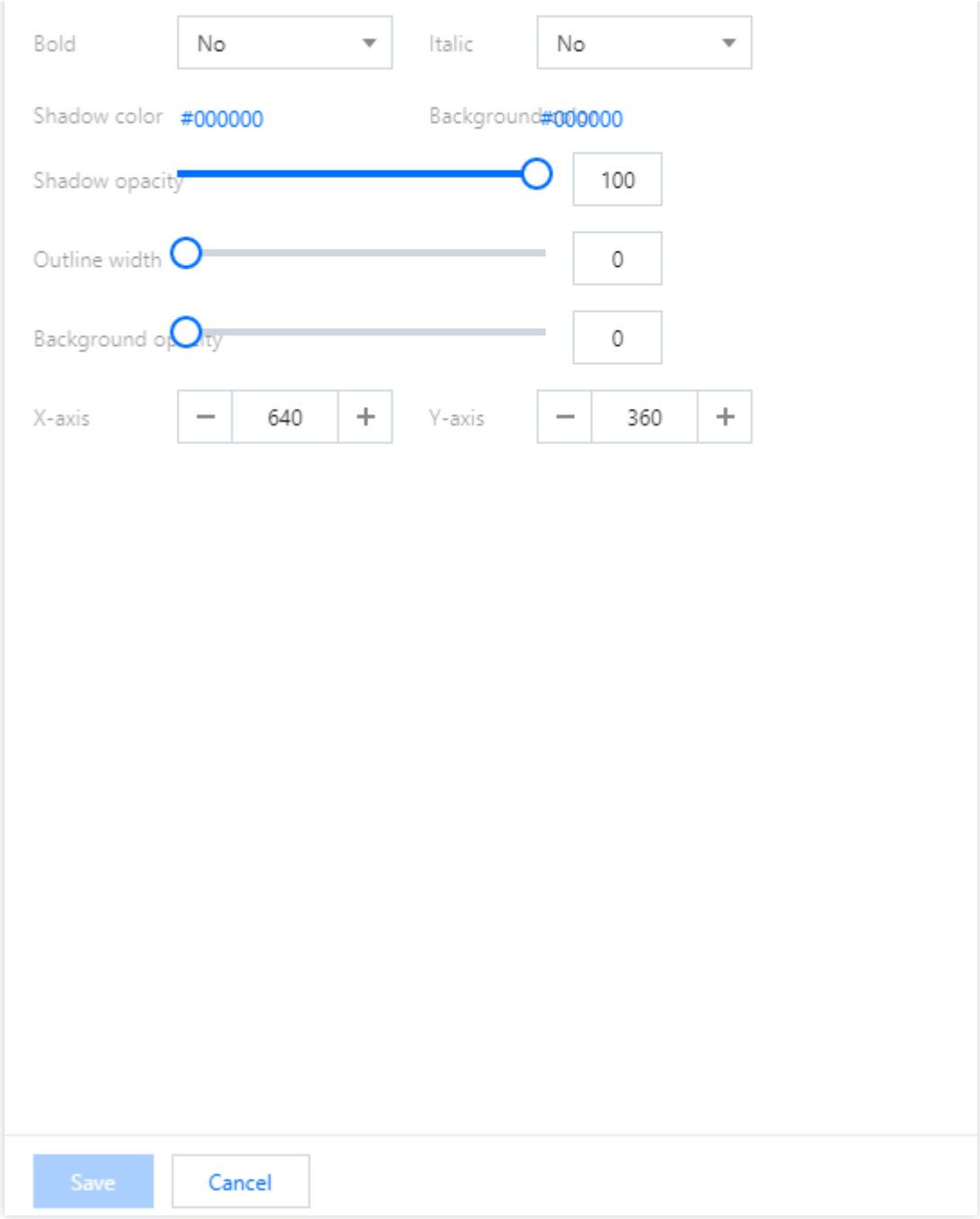




Text configuration allows you to add text to the mixed streaming image and then push it to the cloud live streaming service using a Web-based push tool. Enter text in the text content field.

In the image configuration, you can set the font, color, shadow, transparency, thickness, and text coordinates. The default text coordinates are in the center of the page.



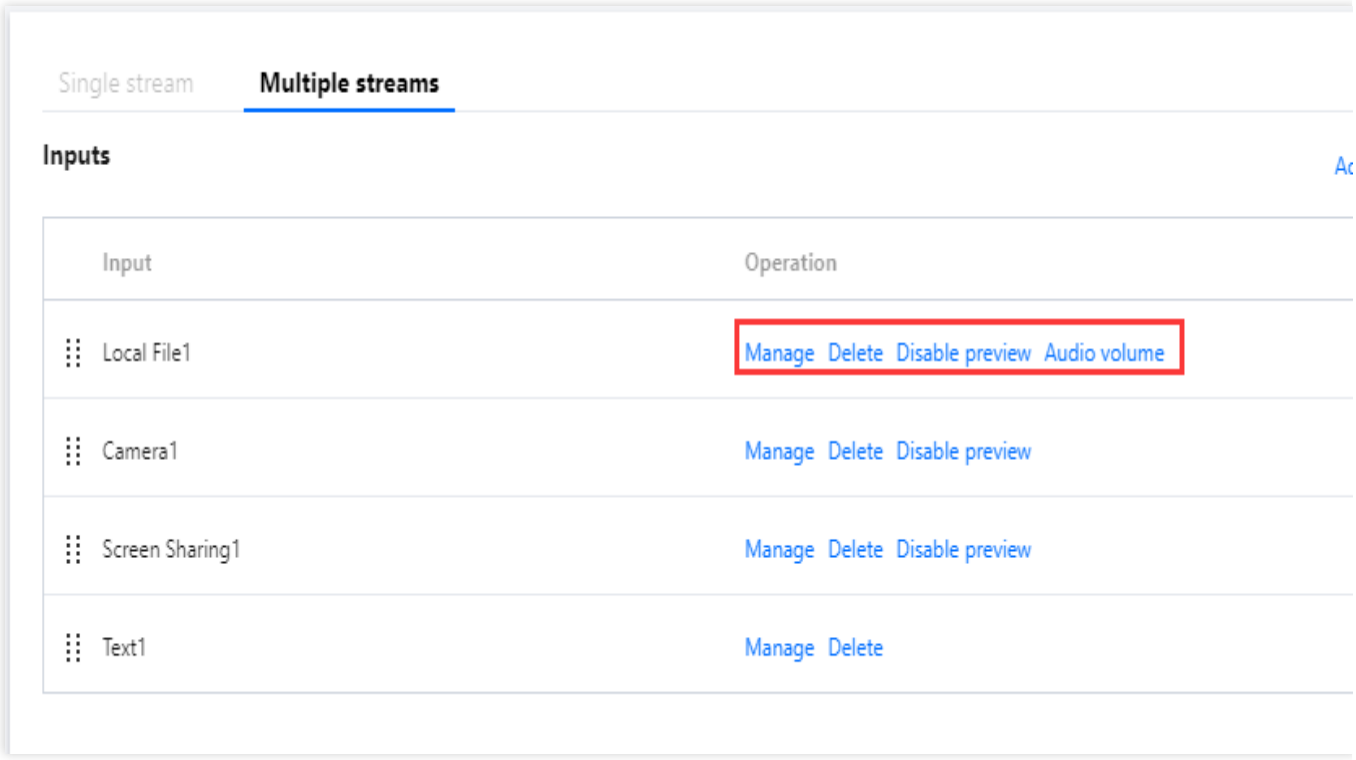


3. You can set capture configurations for camera capture, screen sharing capture, and local file capture. The default is the recommended configuration (different resolutions have different recommended configurations). Switching or modifying the configuration is not supported during the capture process. You need to make changes when the preview is closed.
4. You can set advanced configurations for camera capture, screen sharing capture, and local file capture. You can adjust the image, coordinates, mirroring, contrast, brightness, and saturation.
5. Click **Save**, and the input source will be added to the configuration.

Change setting

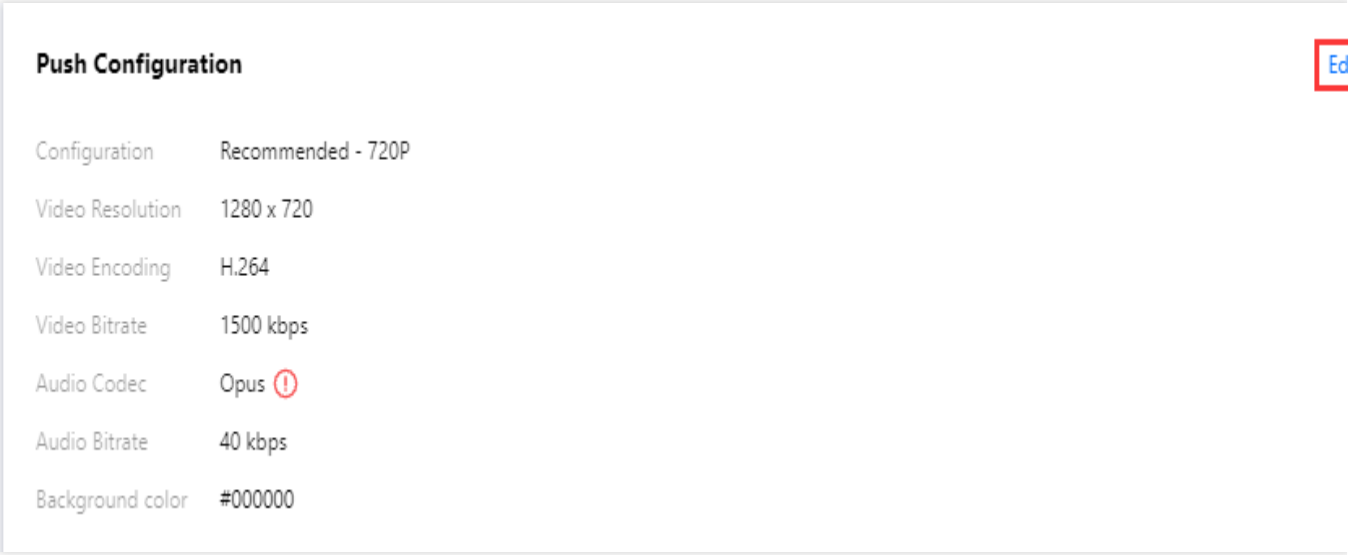
1. In the input configuration, you can perform operations on the configured input sources.

2. Select the input source you want to modify and click **Configure**. The right-side pop-up window will display the configuration information of this input source, and you can modify the configuration information again. Switching or modifying the configuration is not supported during the capture process. You need to make changes when the preview is closed.
3. You can adjust the display order of input sources by dragging the buttons on the left side of the input sources up or down.
4. Click **Delete** to remove the input source.
5. Click **Disable Preview** to close the preview of the input source, but you can still select the image for editing in the image editing area.
6. For input sources with audio, you can adjust the volume. Click "Adjust Volume", drag the volume slider, and click **Confirm** to confirm.



Push configuration

Push configuration: Set the push configuration, with the default being the recommended configuration (different resolutions have different recommended video bitrates, and audio bitrate cannot be modified). You can click **Edit** in the upper right corner to enter custom editing configuration, where you can customize and modify the video and audio bitrates.

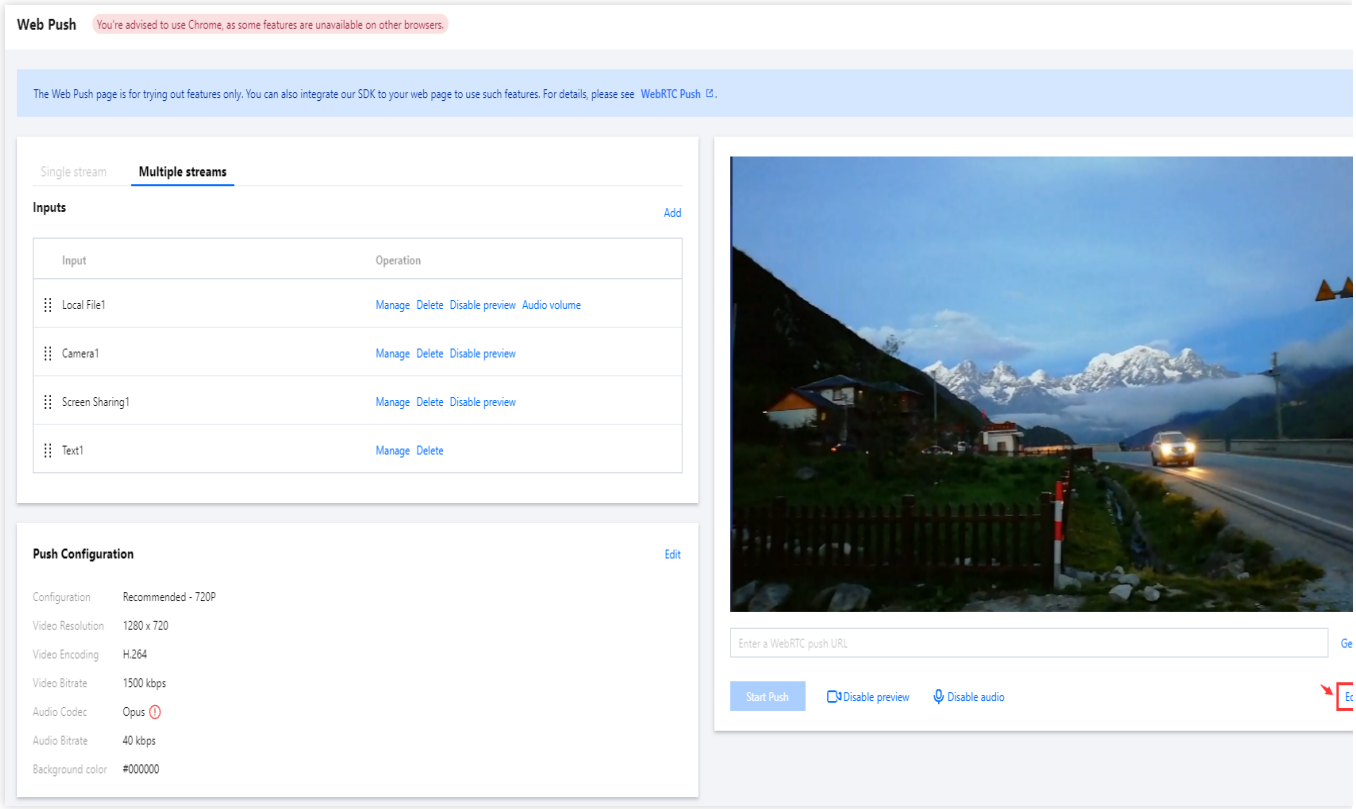


Note：

The audio encoding method for web push is Opus encoding, and it is recommended to use the Live Event Broadcasting (LEB) WebRTC address for playback. If you use the playback address of the standard live streaming (RTMP/FLV/HLS), the system will automatically convert it to AAC encoding for normal playback, which will generate audio transcoding fees. For details, please refer to the Billing Documentation.

Screen editing

1. After confirming the input configuration and push configuration, you can see the preview image in the preview box on the right, and you can edit the image as needed.
2. Click **Edit**, select the image in the preview box that needs to be adjusted, and you can drag and resize the image as needed.
3. After adjusting, click **Exit Edit**. If you are in the middle of pushing the stream, saving the changes will continue pushing the stream with the new image layout.

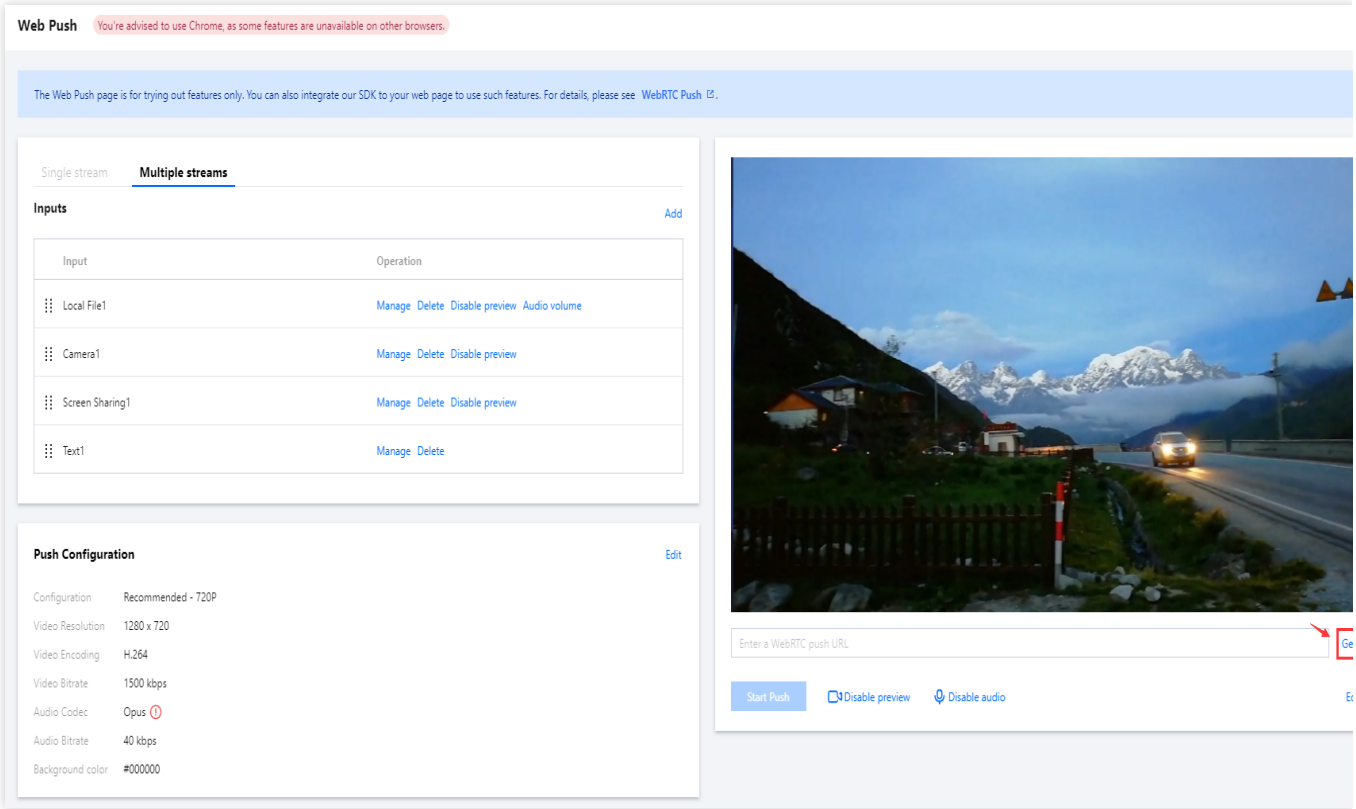


Note：

When you enter the image editing mode, you can adjust the image layout in the preview box. Exiting the image editing mode allows you to view the preview image of the push stream in the preview box. Editing the page does not affect the real-time push stream, and the configuration will be saved only when you exit the editing mode.

Push address

1. Enter the WebRTC push address in the preview box below or click **Generate**, and configure the following information in the pop-up window:



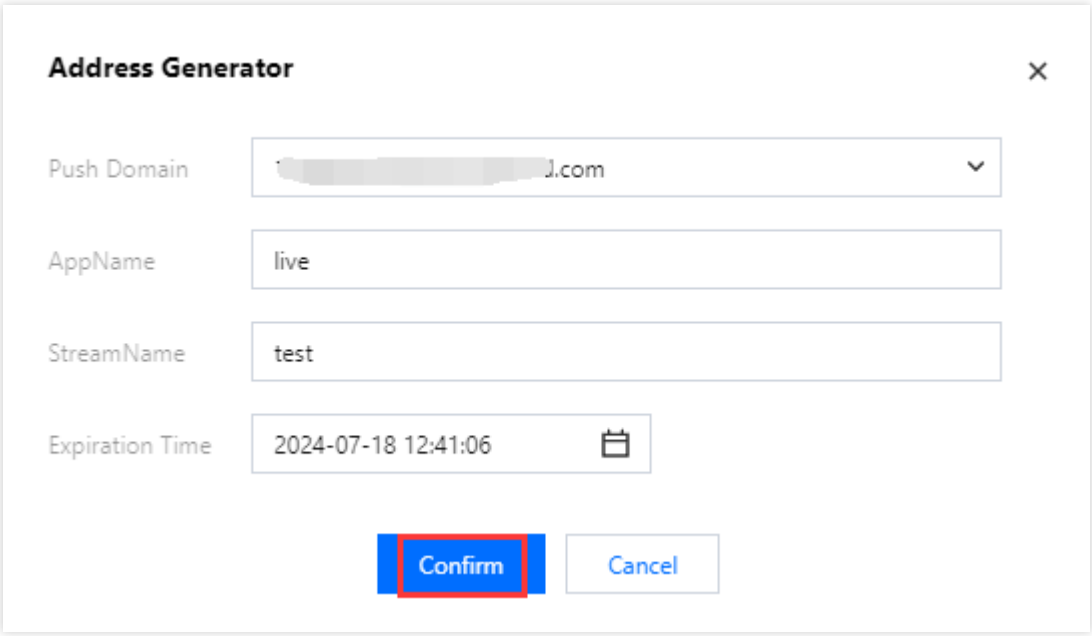
1.1 Select your push domain.

1.2 Enter a unique AppName for an application to distinguish it from other applications under the same domain name. AppName is live by default.

1.3 Enter a custom StreamName, such as test.

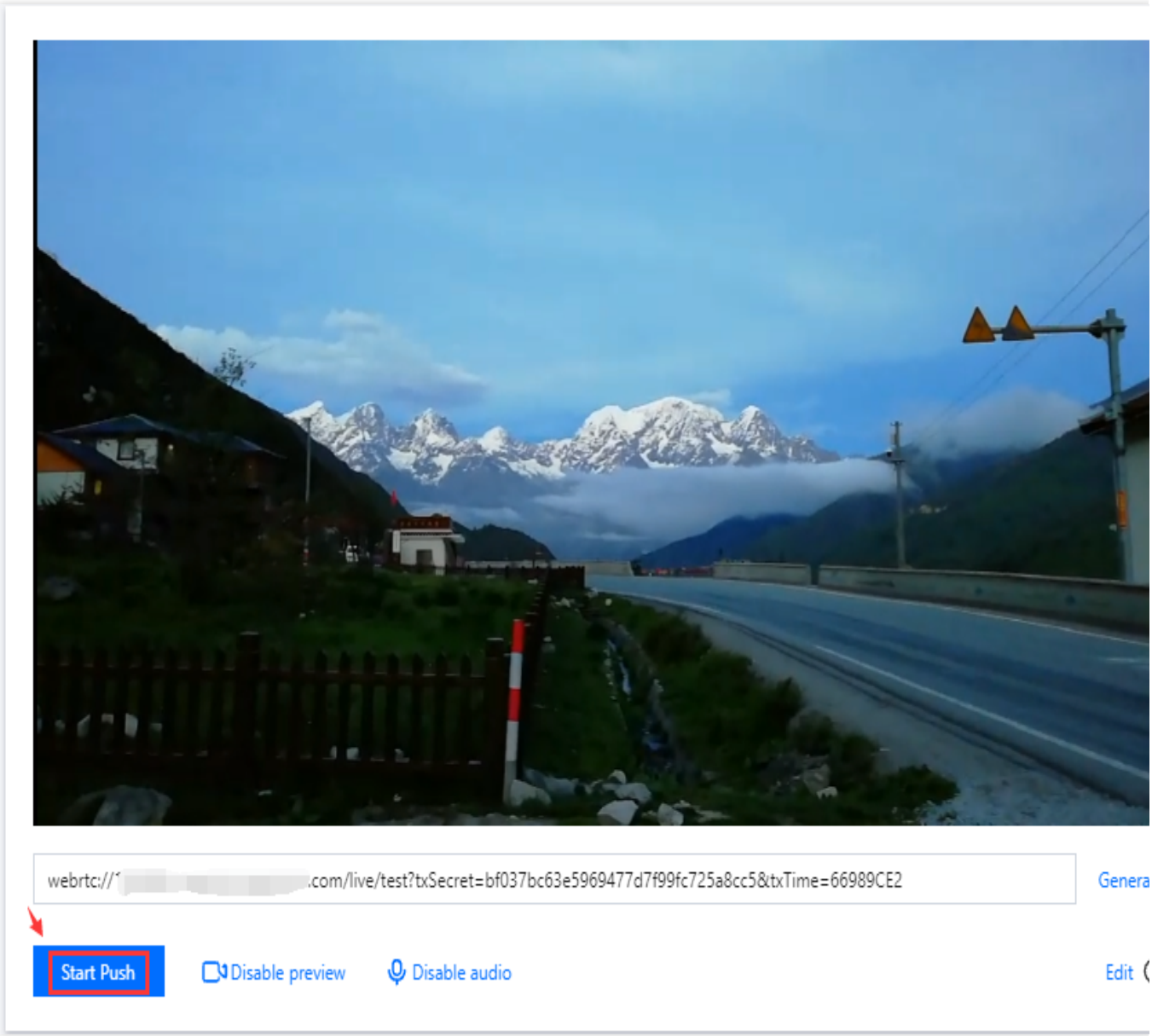
1.4 Select an expiration time, such as `2024-07-18 12:41:06` .

1.5 Click **Confirm**, and a push URL is auto-generated.

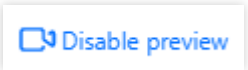


Start streaming

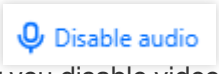
1. To enable/disable video or audio.



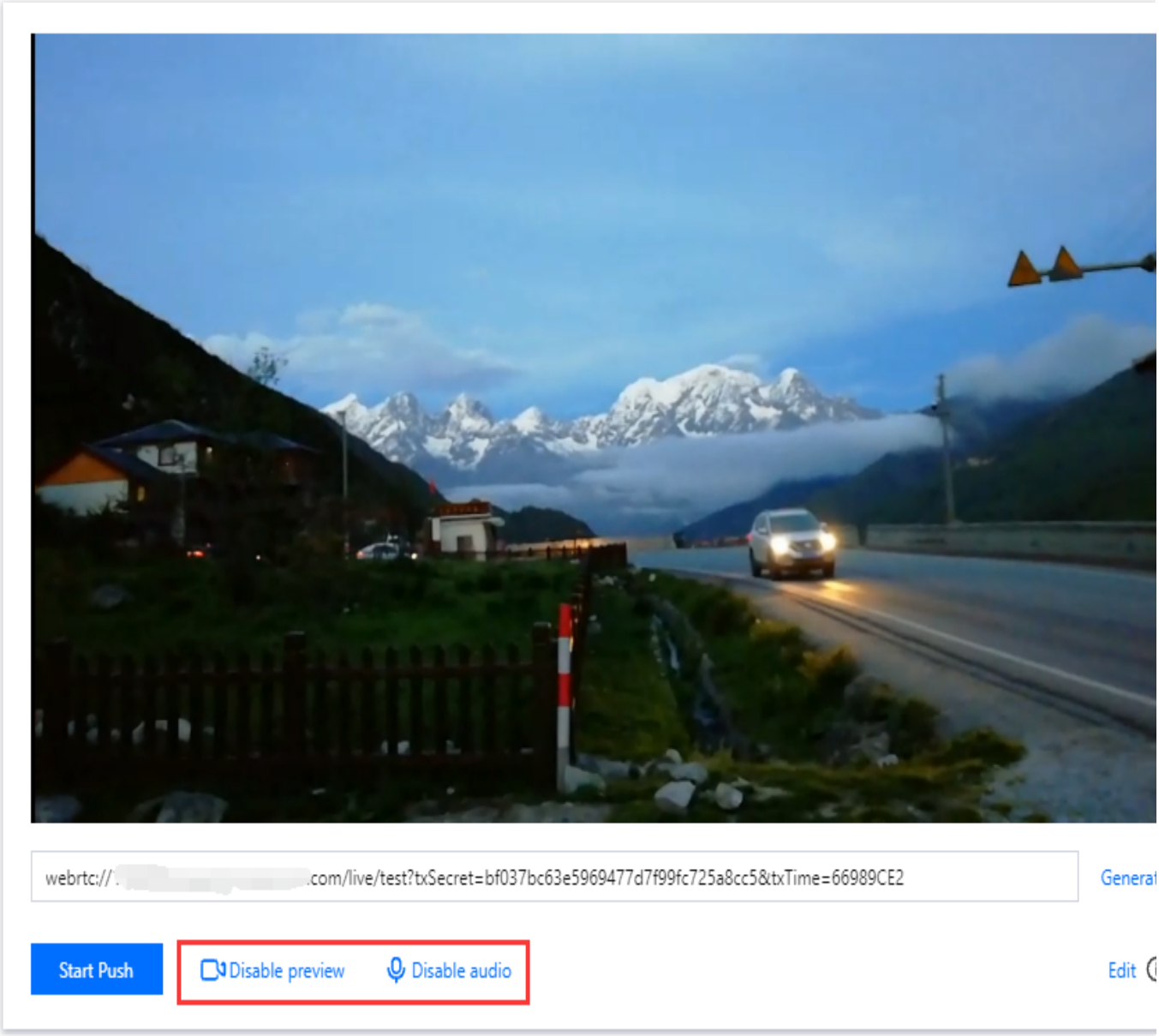
1.1 click



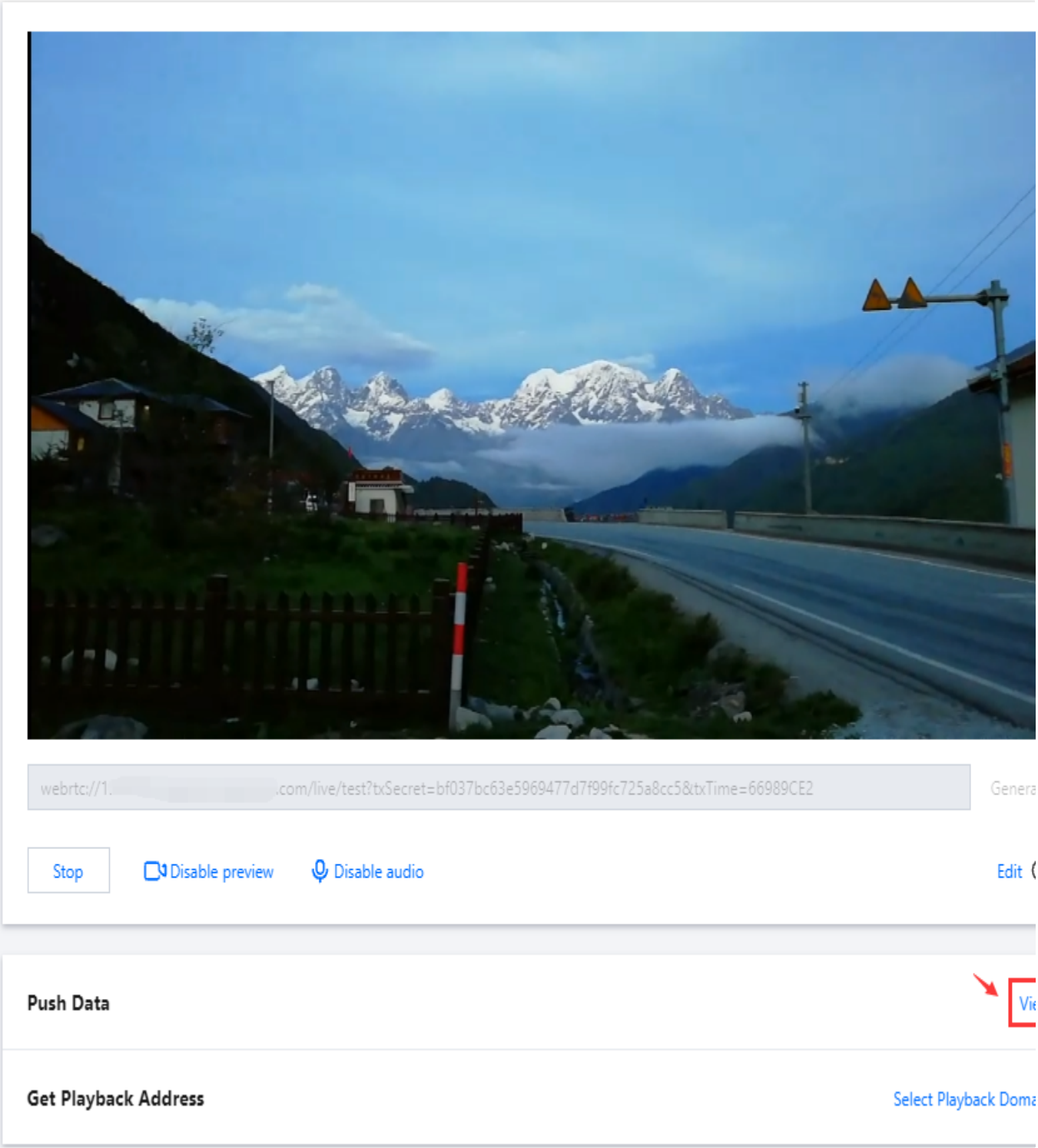
or



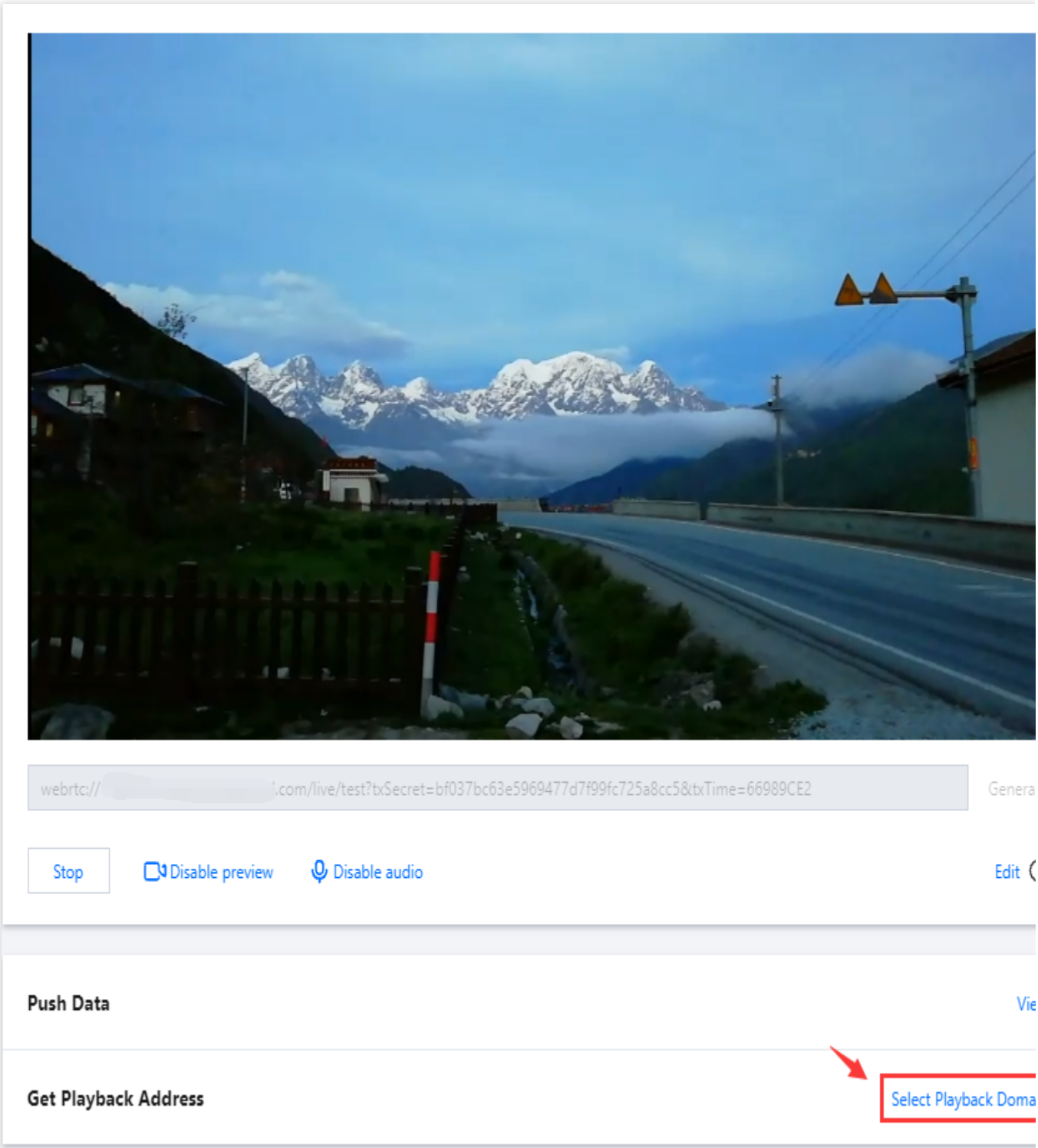
. After you disable video/audio, data capturing will continue and push will still succeed, but the stream cannot be previewed and will have no video or audio.

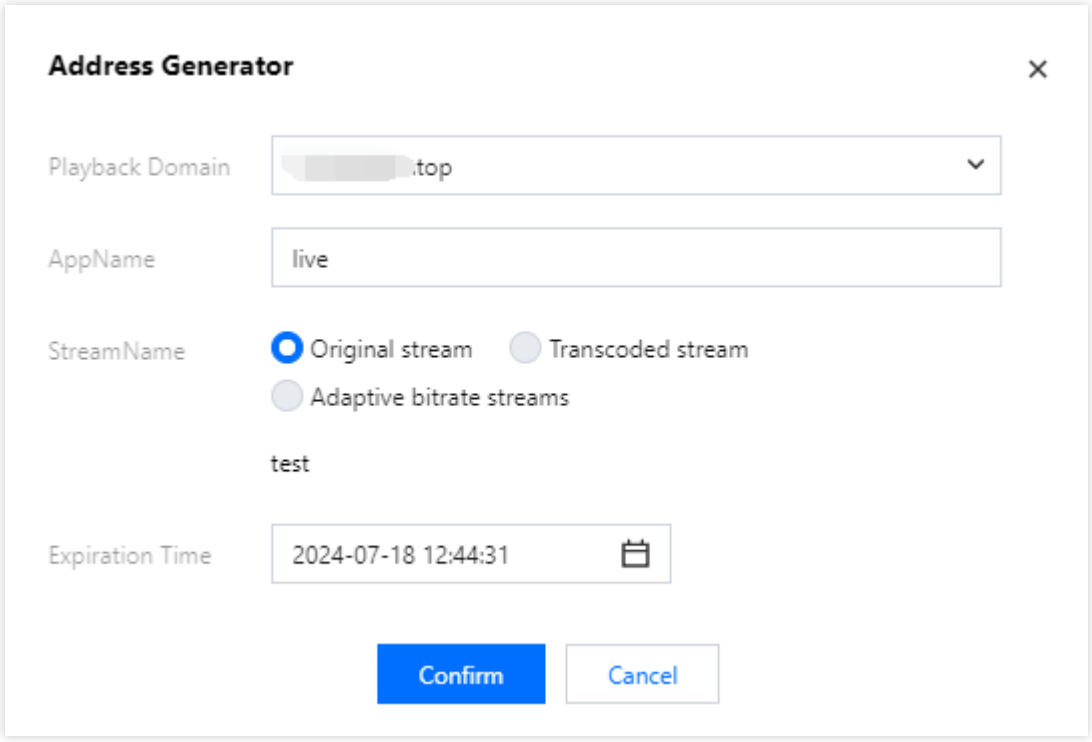


1.2 After push succeeds, click **View** below the preview to view streaming statistics. You cannot obtain statistics or playback URLs for push URLs not under your account. Please use a push domain under your account to generate push URLs or relay streams to your account.

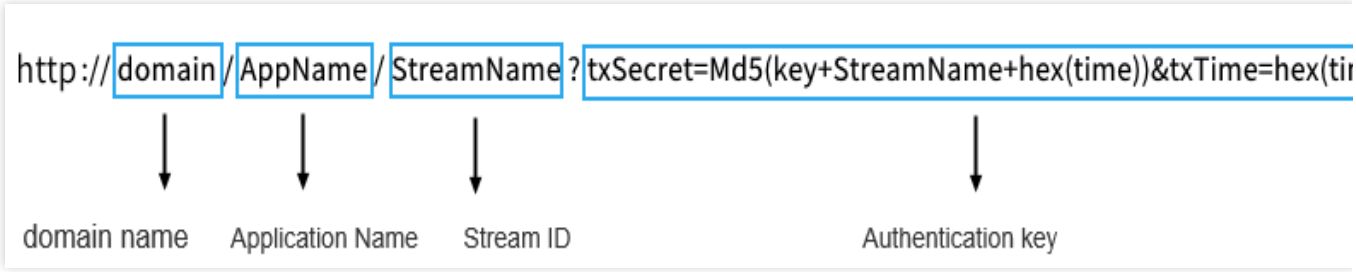


1.3 If you have added a playback domain in **Domain Management**, you can **select the domain** to generate a playback URL. If you need to generate a playback address with transcoding or adaptive transcoding configuration, you must first bind the playback domain to a transcoding template or adaptive transcoding template to generate a transcoded stream or adaptive transcoded stream.

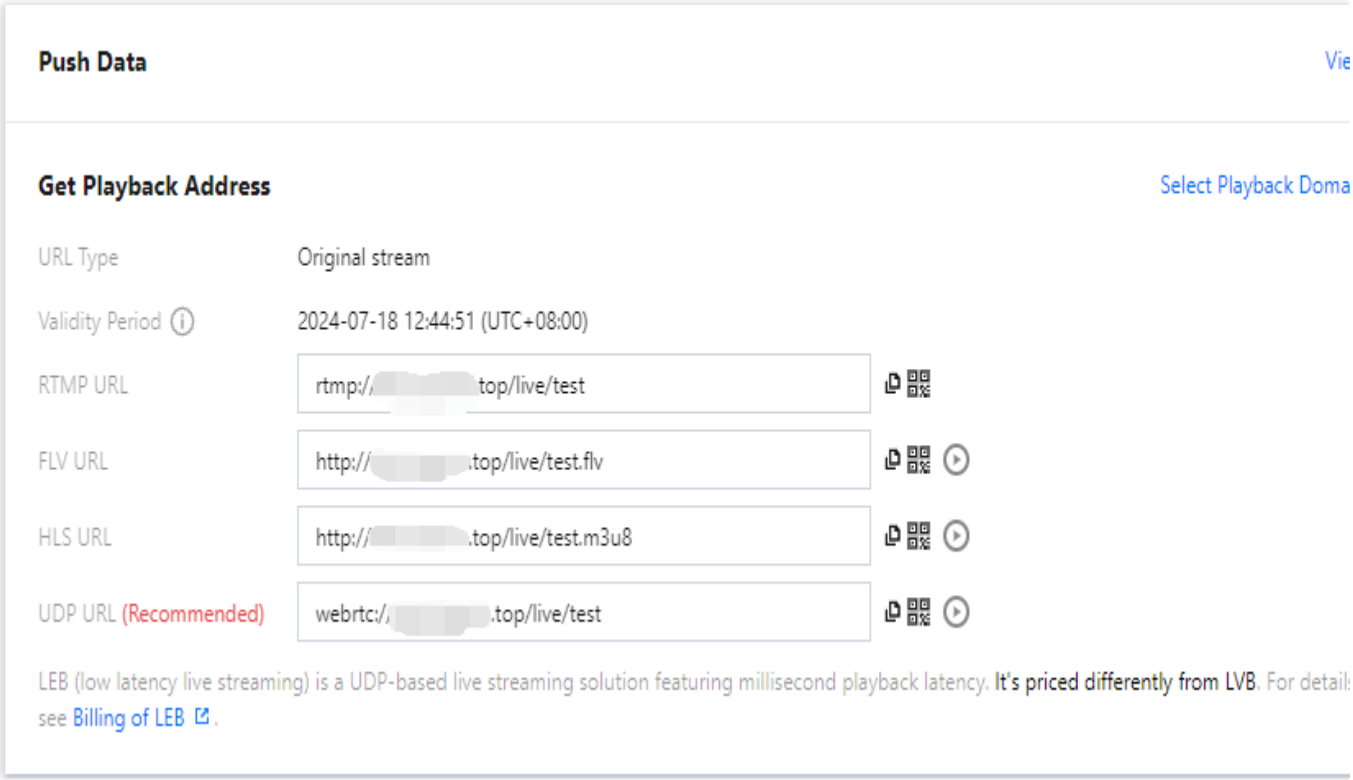

webrtc://
.com/live/test?txSecret=bf037bc63e5969477d7f99fc725a8cc5&txTime=66989CE2
Genera
Stop
Disable preview
Disable audio
Edit
Push Data
Vie
Get Playback Address
Select Playback Doma



A playback URL is made up of four parts, as shown below:



Supported protocols include RTMP, FLV, HLS, and UDP. You can also click the QR code icon and scan the QR code using the TCToolkit app to obtain the playback URL.



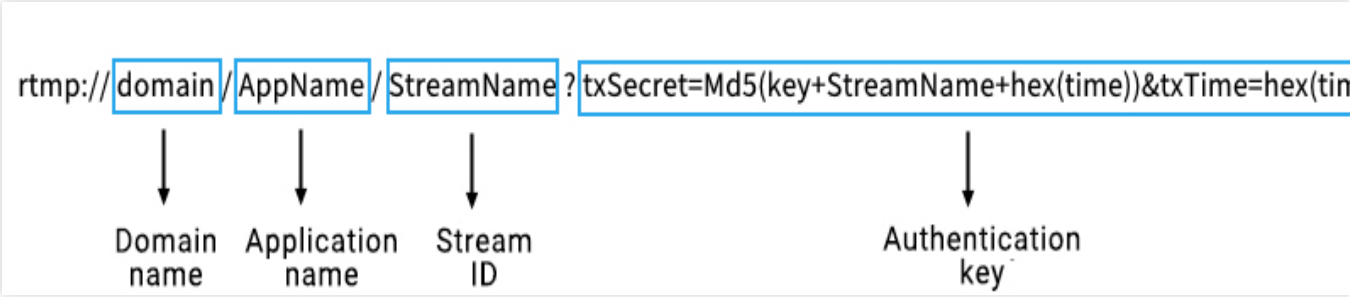
Note：

If HTTPS is enabled for the playback domain selected, the FLV and HLS URLs generated will start with https.

Address Generator

Last updated：2024-11-08 16:07:28

The CSS console provides an address generator which you can use to quickly generate push/playback URLs. The main parts of a live streaming URL include a domain name (`domain`), an application name (`AppName`), a stream name (`StreamName`) and an authentication key (`Key`).



After URLs are generated, you can **select and copy** the one you need or copy it by **clicking the copy icon**. You can also get the URL by **scanning the QR code**.

Support and Limits

If you need to generate multiple live streaming URLs, we recommend that you splice them as instructed in Splicing Live Streaming URLs.
CSS provides a test domain name `xxxx.livepush.myqcloud.com` . You can use it to test push, but we do not recommend using it for business purposes.
When playing a transcoded stream, the StreamName in the playback address should be suffixed with "_TranscodingTemplateName" to work. It is recommended not to include "_" in the StreamName. If the string after "_" is the same as the transcoding template name, the part after "_" will be recognized as the transcoding template name, which may cause the stream pulling to fail.
You can get a URL generated by scanning the QR code with TCToolkit .
The recent records of the address generator are stored in the local cache of a browser. Clearing the cache will also remove these records..

Prerequisites

You have logged in to the CSS console, and have added a push/playback domain name.

Parameter Description

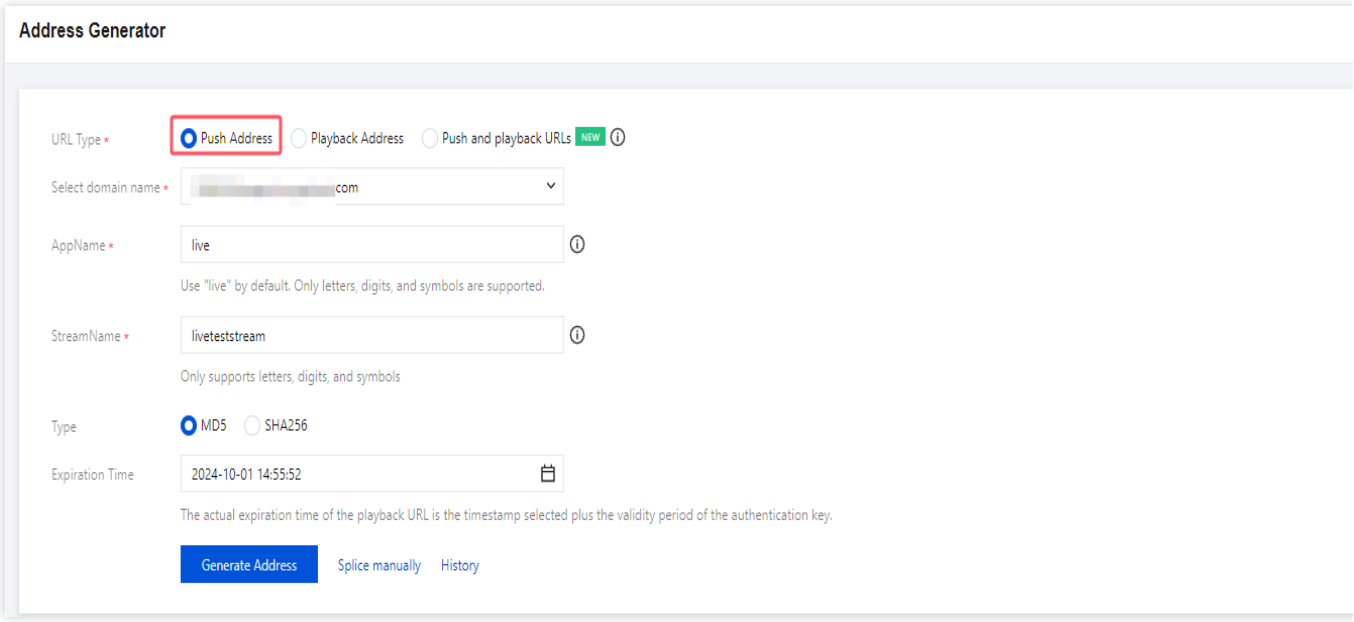
Parameter	Description
URL Type	You can choose from the following three address types for configuration: Push Address Playback Address Push and playback URLs
Select Domain Name	You can choose: Push Domain Name Playback Domain Name Select both Push Domain Name and Playback Domain Name
AppName	The application name, which is used to identify a streaming file path. Default value: `live`.Only letters, digits, and symbols are allowed.
StreamName	A custom stream name is a unique identifier for each live stream. It only supports English letters, numbers, and symbols. The length of the StreamName is limited to 255 characters.
Type	Default encryption type: MD5, alternative option: SHA256
Expiration Time	The actual expiration time of a playback URL is the specified time plus the validity period of the authentication key. The expiration time of a push URL is the specified time.
Transcoding Template	This option is only used when selecting the address type as Playback Address and choosing the domain name as Playback Domain Name. If you choose a Transcoding Template, the generated playback address will be for the transcoded live stream. If you need to play the original live stream, there is no need to select a transcoding template to generate the address. If you choose an Adaptive Bitrate Template, the generated playback address will be for the adaptive bitrate live stream. If you need to play the original live stream, there is no need to select a transcoding template to generate the address.

Generating Push URLs

Directions

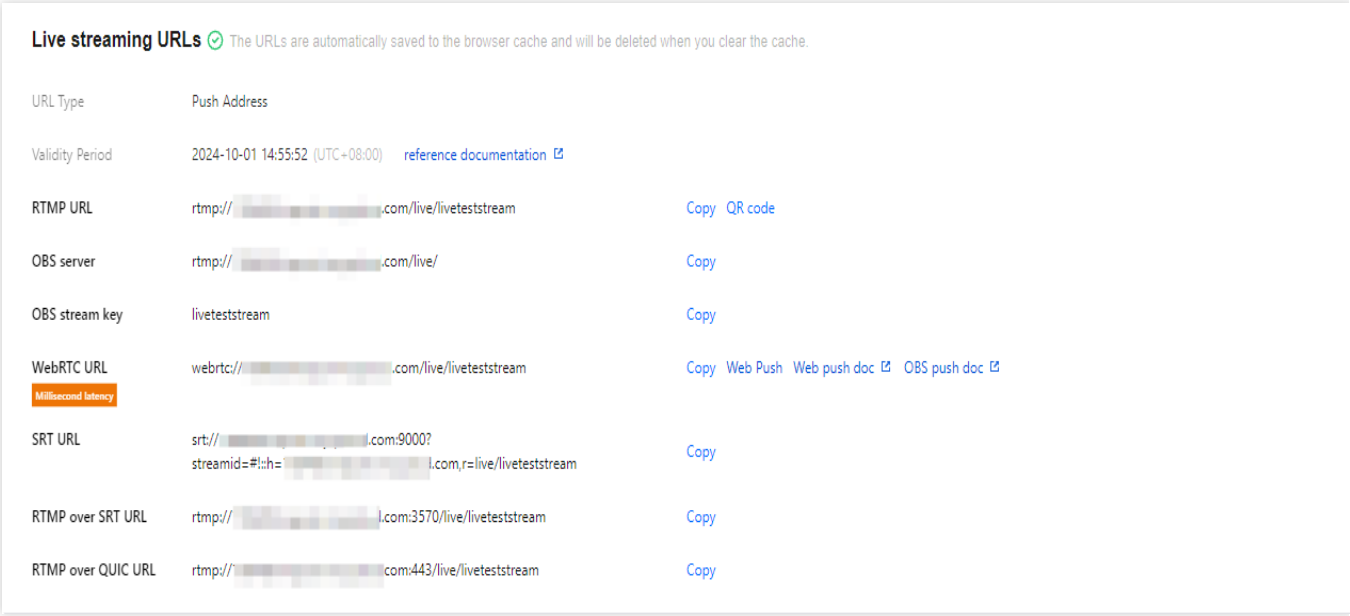
1. Log in to the CSS console and select Address Generator on the left sidebar.
2. Select the address type as **Push Address**.
3. Select the push domain name that you have added to Domain Management.

4. Enter an **AppName**. It is `live` by default.
5. Enter a **StreamName**, such as `liveteststream` .
6. Select your **Encryption Type**.
7. Select the expiration time of the URL, such as `2024-10-01 14:55:52` .
8. Click **Generate Address**.



Push URL format

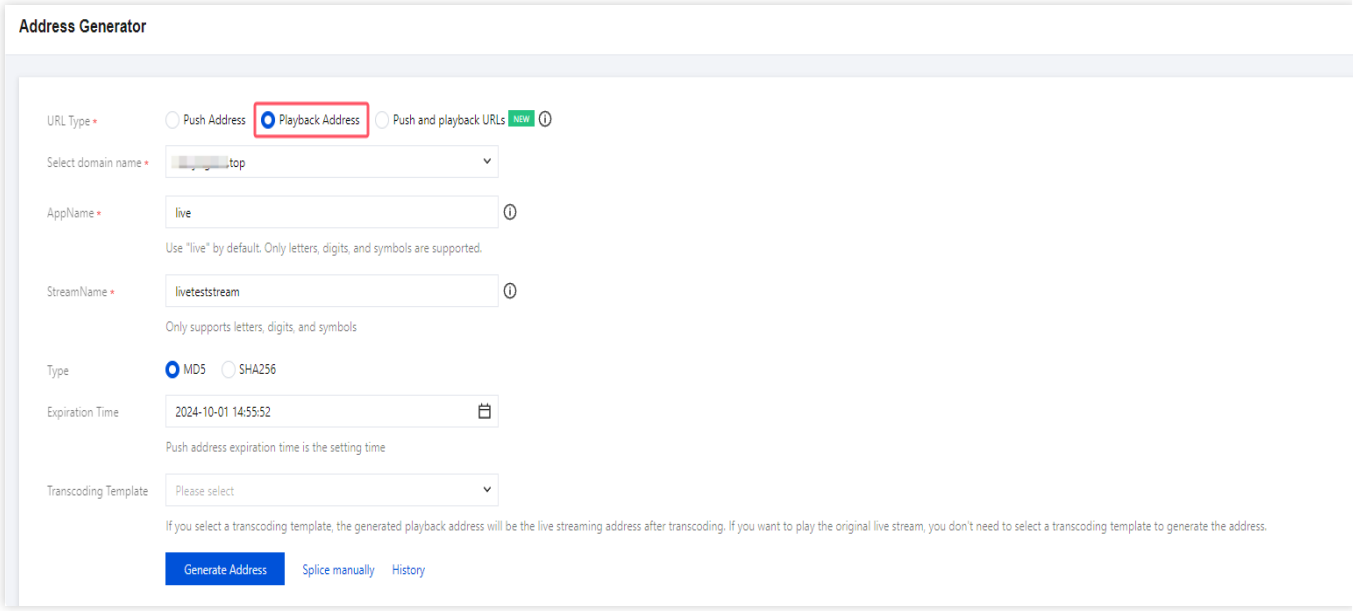
CSS supports RTMP, WebRTC, SRT, RTMP over SRT and RTMP over QUIC for push. As a result, the push URLs generated will start with `rtmp://` , `webrtc://` , `srt://` or `rtmp://` .



Generating Playback URLs

Directions

1. Log in to the CSS console and select Address Generator on the left sidebar.
2. Select the address type as **Playback Address** and choose the playback domain name that you have added to Domain Management.
3. Enter an **AppName**. It is `live` by default.
4. Enter a **StreamName**, such as `liveteststream` .
5. Select your **Encryption Type**.
6. Select the URL expiration time, such as `2024-10-01 14:55:52` .
7. Select an existing transcoding template (optional).
8. Click **Generate Address**.

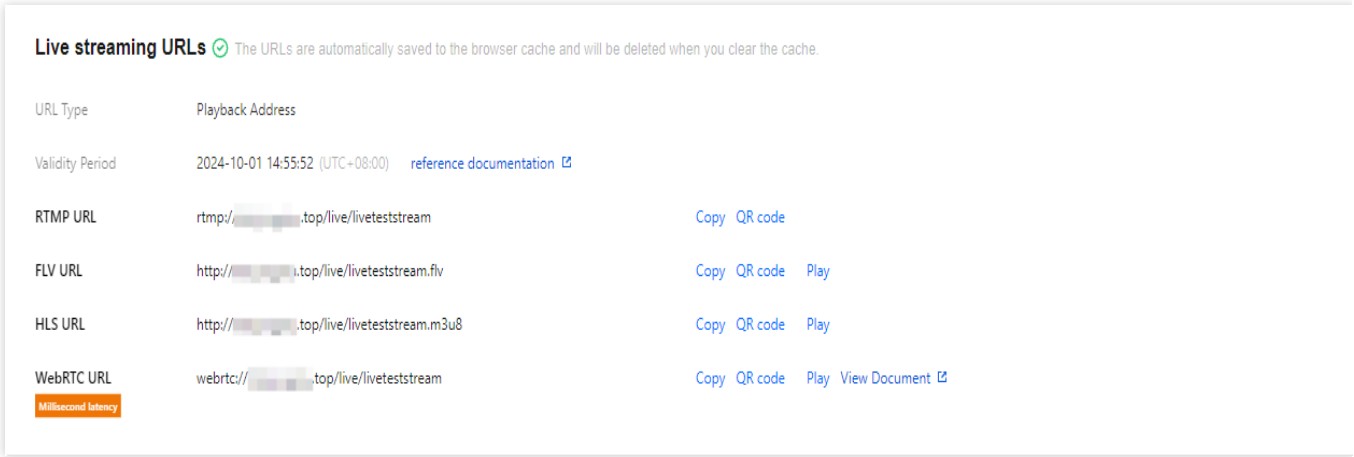


Playback URL format

If a transcoding template is used, the generated playback address will be for the transcoded live stream. The playback supports RTMP, FLV, HLS, and WebRTC protocols. You can generate playback addresses with prefixes such as `rtmp://`, `http://`, and `webrtc://` using the address generator. Compared to the original live stream, you need to append "_TranscodingTemplateName" after the StreamName.

Note:

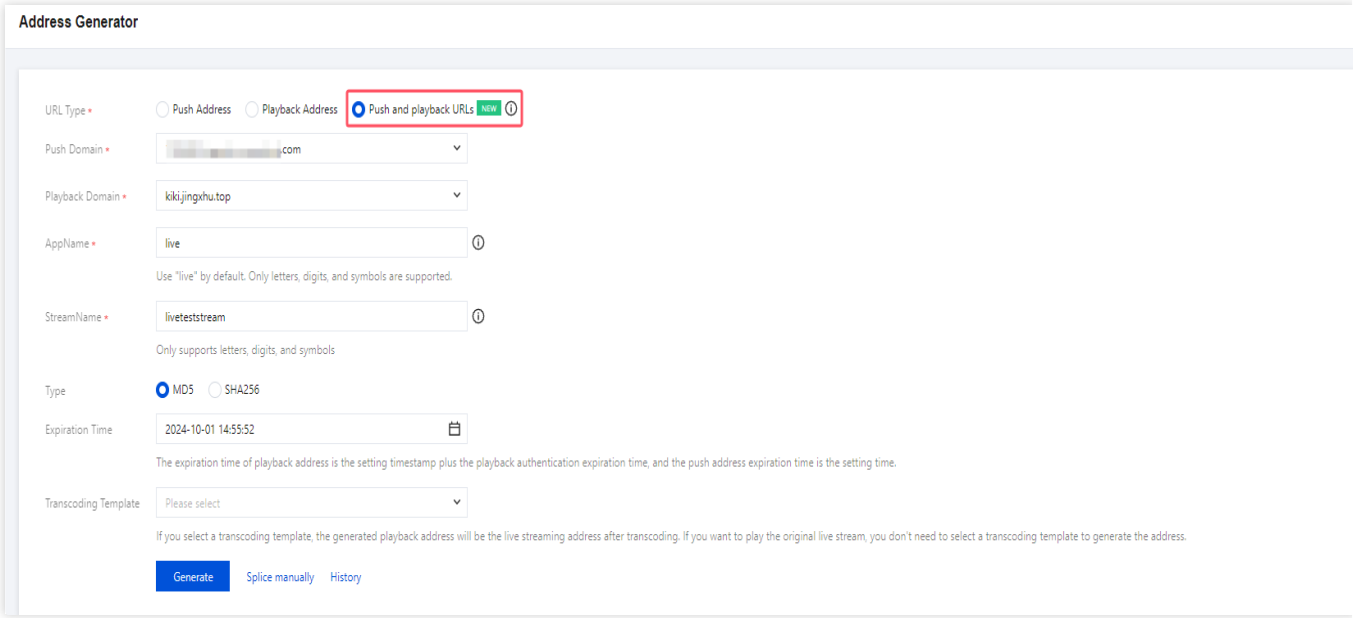
UDP playback URLs are for LEB. To learn about the billing of LEB, see Billing Overview.



Generate Push and Playback Address Group

Directions

1. Log in to the CSS console and select Address Generator on the left sidebar.
2. Select the address type as **Push and playback URLs**.
3. Select the **Push Domain Name** and **Playback Domain Name** that you have added to Domain Management.
4. Enter an **AppName**. It is `live` by default.
5. Enter a StreamName, such as `liveteststream`.
6. Select your **Encryption Type**.
7. Select the URL expiration time, such as `2024-10-01 14:55:52`.
8. Select an existing transcoding template (optional).
9. Click **Generate Address**.

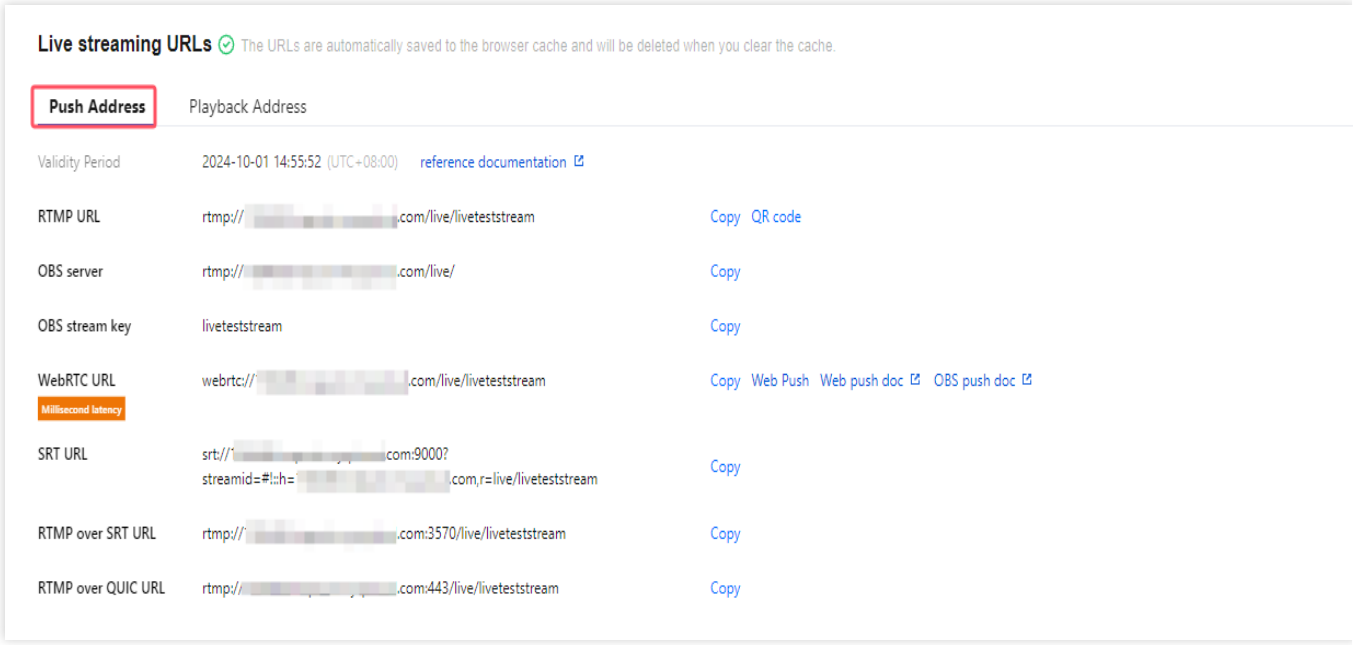


Push and Playback Address Group Explanation

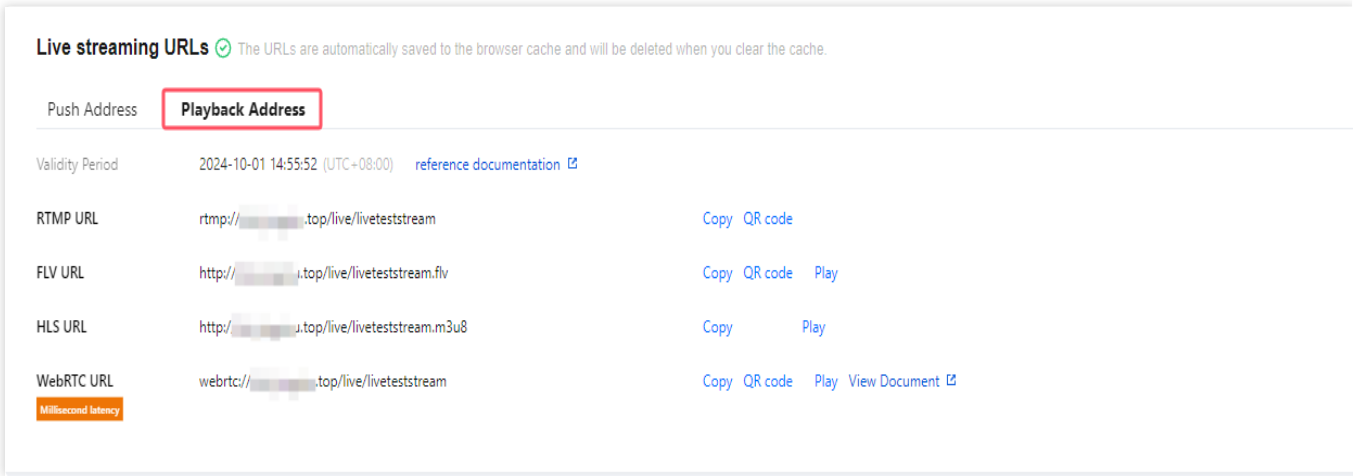
Push Address

Playback Address

CSS supports RTMP, WebRTC, SRT , RTMP over SRT and RTMP over QUIC for push. As a result, the push URLs generated will start with `rtmp://` , `webrtc://` , `srt://` or `rtmp://` .



IIf a transcoding template is used, the generated playback address will be for the transcoded live stream. The playback supports RTMP, FLV, HLS, and WebRTC protocols. You can generate playback addresses with prefixes such as `rtmp://` , `http://` , and `webrtc://` using the address generator. Compared to the original live stream, you need to append "_TranscodingTemplateName" after the StreamName.



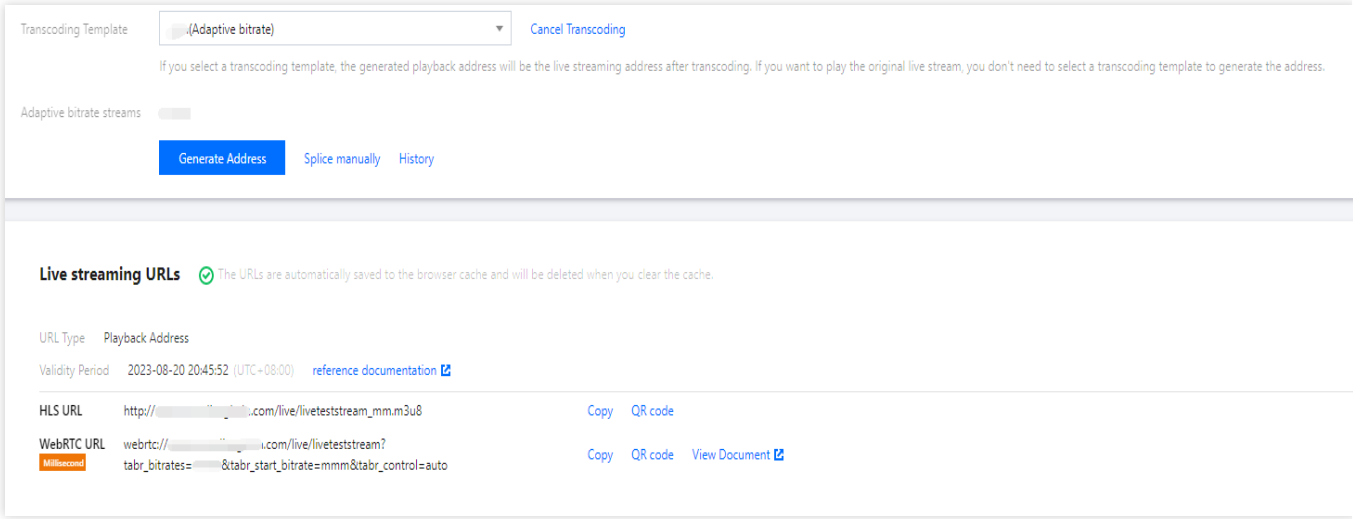
Adaptive bitrate URL format

If you use an Adaptive Bitrate Template, the generated playback address will be for adaptive bitrate playback.

This playback address supports HLS and WebRTC protocols. You can generate playback addresses with prefixes such as `http://` and `webrtc://` using the address generator.

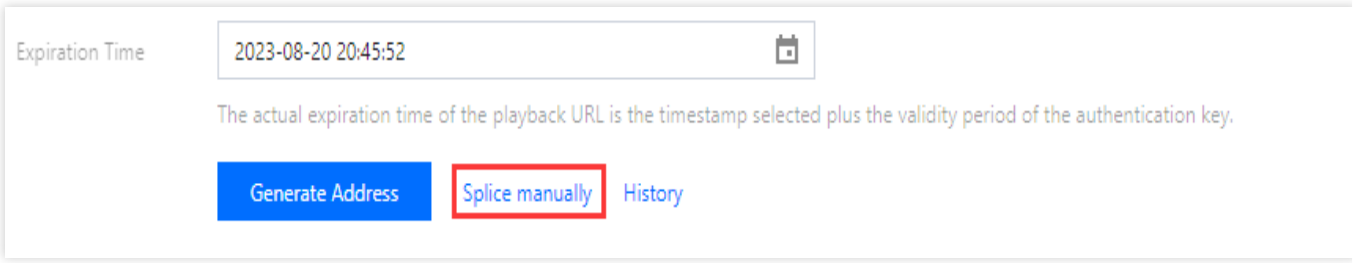
For adaptive bitrate pull addresses using the HLS protocol, the processing method is the same as that for regular transcoded addresses.

For adaptive bitrate pull addresses using the WebRTC protocol, there is no need to append the transcoding template name after the StreamName. Instead, you need to append `"&tabr_bitrates=AdaptiveBitrateSubTemplateNameList&tabr_start_bitrate=StartingPlaybackBitrateSubTemplateName&tabr_control=auto" after the original live stream URL`. The adaptive bitrate sub-template names in the list should be arranged in descending order of bitrate, separated by commas..



Custom Concatenation Explanation

1. Log in to the CSS console and select Address Generator on the left sidebar.Click **Splice manually** to enter theCustom Concatenation Management page.



2. In the pop-up **Address Resolution Sample** window, the examples are as follows:

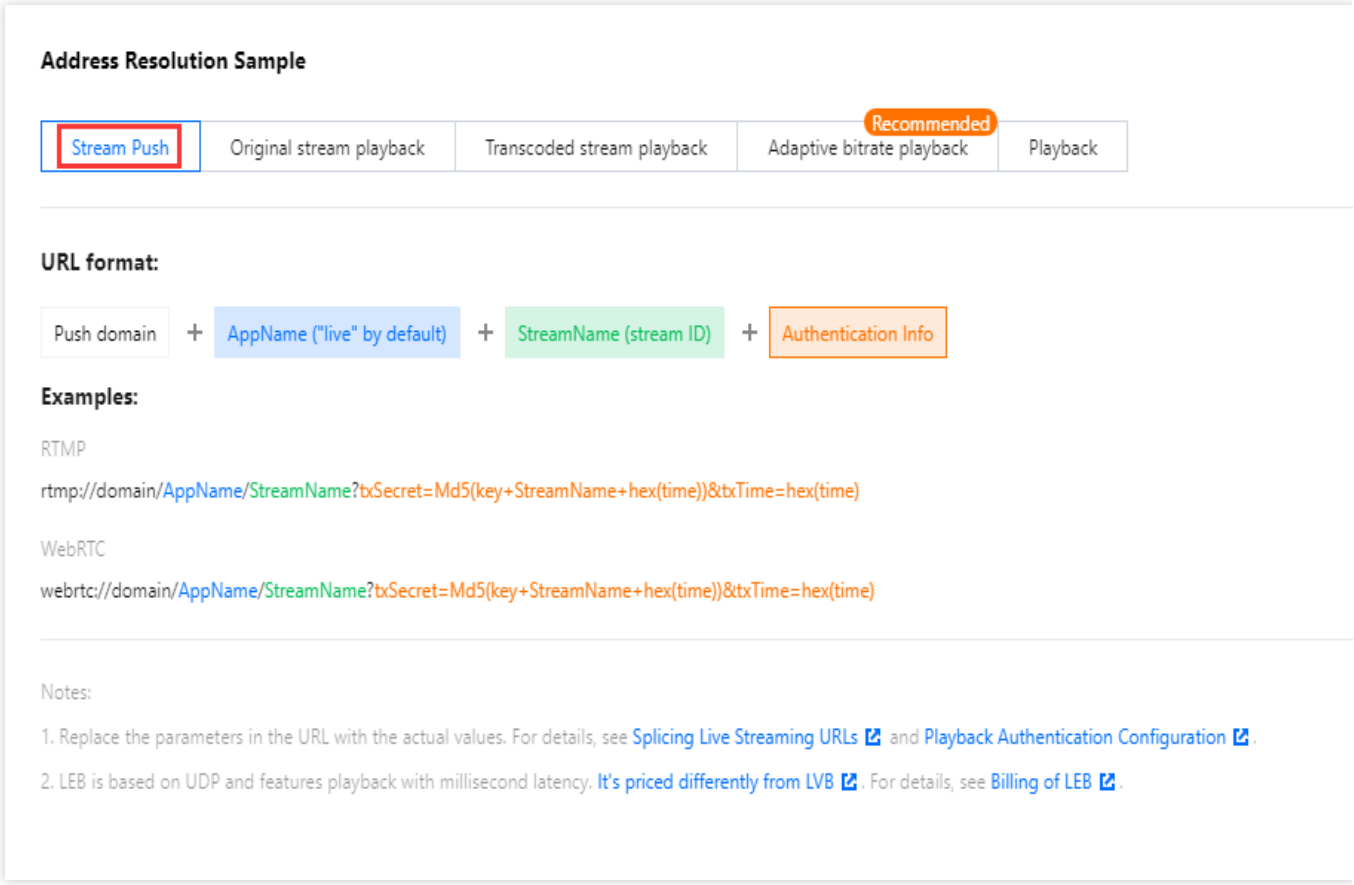
Stream Push

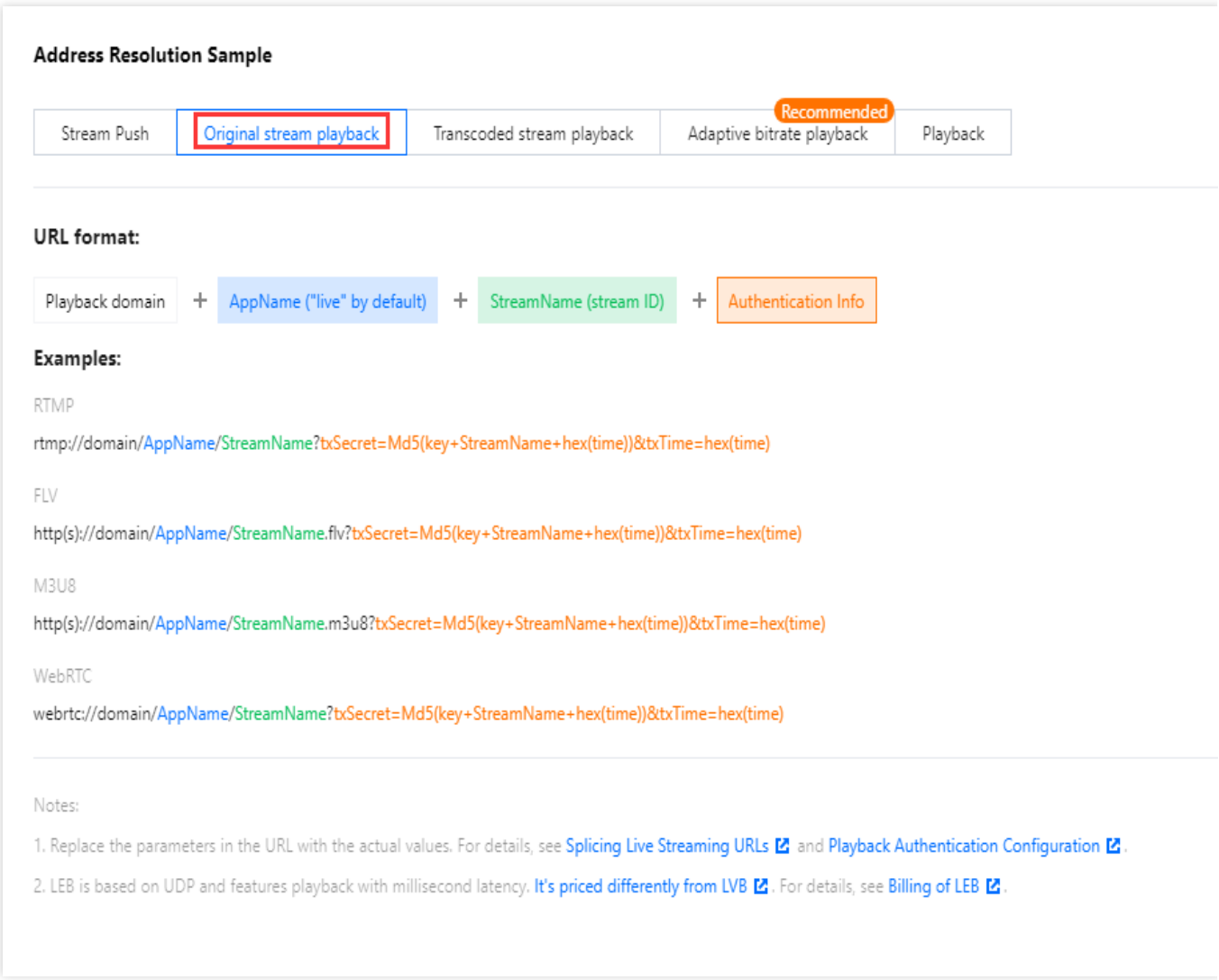
Original stream playback

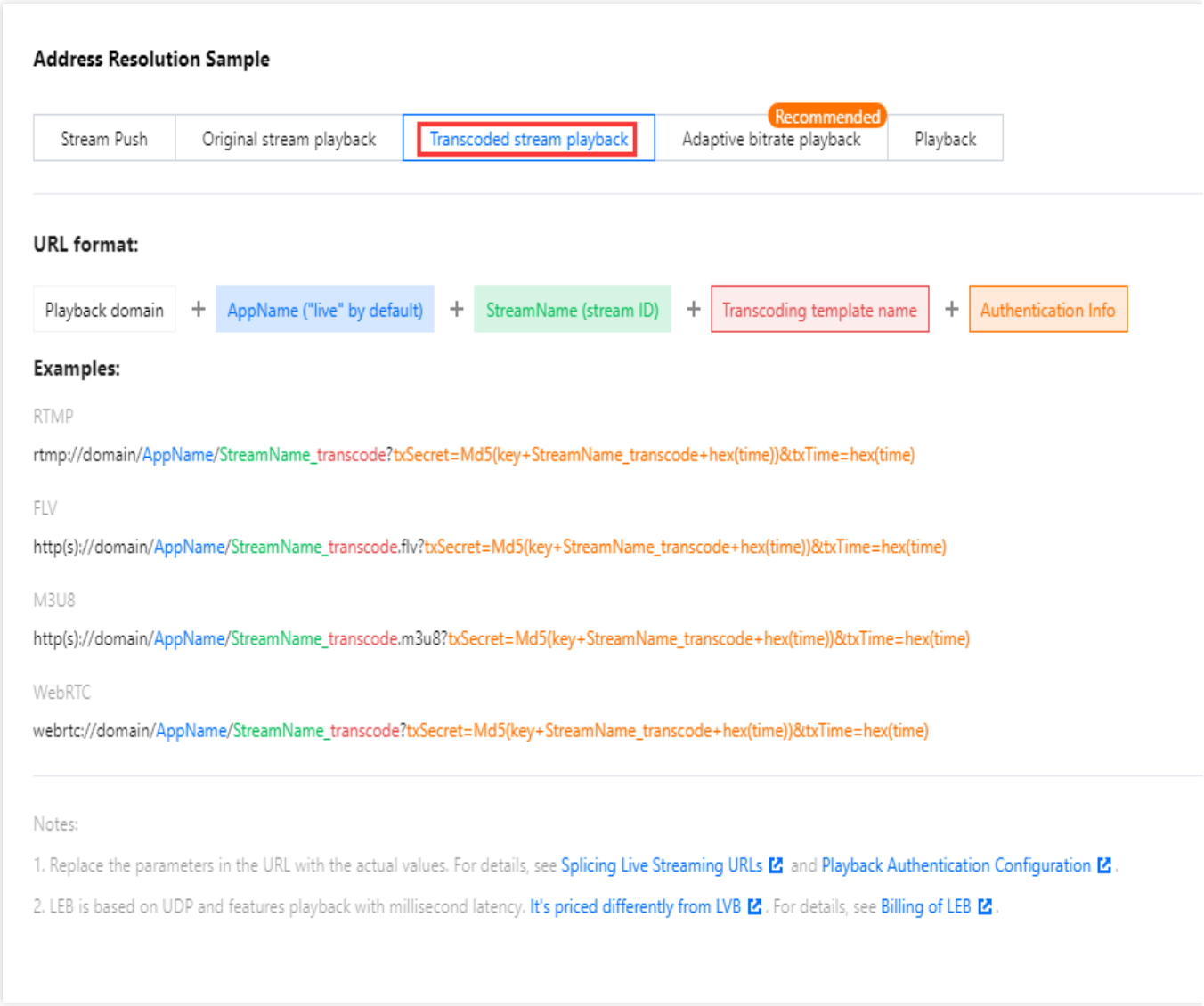
Transcoded stream playback

Adaptive bitrate playback

Playback


Address Resolution Sample
Stream Push
Original stream playback
Transcoded stream playback
Recommended
Adaptive bitrate playback
Playback
URL format:
Push domain
+
AppName ("live" by default)
+
StreamName (stream ID)
+
Authentication Info
Examples:
RTMP
rtmp://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)
WebRTC
webrtc://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)
Notes:
1. Replace the parameters in the URL with the actual values. For details, see Splicing Live Streaming URLs and Playback Authentication Configuration.
2. LEB is based on UDP and features playback with millisecond latency. It's priced differently from LVB. For details, see Billing of LEB.


Address Resolution Sample
Stream Push
Original stream playback
Transcoded stream playback
Recommended
Adaptive bitrate playback
Playback
URL format:
Playback domain
+
AppName ("live" by default)
+
StreamName (stream ID)
+
Authentication Info
Examples:
RTMP
rtmp://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)
FLV
http(s)://domain/AppName/StreamName.flv?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)
M3U8
http(s)://domain/AppName/StreamName.m3u8?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)
WebRTC
webrtc://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)
Notes:
1. Replace the parameters in the URL with the actual values. For details, see Splicing Live Streaming URLs and Playback Authentication Configuration.
2. LEB is based on UDP and features playback with millisecond latency. It's priced differently from LVB. For details, see Billing of LEB.


Address Resolution Sample
Stream Push
Original stream playback
Transcoded stream playback
Recommended
Adaptive bitrate playback
Playback
URL format:
Playback domain
+
AppName ("live" by default)
+
StreamName (stream ID)
+
Transcoding template name
+
Authentication Info
Examples:
RTMP
rtmp://domain/AppName/StreamName_transcode?txSecret=Md5(key+StreamName_transcode+hex(time))&txTime=hex(time)
FLV
http(s)://domain/AppName/StreamName_transcode.flv?txSecret=Md5(key+StreamName_transcode+hex(time))&txTime=hex(time)
M3U8
http(s)://domain/AppName/StreamName_transcode.m3u8?txSecret=Md5(key+StreamName_transcode+hex(time))&txTime=hex(time)
WebRTC
webrtc://domain/AppName/StreamName_transcode?txSecret=Md5(key+StreamName_transcode+hex(time))&txTime=hex(time)
Notes:
1. Replace the parameters in the URL with the actual values. For details, see Splicing Live Streaming URLs and Playback Authentication Configuration.
2. LEB is based on UDP and features playback with millisecond latency. It's priced differently from LVB. For details, see Billing of LEB.

Address Resolution Sample

Stream Push	Original stream playback	Transcoded stream playback	Adaptive bitrate playback (Recommended)	Playback

M3U8 URL format:

Playback domain + AppName ("live" by default) + StreamName (stream ID) + Adaptive bitrate template name + Authentication Info

Examples: Assume that your adaptive bitrate template is named "test".

URL

http(s)://domain/AppName/StreamName_test.m3u8?txSecret=Md5(key+StreamName_autobitrate+hex(time))&txTime=hex(time)

WebRTC URL format:

Playback domain + AppName ("live" by default) + StreamName (stream ID) + Authentication Info + Adaptive bitrate stream names + Name of the initially played stream + Bitrate control mode

Examples:

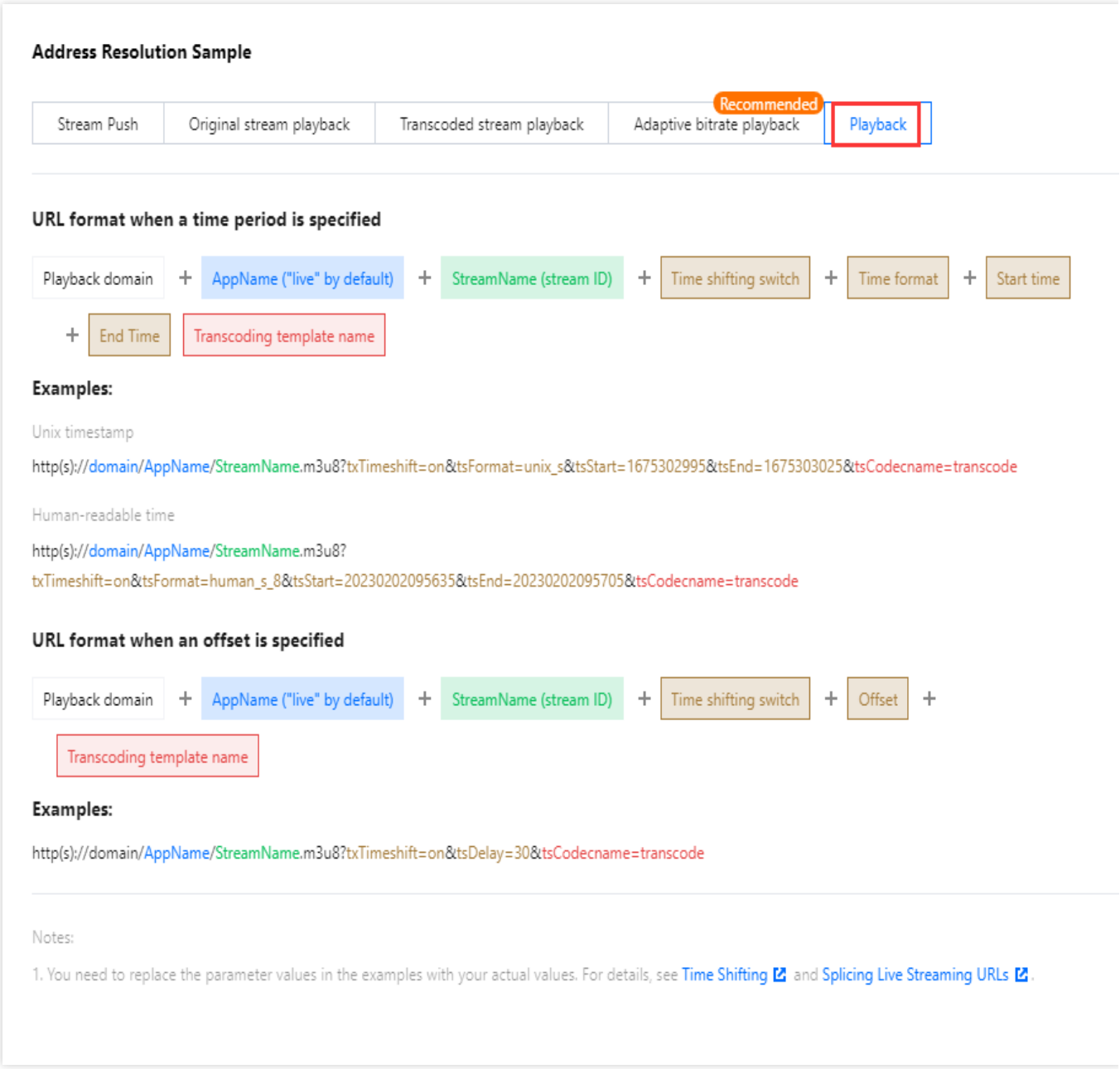
Assume that your adaptive bitrate template has three streams. Their names are "test 1", "test 2", and "test 3", and their bitrates are 200 Kbps, 300 Kbps, and 400 Kbps respectively.

URL

webrtc://domain/AppName/StreamName?txSecret=Md5(key+StreamName+hex(time))&txTime=hex(time)&tabr_bitrates=test3,test2,test1&tabr_start_bitrate=test1&tabr_control=auto

Notes:

1. Replace the parameters in the URL with the actual values. For details, see Splicing Live Streaming URLs and Playback Authentication Configuration.
2. LEB is based on UDP and features playback with millisecond latency. It's priced differently from LVB. For details, see Billing of LEB.

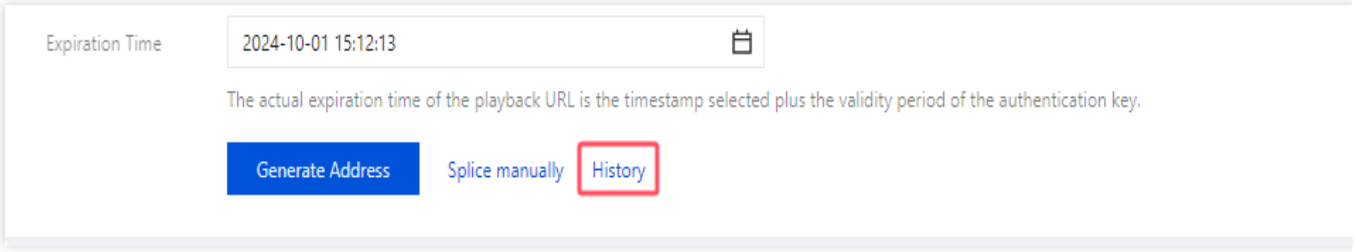


Recent Record Explanation

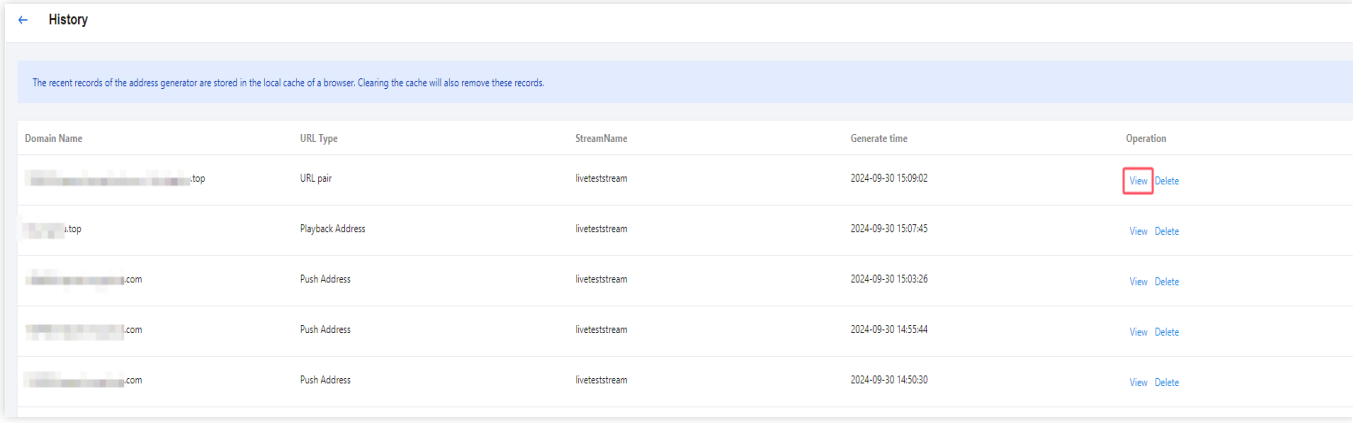
Based on your business needs, you can view or delete the records of recently generated addresses. These records include push addresses, playback addresses, address groups, and other information.

View Records

1. Log in to the CSS console and select Address Generator on the left sidebar.Click **History** to enter the Recent Record Management page.

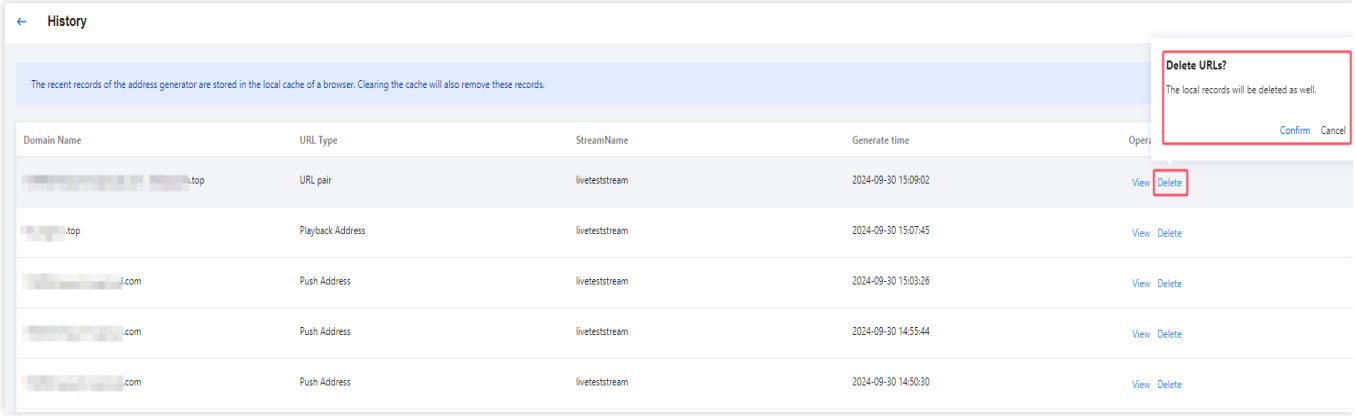


2. Select the live address record information you want to view and click **View**.



Delete Live Address Record

If you need to delete a live address record, first select the address type you want to delete, and then click **Delete** on the right side of the page. Next, you will be redirected to the delete confirmation window; click **Confirm** again to delete the corresponding live address record.



Note:

The URLs are automatically saved to the browser cache and will be deleted when you clear the cache


Live streaming URLs
The URLs are automatically saved to the browser cache and will be deleted when you clear the cache.

Self-Diagnosis

Last updated：2024-10-17 16:30:10

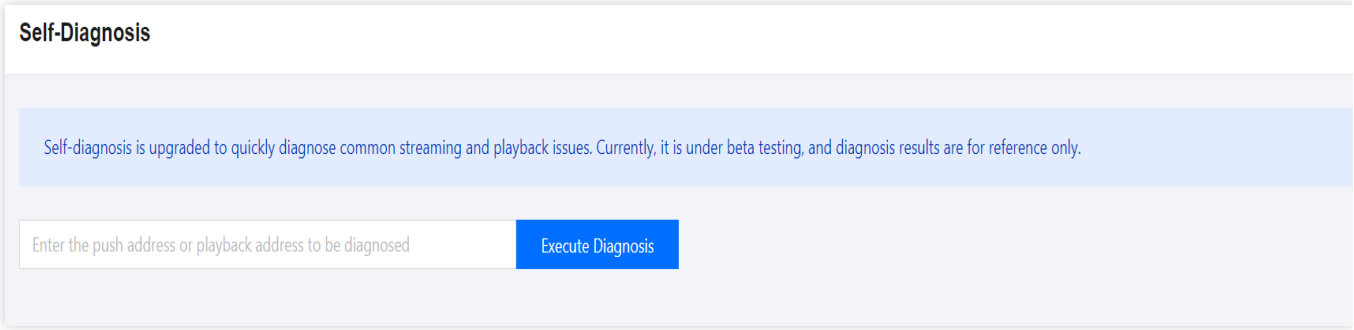
CSS offers a self-diagnosis tool for you to quickly detect and troubleshoot push and playback issues related to users, URLs, domain names, streams, and other factors. This feature is in beta testing now. The diagnostic results are for reference only.

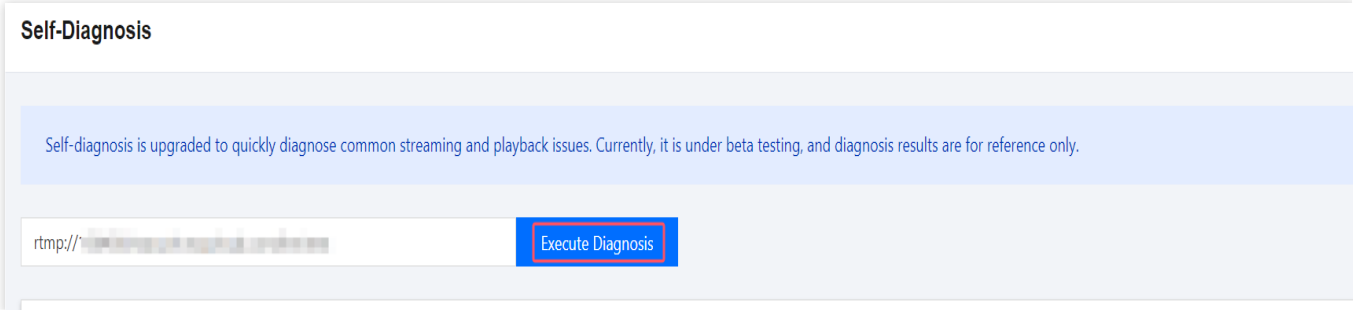
Prerequisites

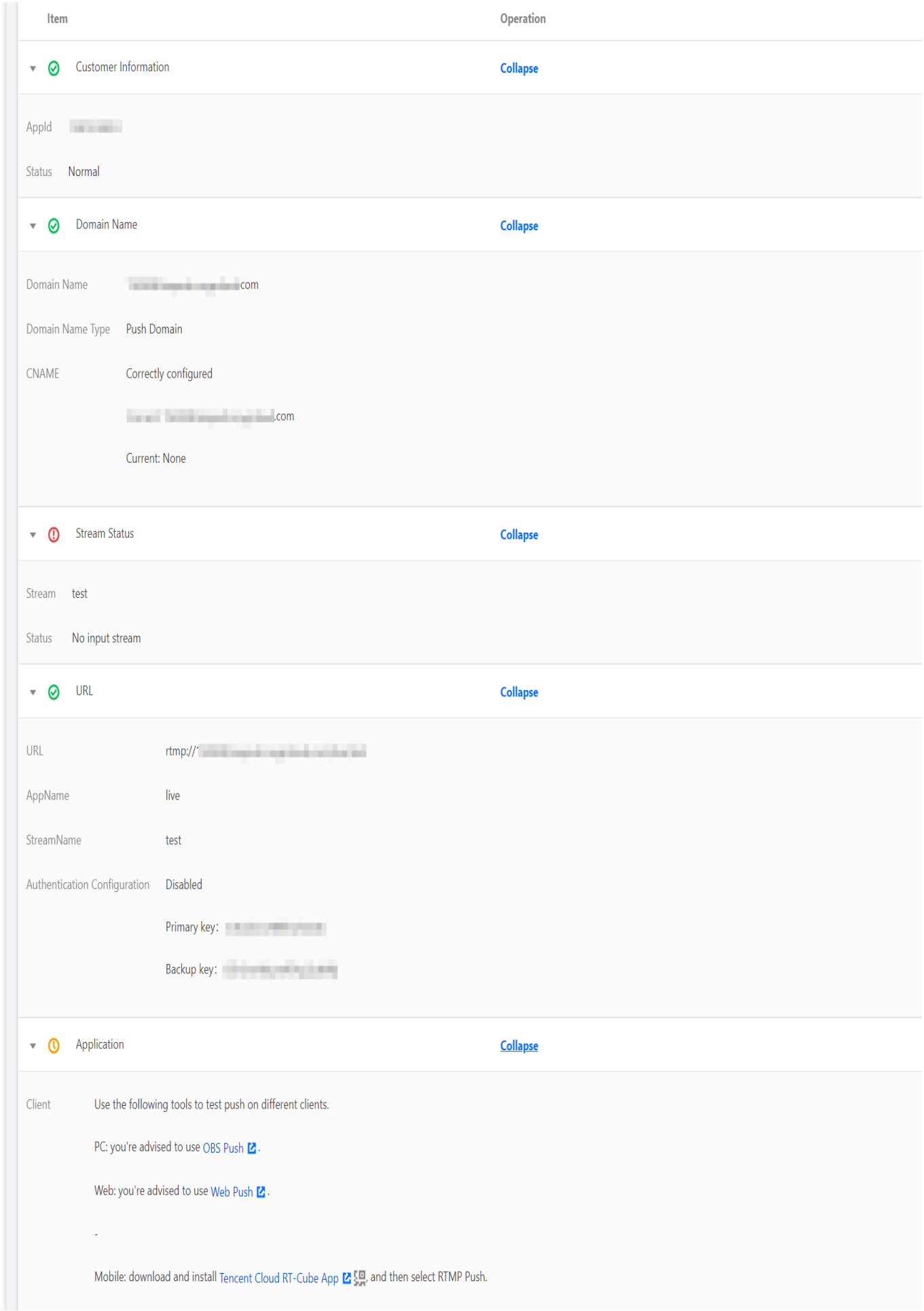
There is a push/playback URL spliced by you or generated by the Address Generator.
The push URL has been used for push.

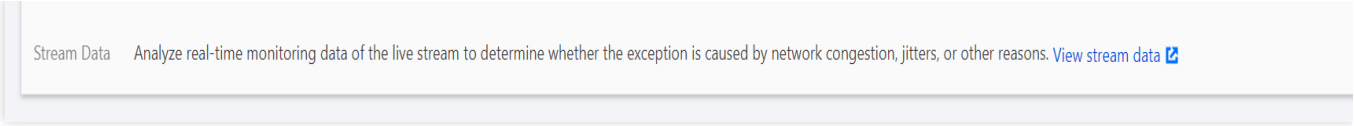
Directions

Follow the steps below to diagnose a push/playback problem in a live stream:
1. Log in to the CSS console and select **Tools** > Select Self-Diagnosis in the left column.
2. Enter the push or playback URL you want to diagnose.
3. Click **Execute Diagnosis**.






Item
Operation
Customer Information
Collapse
AppId
Status Normal
Domain Name
Collapse
Domain Name
Domain Name Type Push Domain
CNAME Correctly configured
Current: None
Stream Status
Collapse
Stream test
Status No input stream
URL
Collapse
URL rtmp://
AppName live
StreamName test
Authentication Configuration Disabled
Primary key:
Backup key:
Application
Collapse
Client Use the following tools to test push on different clients.
PC: you're advised to use OBS Push .
Web: you're advised to use Web Push .
-
Mobile: download and install Tencent Cloud RT-Cube App , and then select RTMP Push.



Result

You will see the diagnostic result and suggestion for troubleshooting the problem.

Item	Sub-Item	Description
Customer Information	APPID	Customer's application ID
	Status	Customer's account status
Domain Name	Domain Name	Domain Name
	Domain Name Type	Push/Playback domain
	CNAME	CNAME resolution information
Stream Status	Stream	Stream ID
	Status	Stream status
URL	URL	Push/Playback URL
	AppName	URL path
	StreamName	Stream name, which is used to calculate `txSecret`
	Authentication Configuration	Whether authentication is enabled
		Primary key
		Backup key
	Push/Playback authentication	Whether authentication succeeded
		Cause
		Authentication StreamName
		txSecret: Authentication string generated after push/playback authentication is enabled.
		txTime: Expiration timestamp set for the push/playback URL

		URL actual expiration time
Access Bandwidth	Bandwidth Cap Configuration	Whether a cap is set for bandwidth
		Acceleration Region
	IP Visit	Status
		Current Bandwidth
Application	Client	Push from PC: We recommend you use OBS for push to test the push. Playback on PC: We recommend you use the VLC player to test the playback.
		Push from web: We recommend you use Web Push to test the push.
		Push from mobile apps: Install TCToolkit App and select "RTMP for push" to test the push. Playback on mobile apps: Install TCToolkit App and select "Standard Live Broadcast" to test the playback.
	IP Restriction	Check for exceptions caused by the IP allowlist/blocklist or regional restrictions
	Stream Data	Analyze real-time monitoring data of the live stream to determine whether the exception is caused by network congestion, jitters, or other reasons. View stream data

Note:

If the diagnostic report cannot solve your problem, please submit a ticket or contact Tencent Cloud technical support.

OOTB live

Last updated：2024-04-24 11:49:03

OOTB live is aready-to-use tool that requires no intricate technical research or personnel investment.With only two simple steps, one can initiate personalized live streaming training or sales sessions. Utilizing this live streaming tool, you can effectively manage private traffic, operate your own brand, introduce and release company products, conduct promotion and training activities, and better track online training and sales results. This document principally outlines the operations for live room management on the enterprise management side, live stream push onthe host side, and live viewing on the viewer side.

Prerequisites

You have logged in to the CSS console.
You have added a playback domain name.

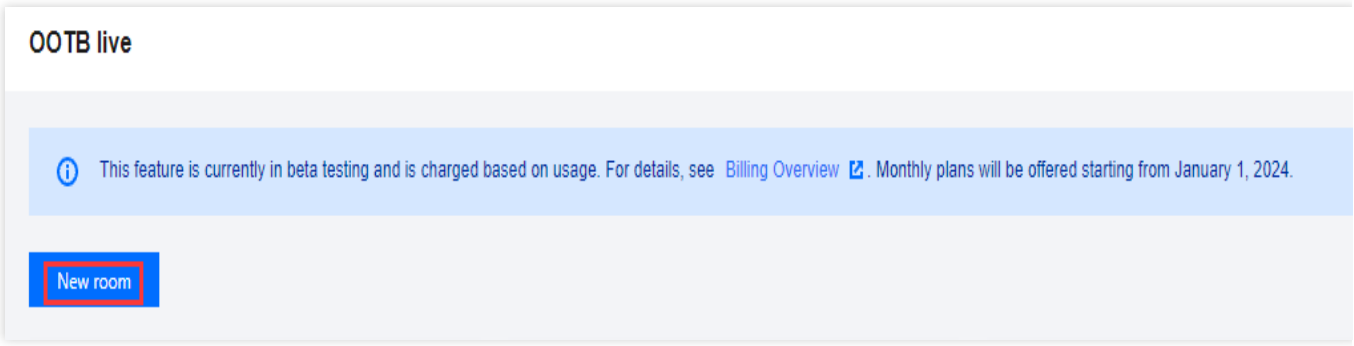
Points of Attention

Currently, this feature is in beta testing. Fees are collected based on the actual use of the function. For more details, refer to Pricing Overview. As of January 1,2024, billing will be based on monthly subscription plans.

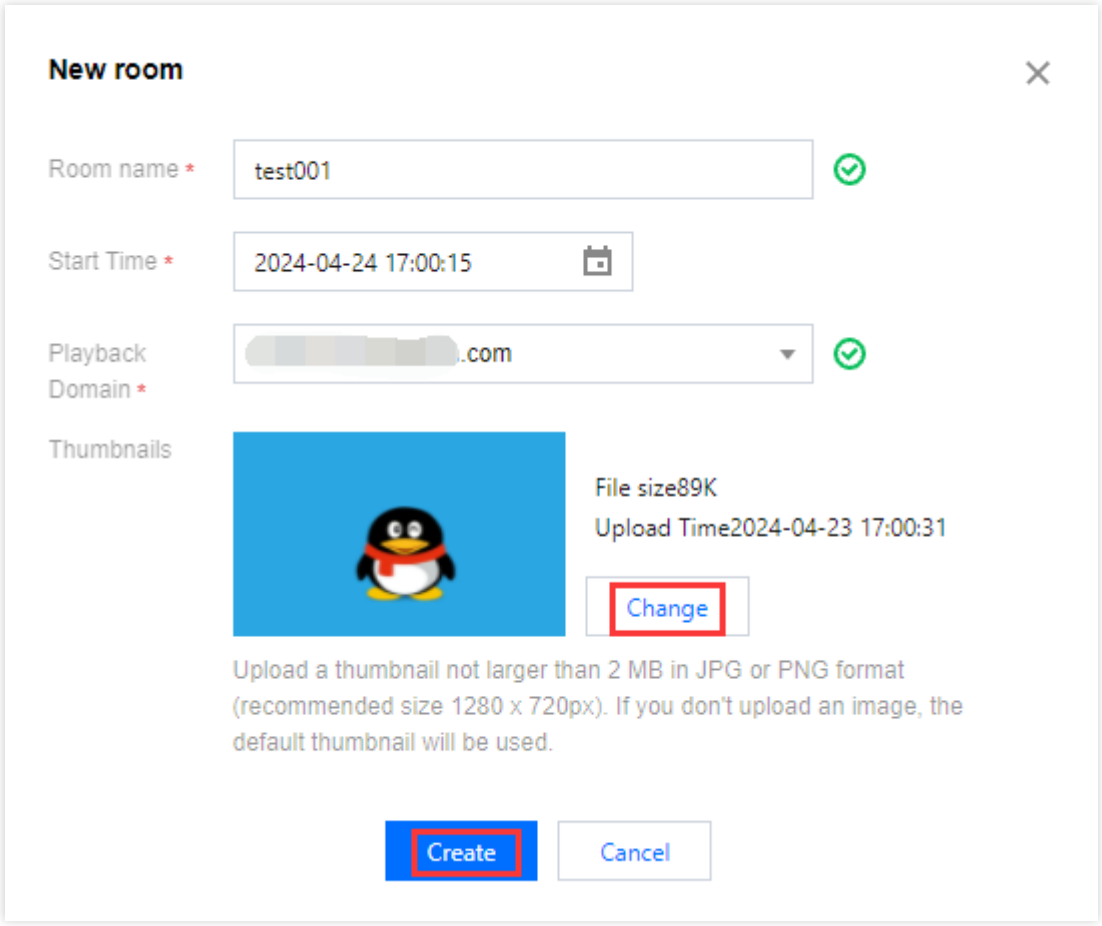
Live Room Management (Management Side)

Creating a Live Room

1. Log in to the CSS console, go to **CSS Toolkit** > OOTB live.
2. Click **New room** to enter the live room creation window.

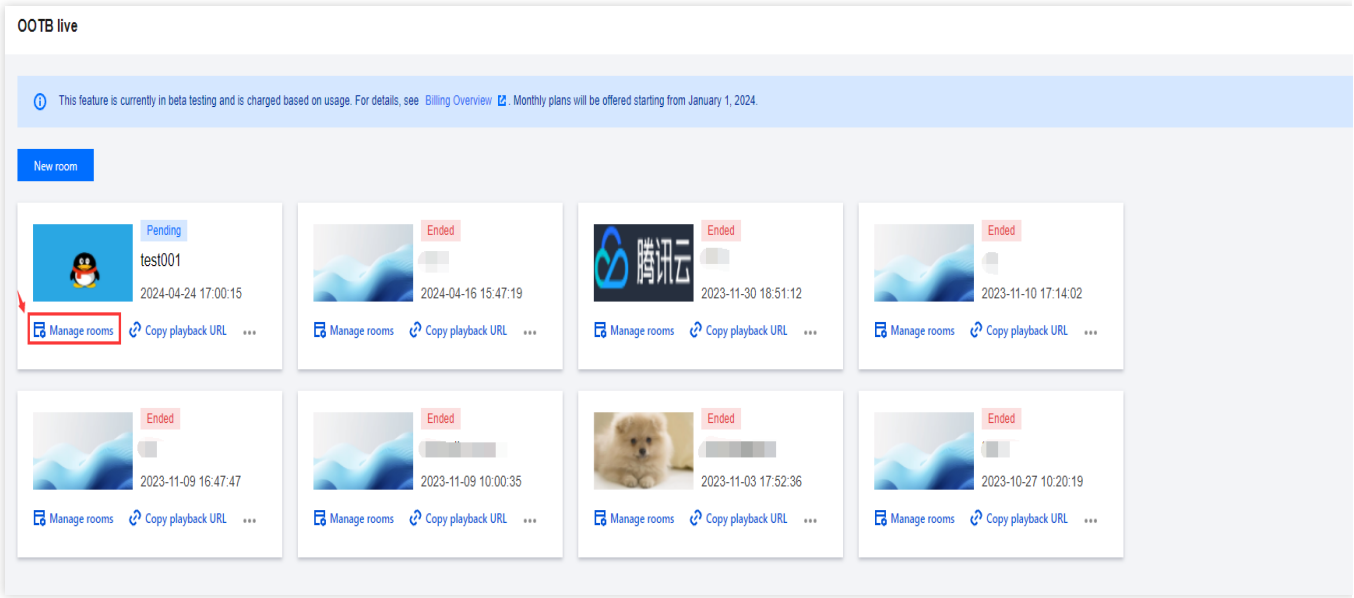


3. Specify **Room name**. The name can contain up to 20 characters and supports only Chinese characters, English letters, numbers, underscores (_), and hyphens (-).
4. Choose **Start Time** based on your actual business needs and click **OK** for confirmation.
5. Select **Playback Domain** that you have already added in the domain name management.
6. A default live streaming cover is provided. If you wish to upload your own cover, click on **Change**. We recommend a JPG or PNG image of 2 MB or smaller, with resolution of 1280*720px.
7. Click **Create.**



Live Control

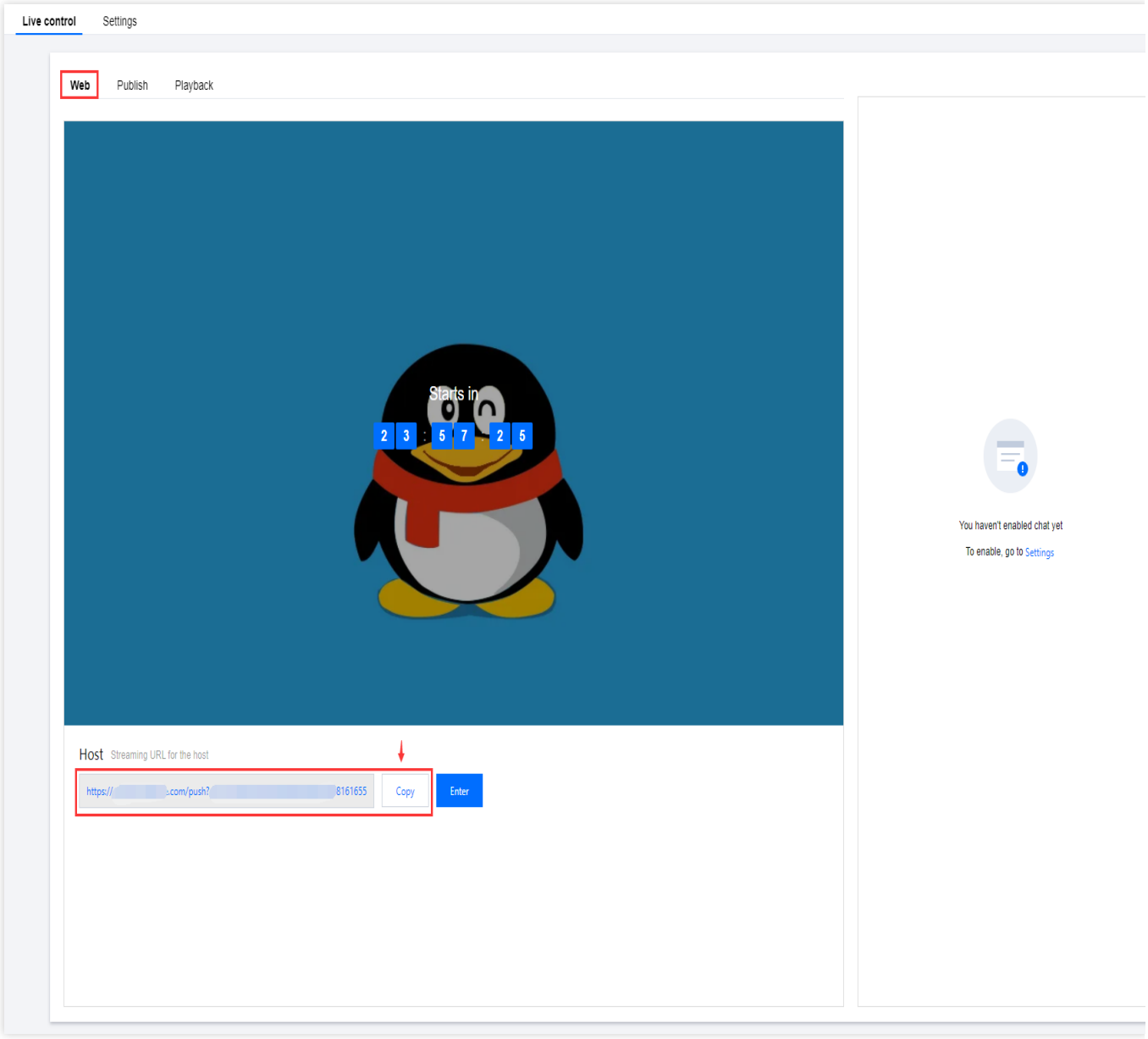
1. Log in to the CSS console, go to **CSS Toolkit** > OOTB live.
2. Select the created live room and click on **Manage rooms**. From the management side, you can delete created live rooms based on actual business needs, or copy and share links for viewing the live streaming.



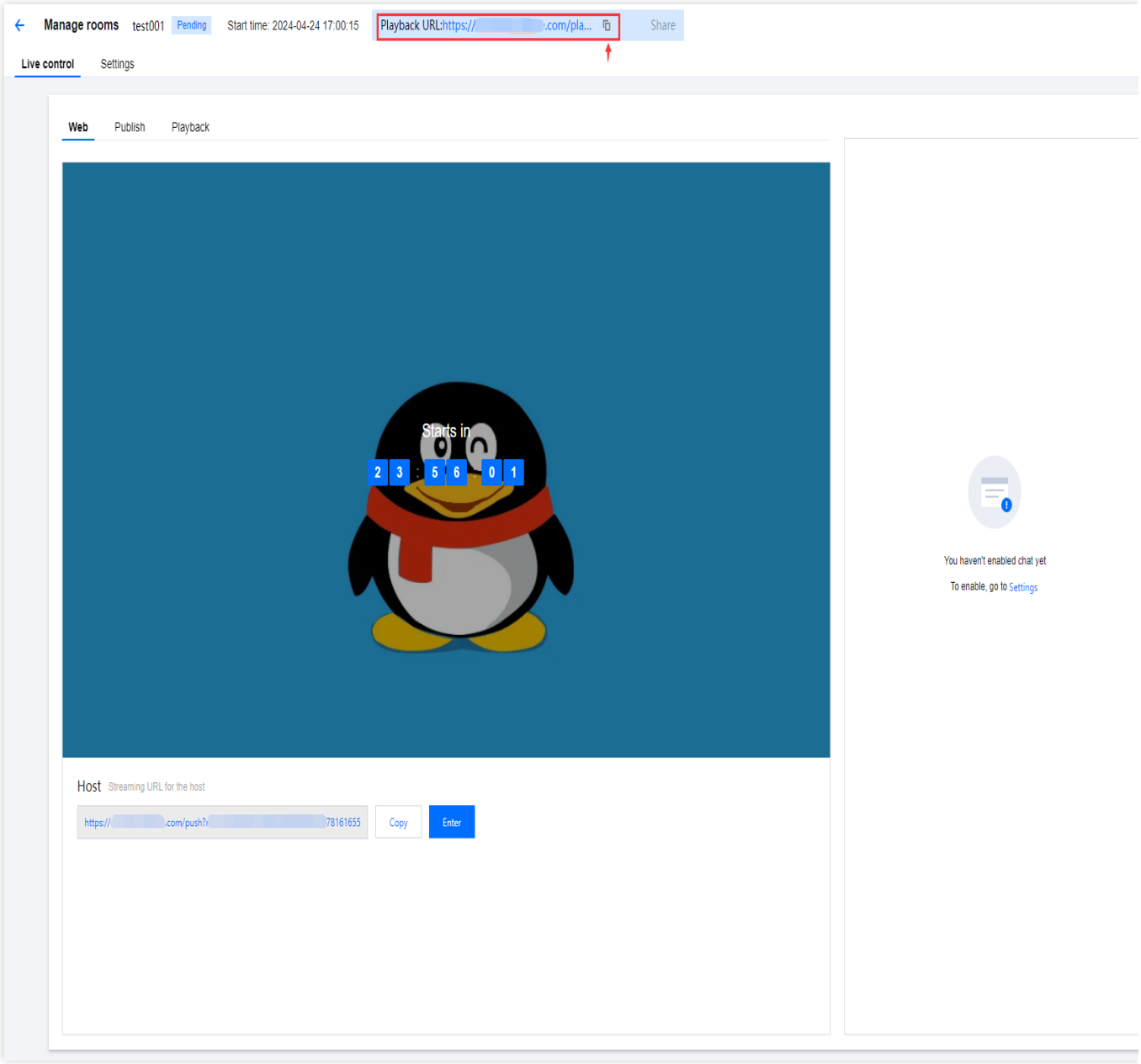
3. Enter the live streaming control page and choose the method of starting the live streaming according to your actual business needs. You can select Web, Publish, or Playback:
Web: The host uses the web-based live streaming tools provided by OOTB live. Options for live streaming include using a camera, local files, or screen sharing.
Publish: The host can stream using third-party tools such as OBS. In this case, the push streaming addresses provided by the system are entered into these third-party tools. For more information, refer to Push via OBS.
Playback: This method is geared towards scenarios that require effectuating recorded video into live streaming (pseudo-live) or pulling streams from third-party platforms for playback on Tencent Cloud.

Scenario 1: Web

This scenario is mainly focused on real-time processing.
1. When you select **Web**, you can allocate the page address to the host. Click on **Copy** to replicate the address.



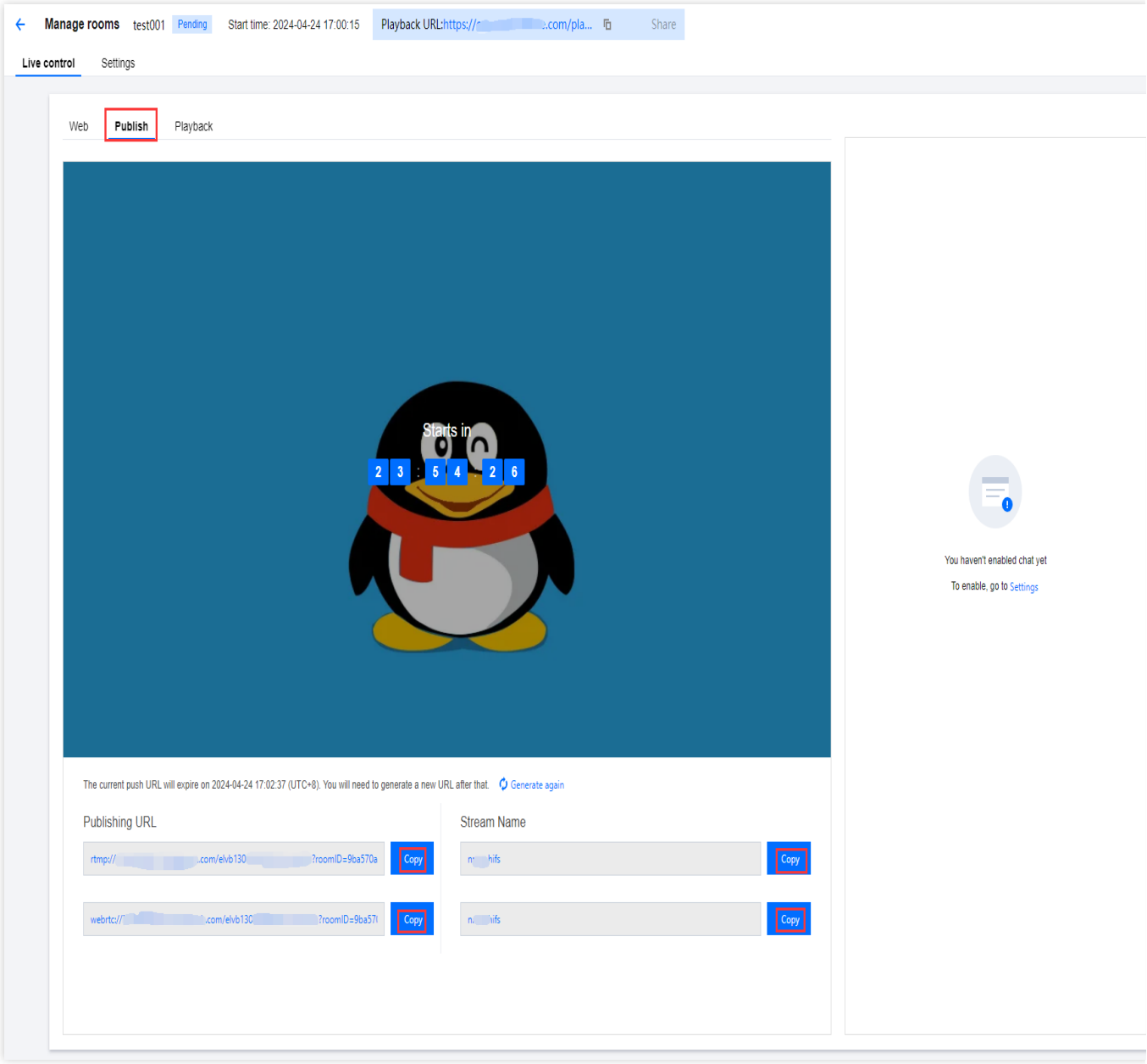
2. Copy the **Playback URL** at the top of the page or click on the copy icon to copy the URL, and then distribute the playback URL to your audience.



3. To activate the comment feature, please go to **Settings**.

Scenario 2: Publish

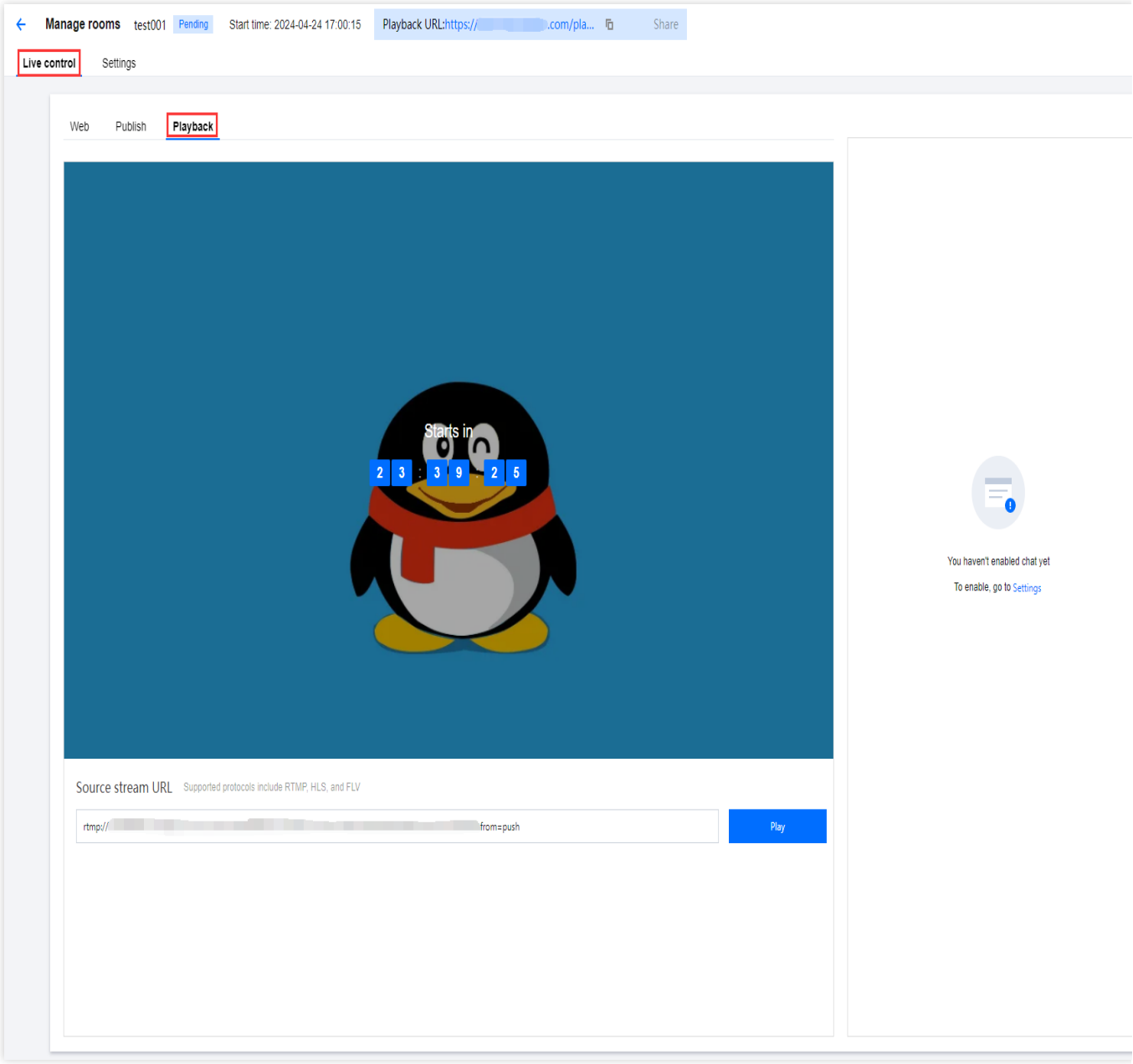
1. By default, the system generates a publish URL and stream name, which can be copied to third-party publish streaming tools such as OBS for live streaming.
2. The copied publish URL and stream name can be pasted into OBS's server and stream code respectively for publishing.



Scenario 3: Playback

1. The source stream address supports live streaming playback protocols such as RTMP, HLS, and FLV, among others.

2. In the source stream address input box, you can enter the source stream address, which is equivalent to setting the content source to a live source in Pull and Push Streaming. After entering the address, click **Play** on the right to pull the corresponding live stream and push it to Tencent Cloud.

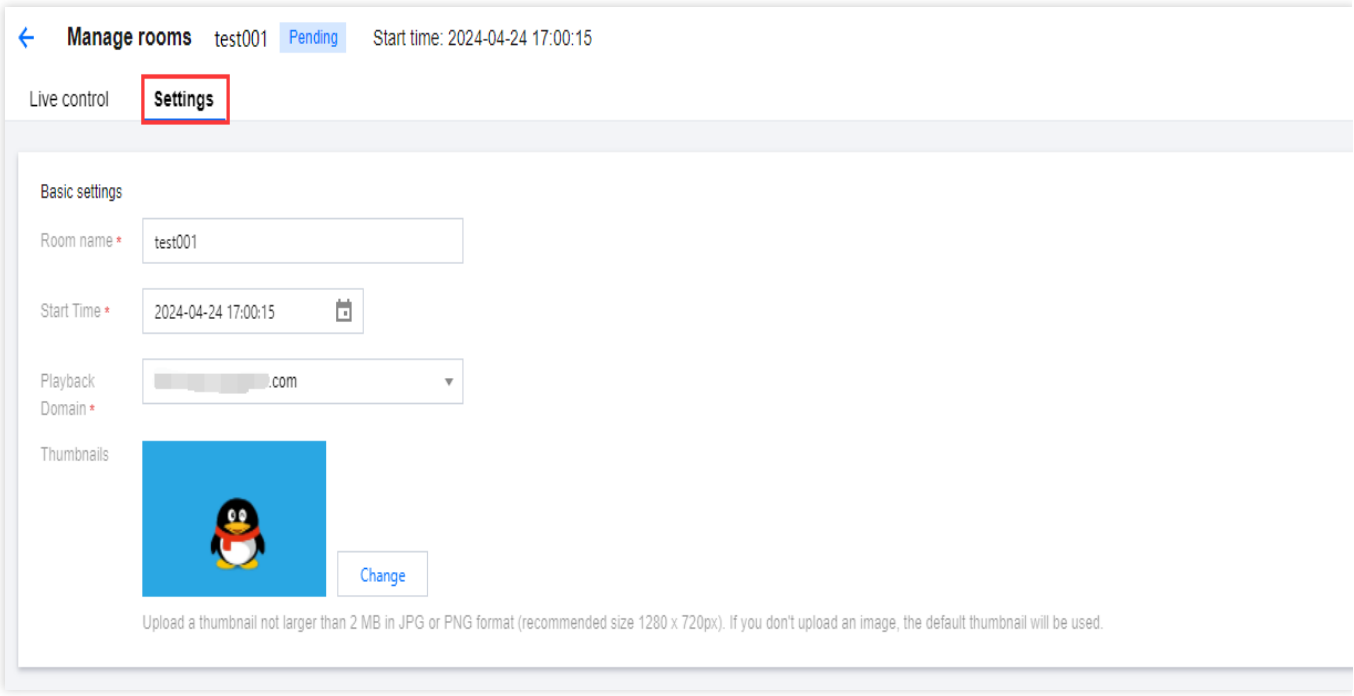


Live Room Configuration

Basic settings

Log in to the CSS console, go to **CSS Toolkit** > OOTB live > **Manage rooms** > **Settings**.

After completing the basic settings, you can adjust and modify the basic settings, including the live room name, start time, playback domain, and live streaming cover.

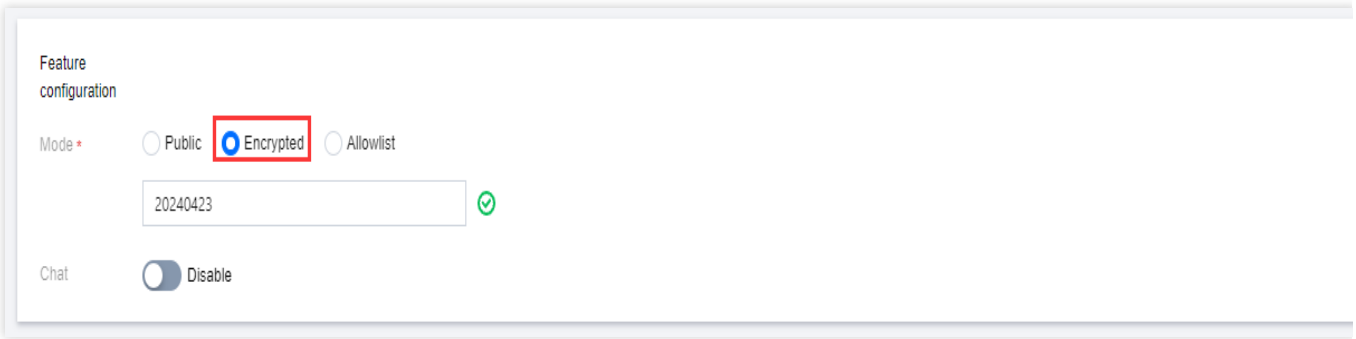


Feature configuration

1. **Viewing Methods**

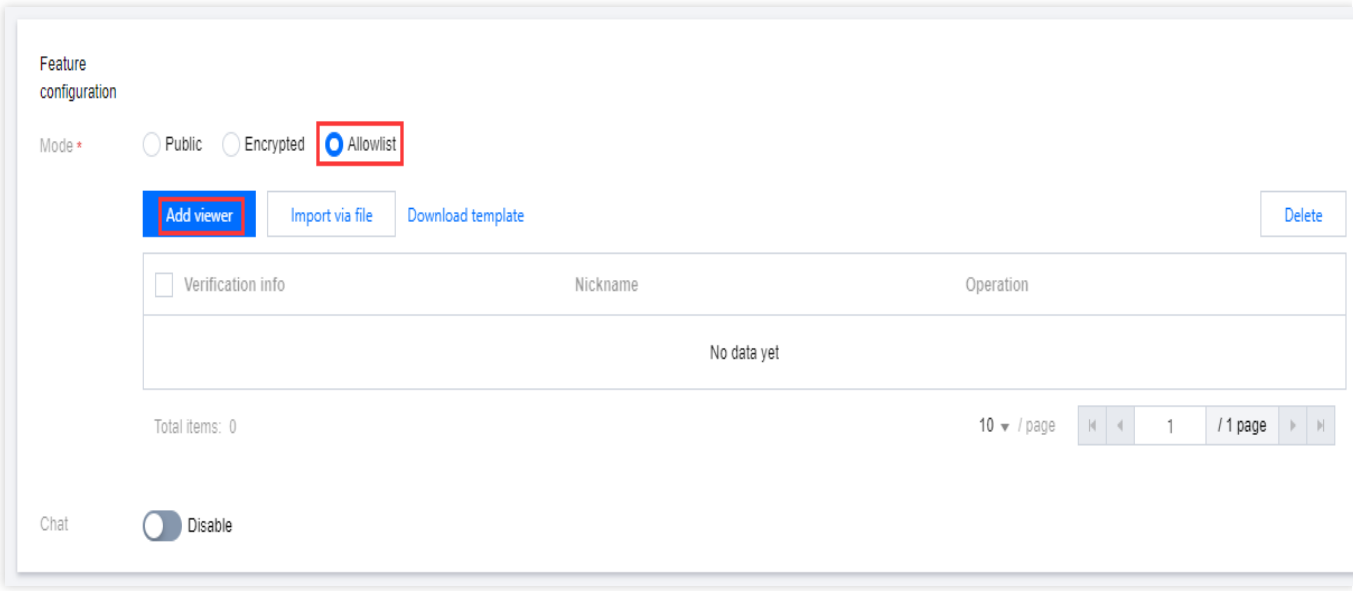
1.1 The default viewing method is **Public**. However, you may opt for **Encrypted** viewing or employ an **Allowlist**.

If you opt for encrypted viewing, a password is required for viewing the live stream. This password should be between 8-14 characters in length and must not contain spaces, Chinese characters, or special symbols.



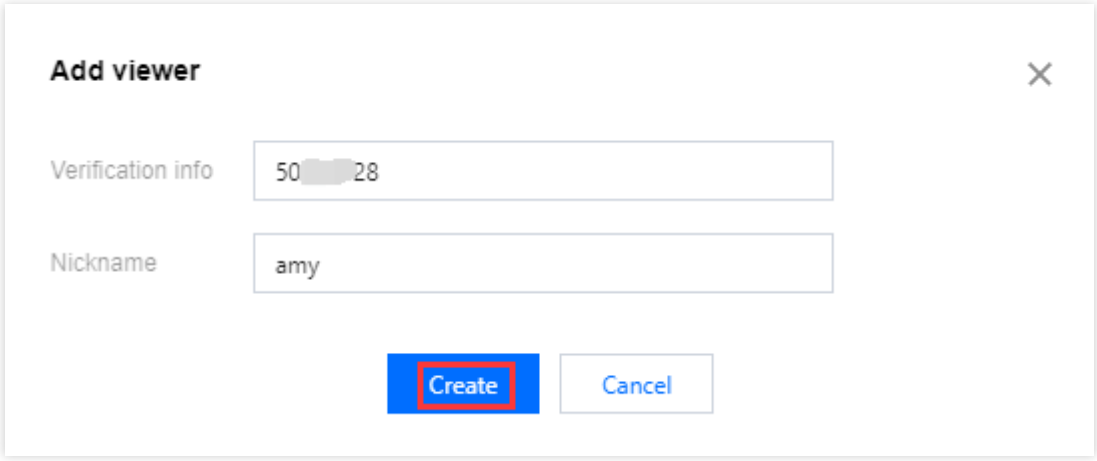
When the viewing method is set to **Allowlist.**

Click on **Add viewer**. In the ensuing pop-up window, you can continuously add new members as required or select and remove existing members.



Verification Info: Please enter the corresponding verification information, such as employee number, mobile number, and so on.

Nickname: Please set a name for the viewer. It could be the viewer's real name or a custom nickname.

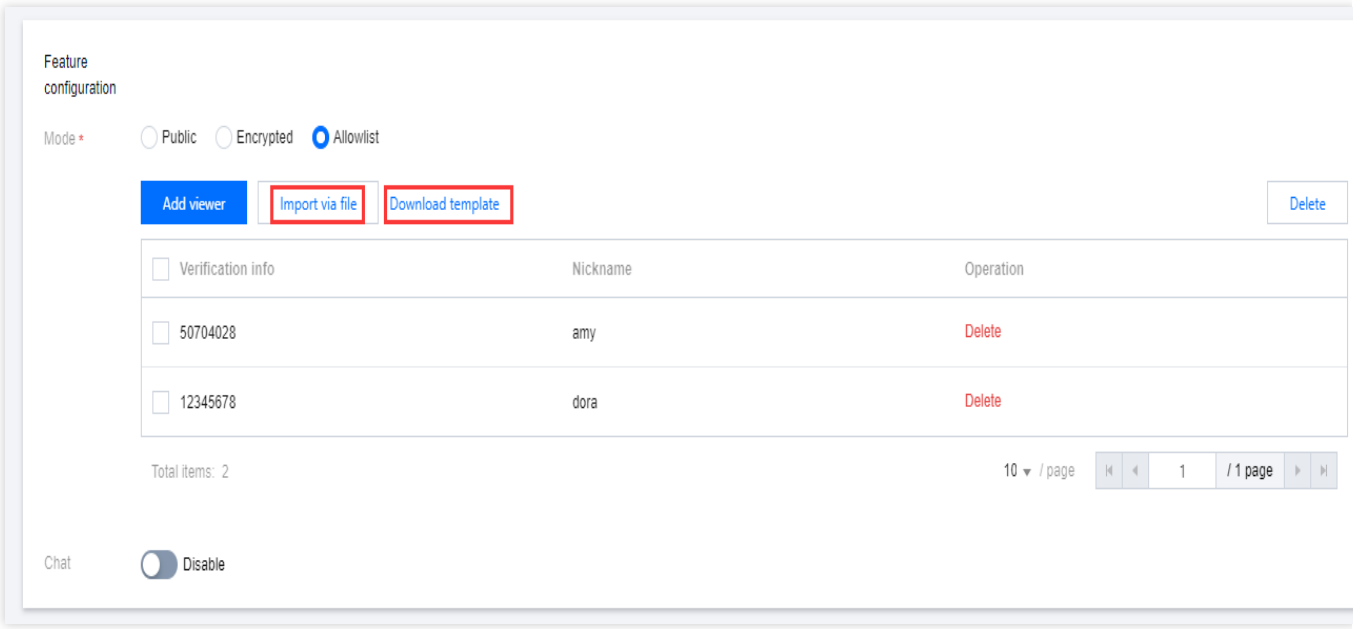


Click **Create**.

Click **Import via file** to import CSV or Excel files to quickly add users allowed to view the live stream.

Click **Download template** to download the import template. Maintain the list information based on this before importing, otherwise it may lead to import anomalies.

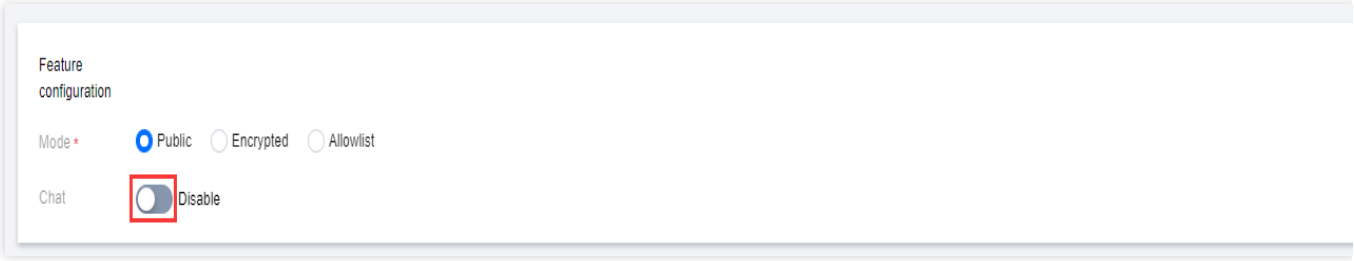
Click **Download template** to download the imported template. Maintain the list information based on this before importing it. Otherwise, exceptions may occur during the import.



2. **Live Stream Interactive Comments**

The live stream interactive comments feature is disabled by default. You can click

to enable this feature according to your actual business needs.



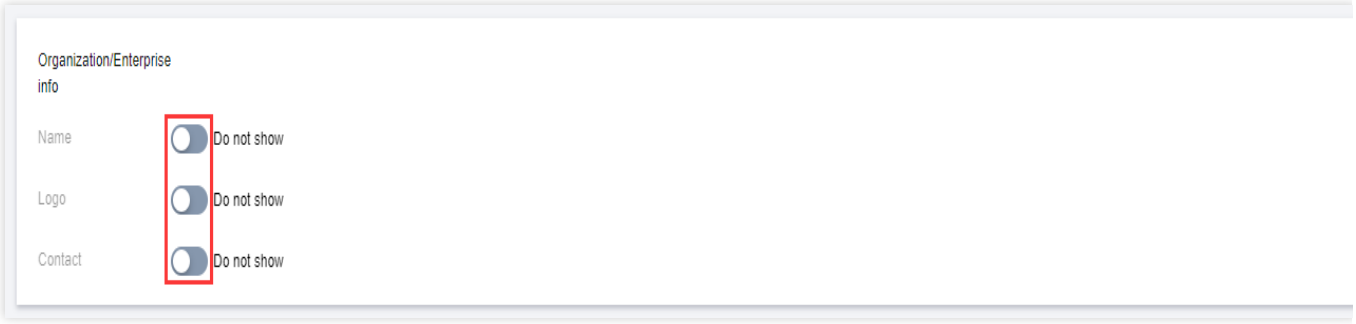
Note:

Live streaming room interactive chat, on-screen comments, and other interactive features are provided by Tencent Cloud IM. The default application is in the development version (the application name starts with "elvb_"), which is validfor one month. After expiration, you can go to the IM console to renew or upgrade the version at any time,according to subsequent business needs.

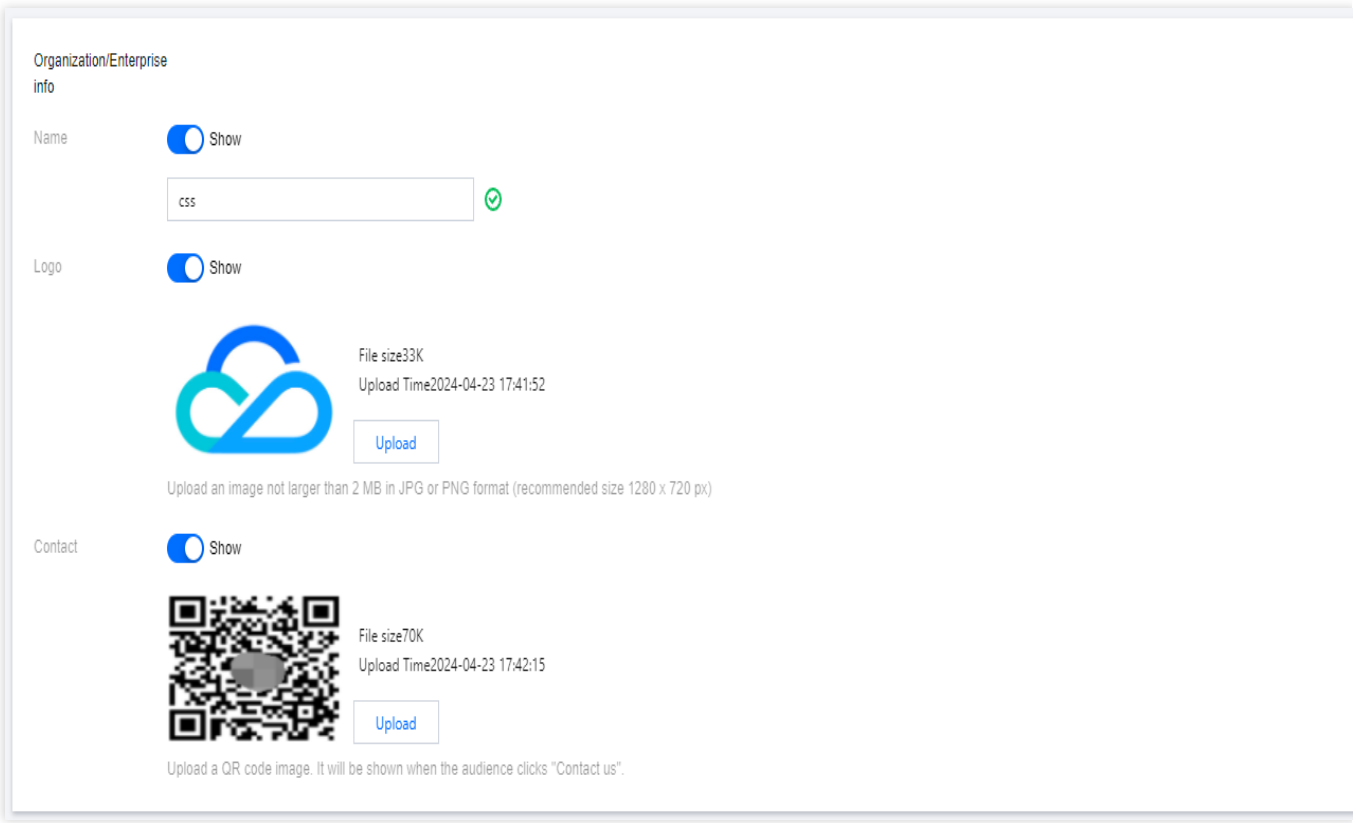
Organization/Enterprise info

The operational configuration information is **disabled** by default. You can click


to activate it according to your actual business needs.

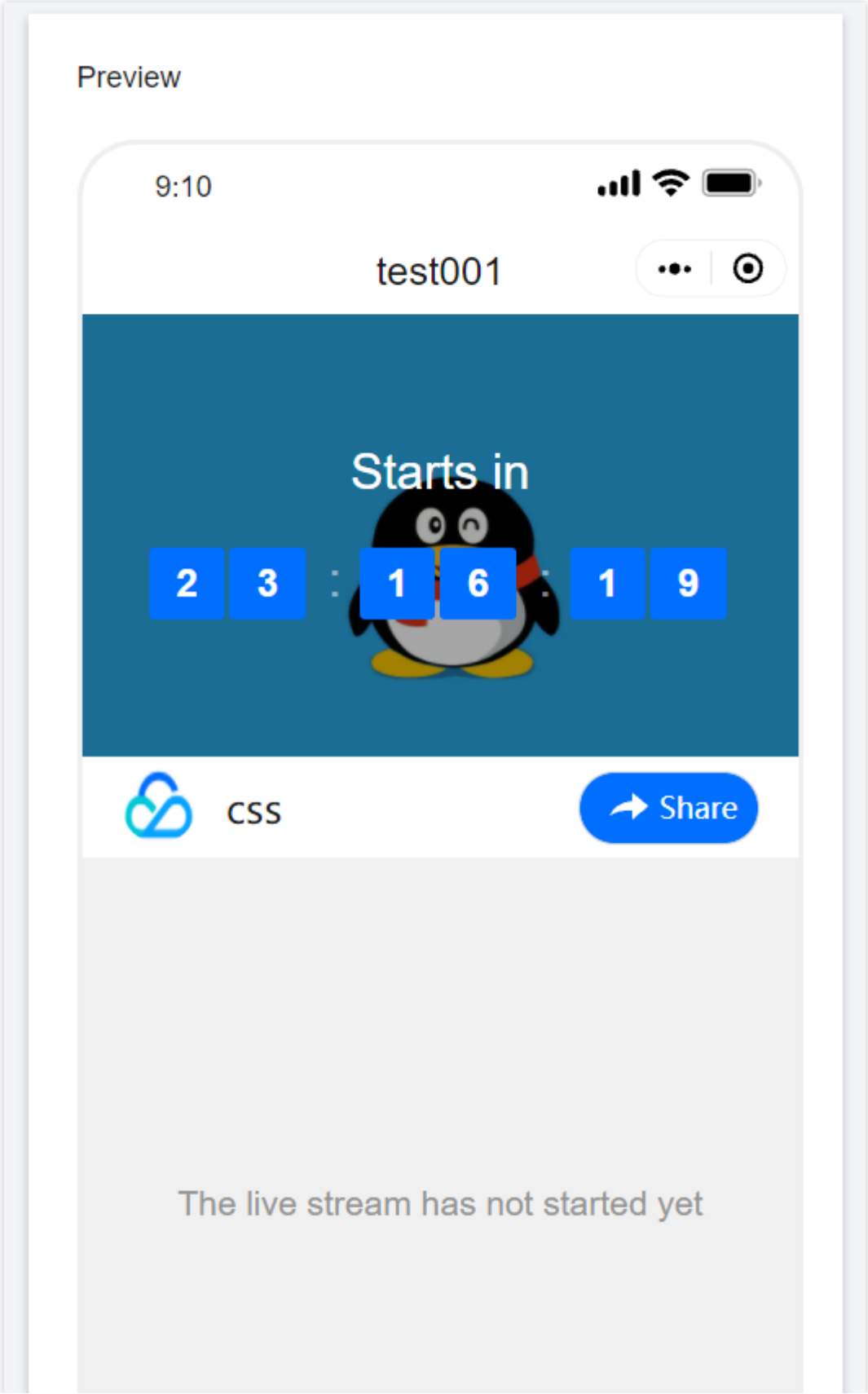


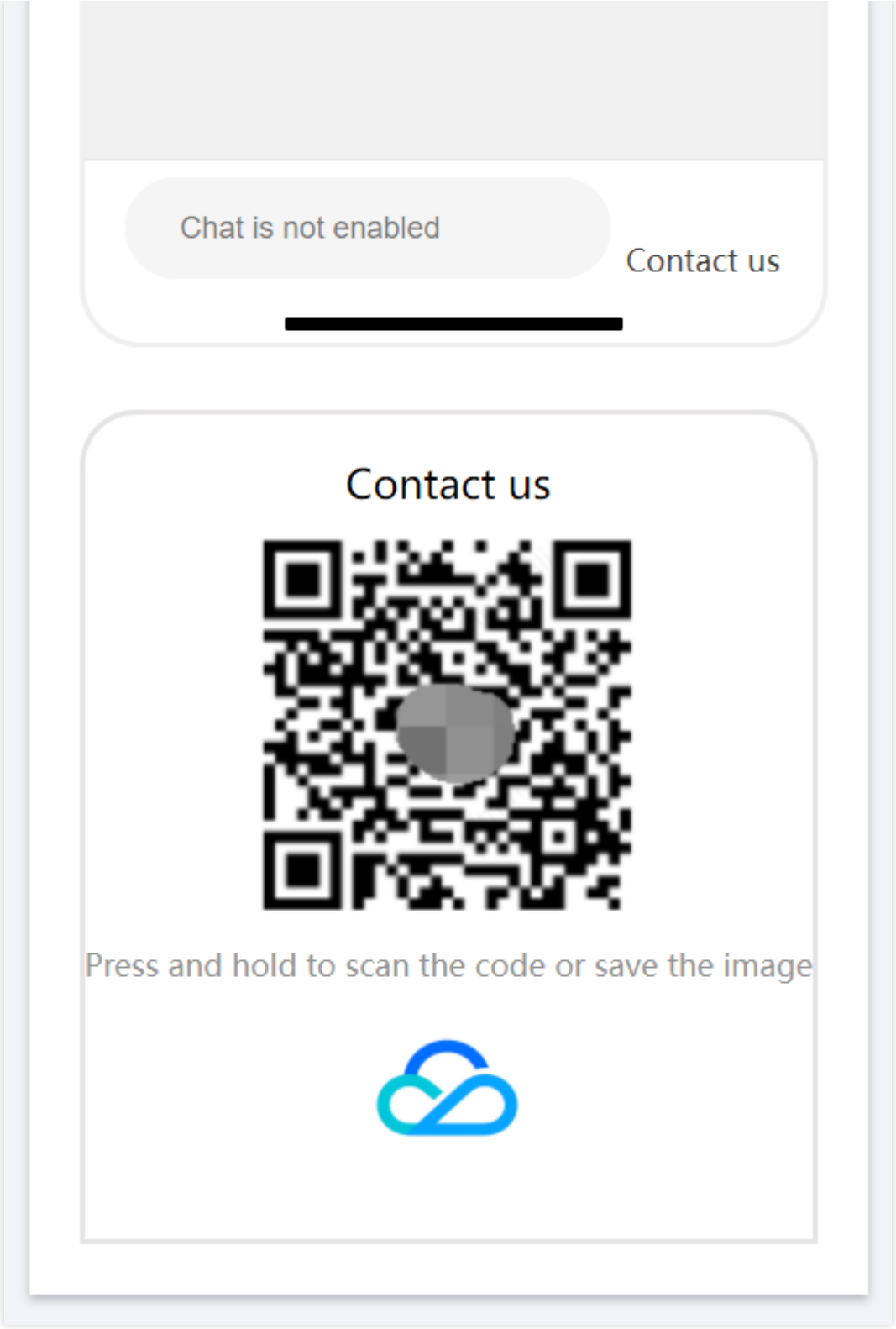
Name: Please enter the name of the organization or enterprise, no more than 60 characters.
Logo: Click **Upload** to set an organization or enterprise's logo. We recommend a JPG or PNG image with the resolution of 1280*720px, of 2 M or smaller.
Contact: Click **Upload** to set a QR code for the audience. When an audience clicks **Contact us**, this QR code will pop u p onthe interface.



Configuration Preview

1. When modifying relevant live room configurations, you can instantly view the effects **through Configuration** Preview on the right.





2. After confirming the preview, click **Save**, and commence the live streaming as needed.

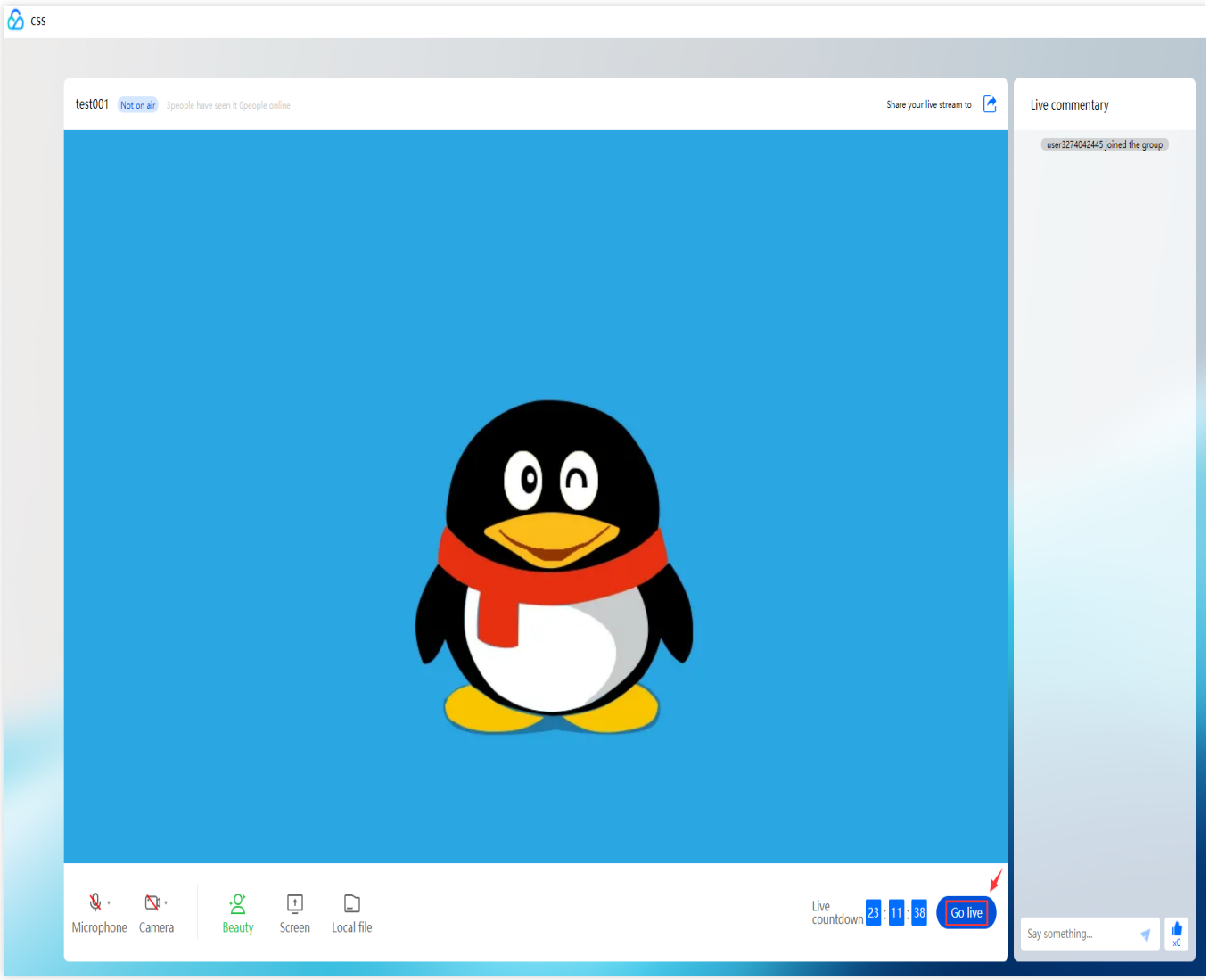
Note:

The configuration will take approximately one minute to take effect after it has been completed.

Host Side

When the Host Is Not Live

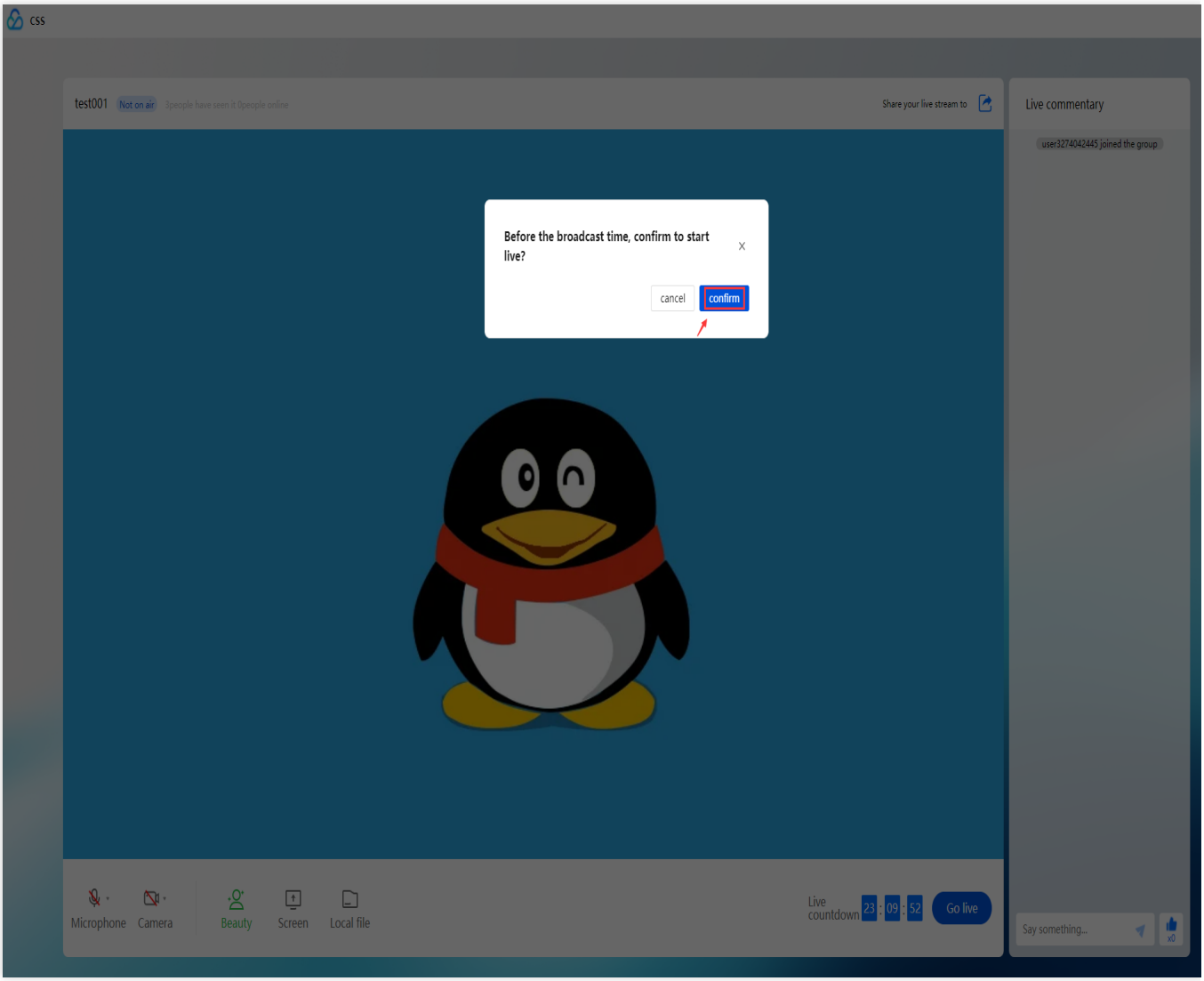
1. Even if the live streaming start time has not yet arrived, you can start your live stream in advance. Just click on **Go live** at the bottom-right corner.



Note:

The live streaming countdown refers to the time difference between the start time of the live stream and the current time.

2. To confirm that you want to start the live stream in advance, click **confirm** inthe prompt box and commence the live stream.

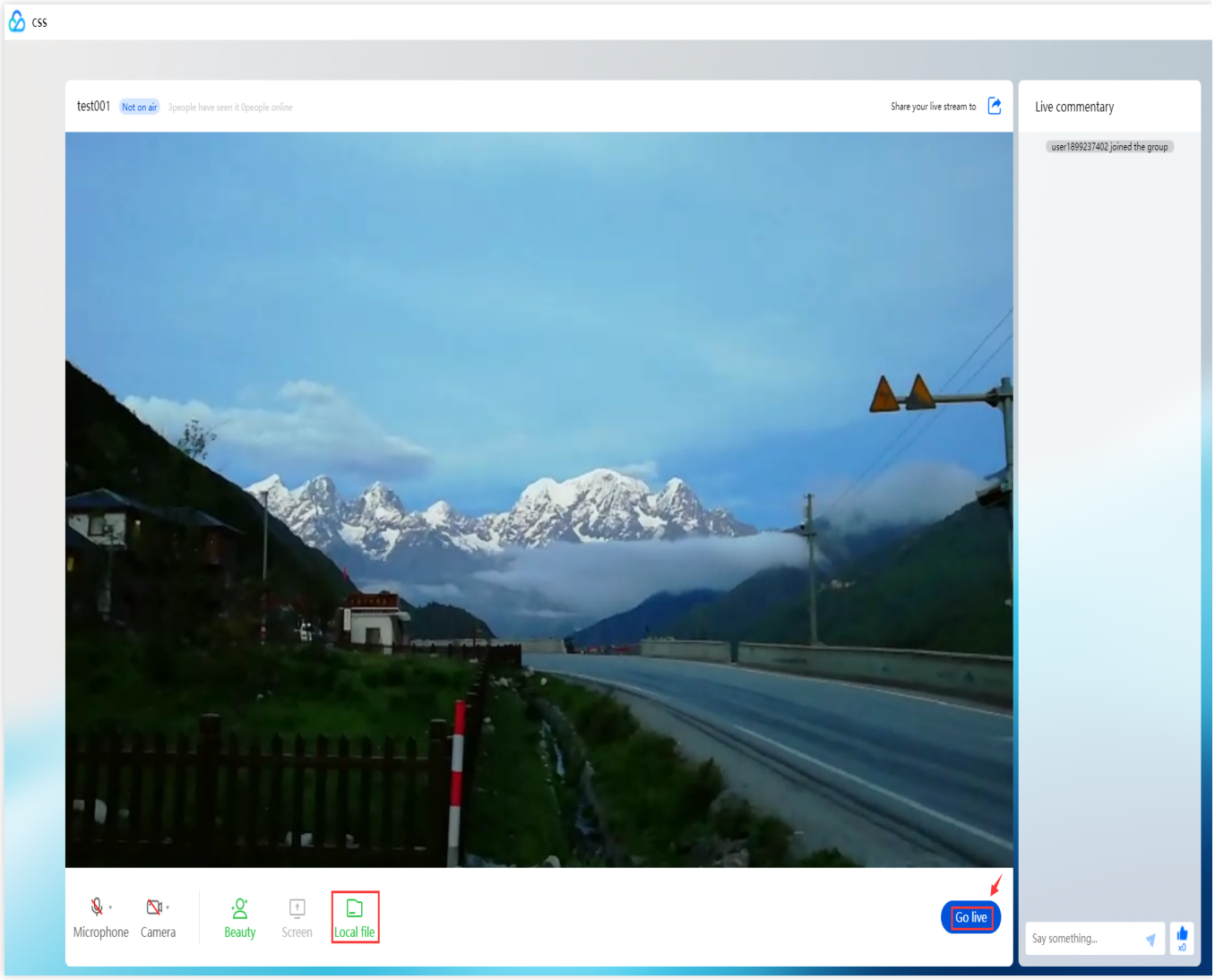


During the Host's Live Stream

1. When the web platform is used to conduct a live stream, the WebRTC stream publishing protocol is employed (it is the only protocol supported on the web platform).

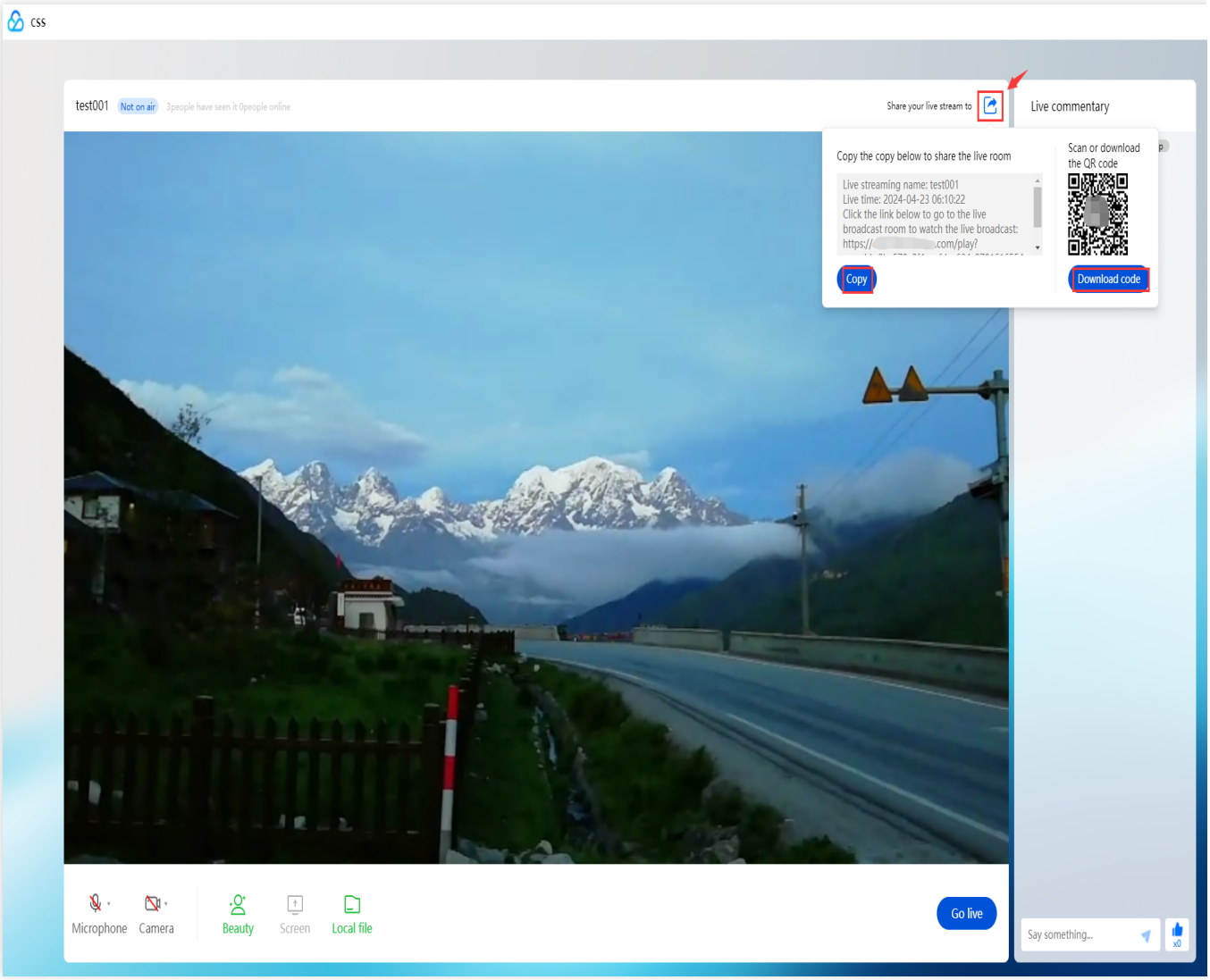
2. You can conduct live streaming through a camera, screen sharing, local files, and so on. Click the **Go live** button and the system will commence streaming. Here's an example of how to live stream through uploading a video from local files:

2.1 On the webpage, select **Local file** and choose the video file you want to upload. After the video is uploaded, click **Go live** to commence the live streaming. It's advised to perform a test in advance to ensure that the live room's settings and video quality meet your requirements.

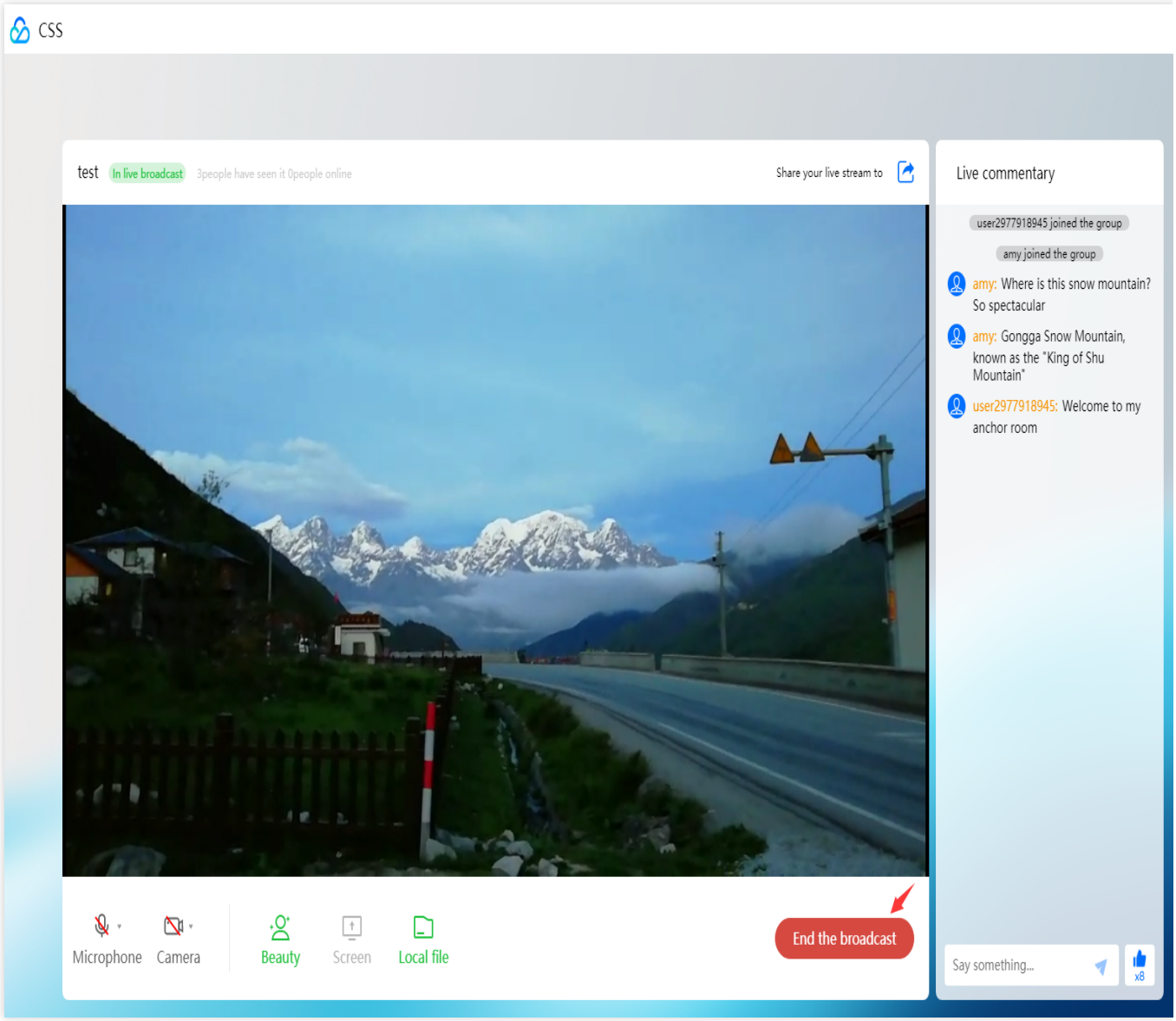


2.2 The host can click the

button in the top-right corner, click **Copy** (the live room's name, time, and URL) or **Download code**, and forward it to viewers. The shared link corresponds to the live stream room. The audience can watch the live stream by scanning the QR code shared by the host or visiting the link.



2.3 Once the official live stream concludes, the host can click **End the broadcast** to cease the live streaming.



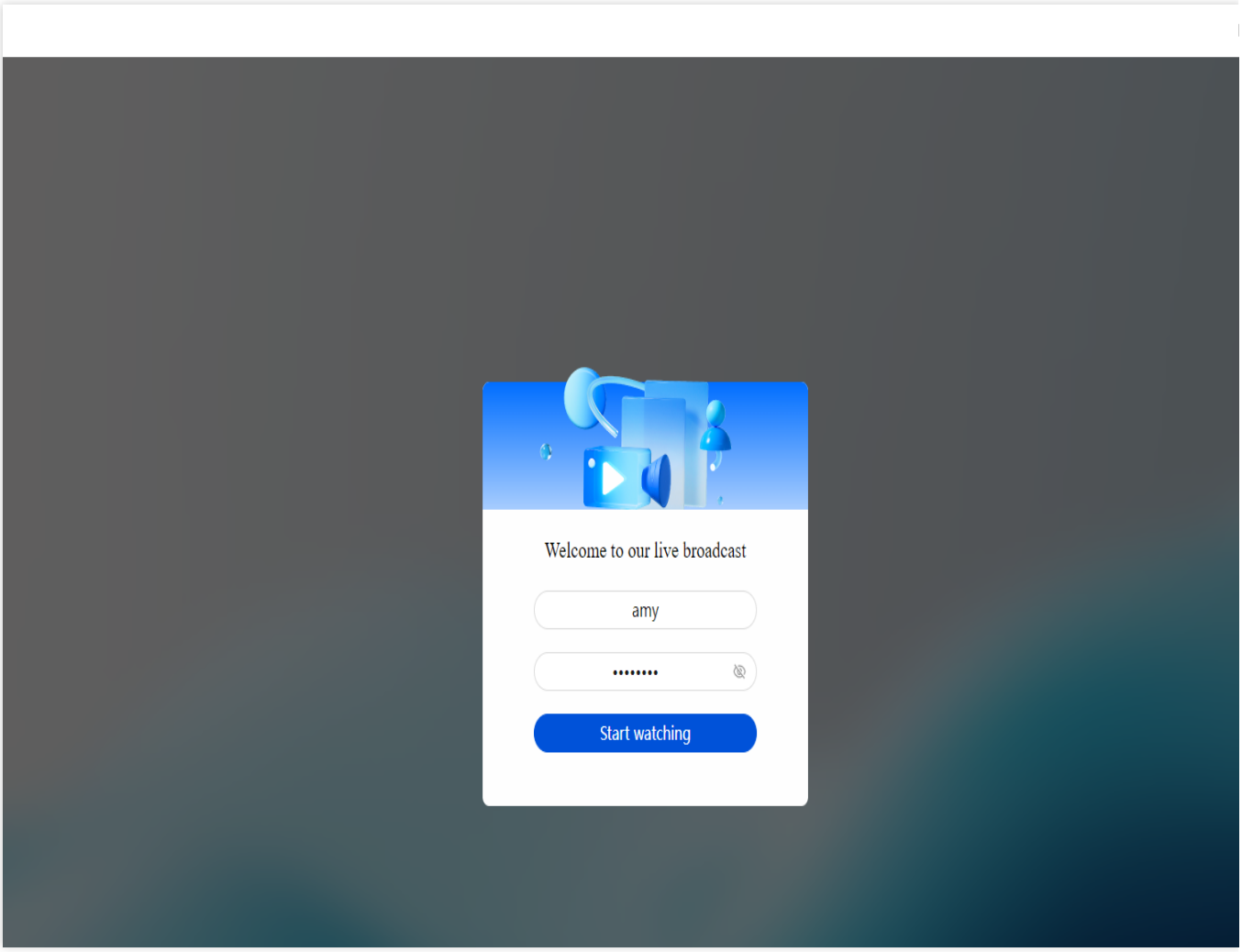
Note:

If the live room is deleted during the live streaming, the ongoing live streaming will not be interrupted.

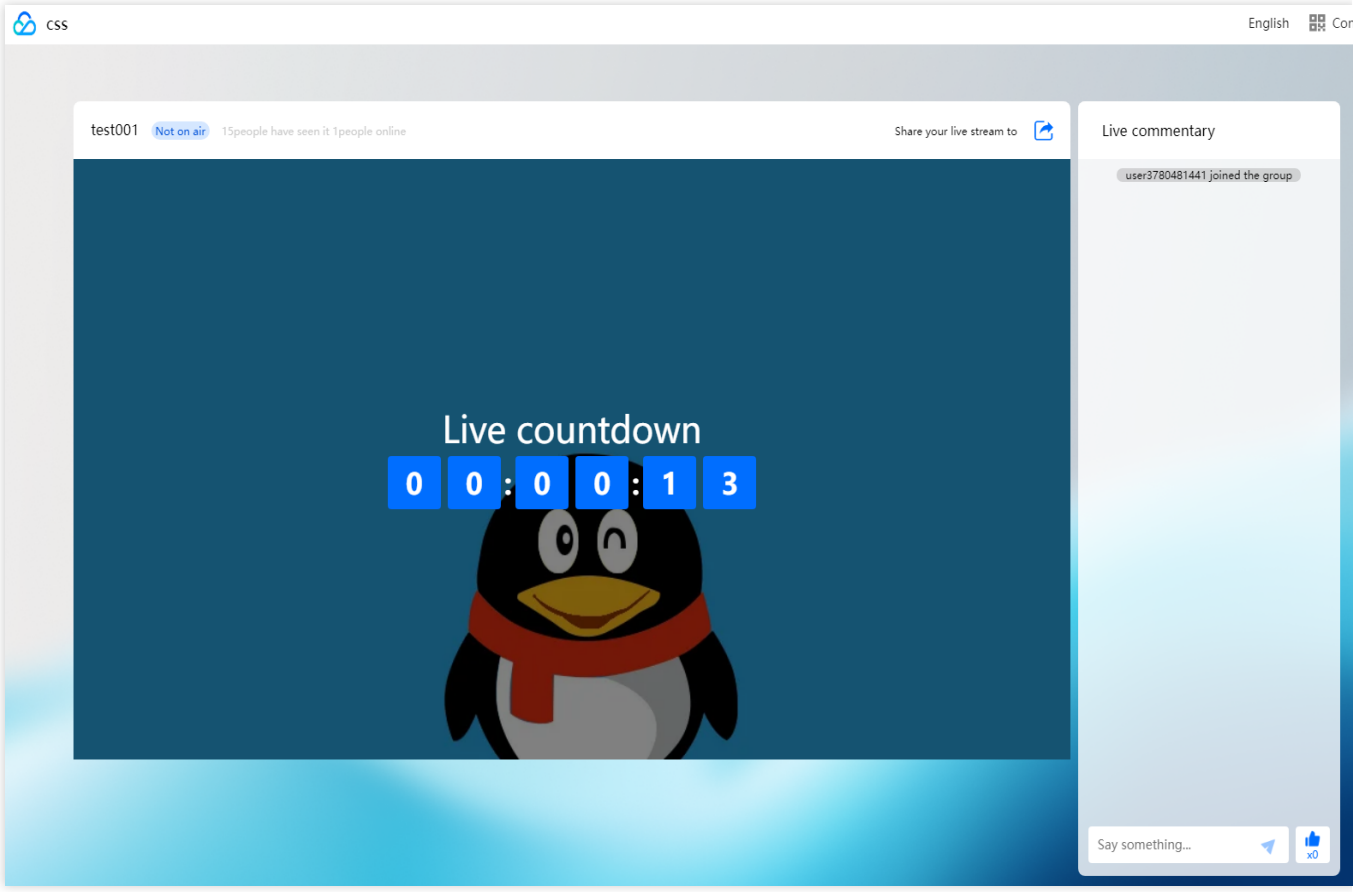
Audience Side

When the Host Is Not Live

1. After visiting the viewing link shared by the host or management side, the audience can, by default, directly open and watch the live streaming. Should the host implement **Encrypted** or **Allowlist** viewing methods, the audience is required to enter verification information (nickname and password) in the pop-up verification bar. Only after successful verification can they proceed to open the live room.

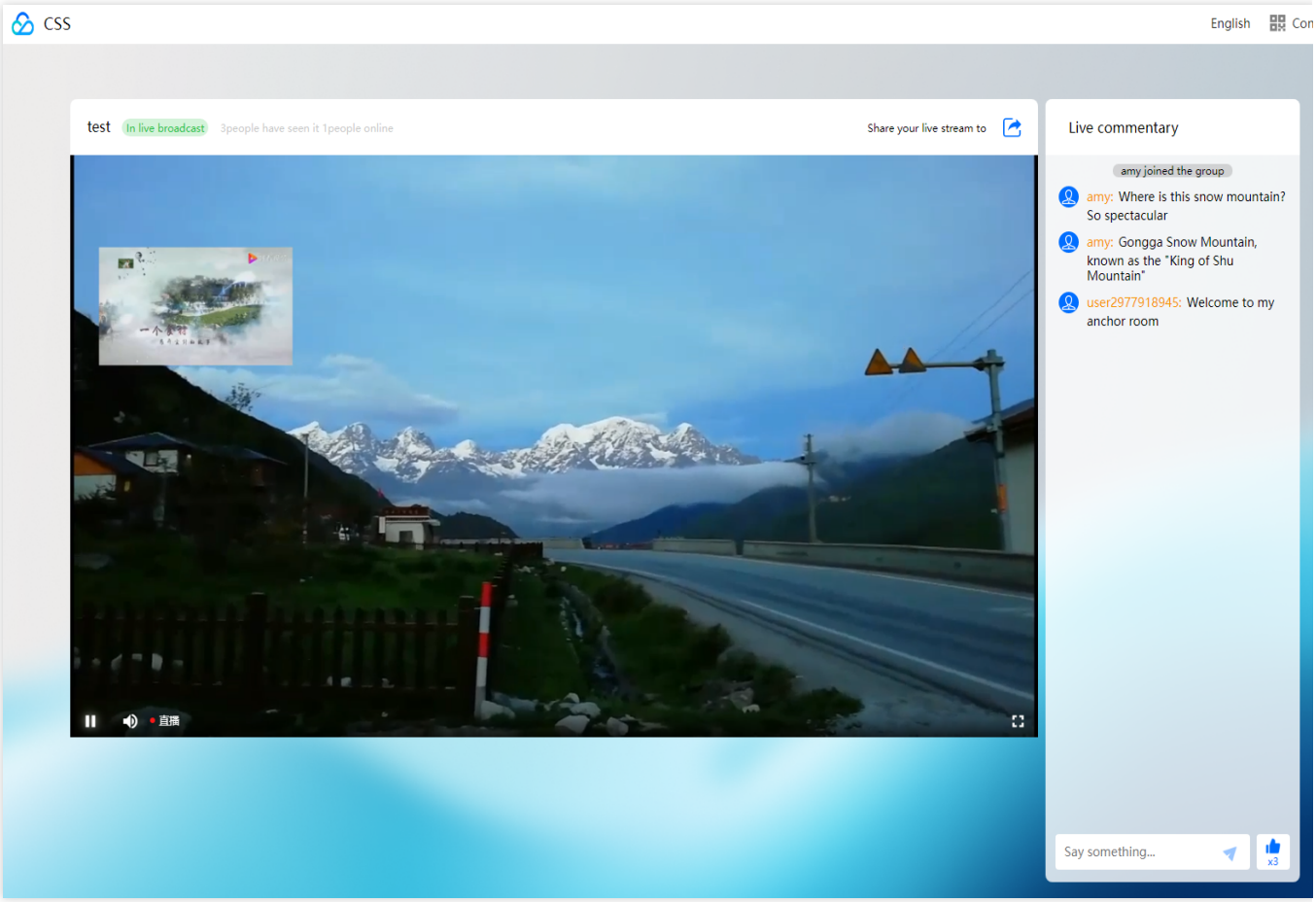


2. When the host is not live, audience entering the live room can see the countdown timer to the live streaming, for them to know the start time of the live streaming.



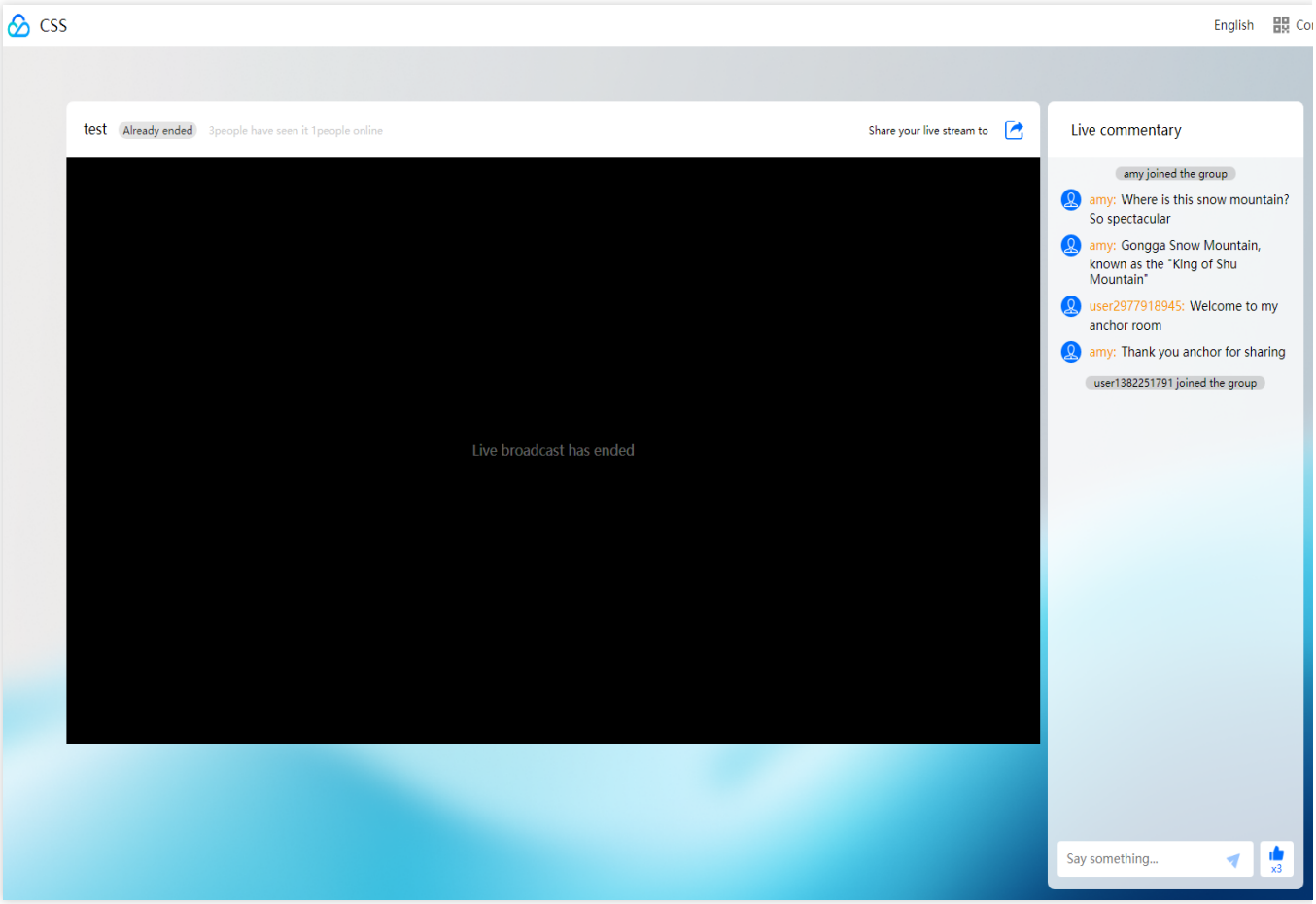
During the Host's Live Stream

After entering the live room, audience can watch the live stream, view and post comments.



End of Live Stream

The live room can still be opened, and the viewers can continue to view and post comments.


CSS
English
test
Already ended
3people have seen it 1people online
Share your live stream to
Live broadcast has ended
Live commentary
amy joined the group
amy: Where is this snow mountain? So spectacular
amy: Gongga Snow Mountain, known as the "King of Shu Mountain"
user2977918945: Welcome to my anchor room
amy: Thank you anchor for sharing
user1382251791 joined the group
Say something...
x3

CAM-Based Access Control

Last updated：2024-10-17 16:32:53

CSS supports permission control via CAM, allowing you to manage access to your CSS domains, settings, and other data. You can create, manage, or terminate users or user groups and grant API access permissions to them to achieve identity management and policy control.
You can use CAM to bind a user or user group to a policy which allows or denies them access to specified resources to complete specified tasks.

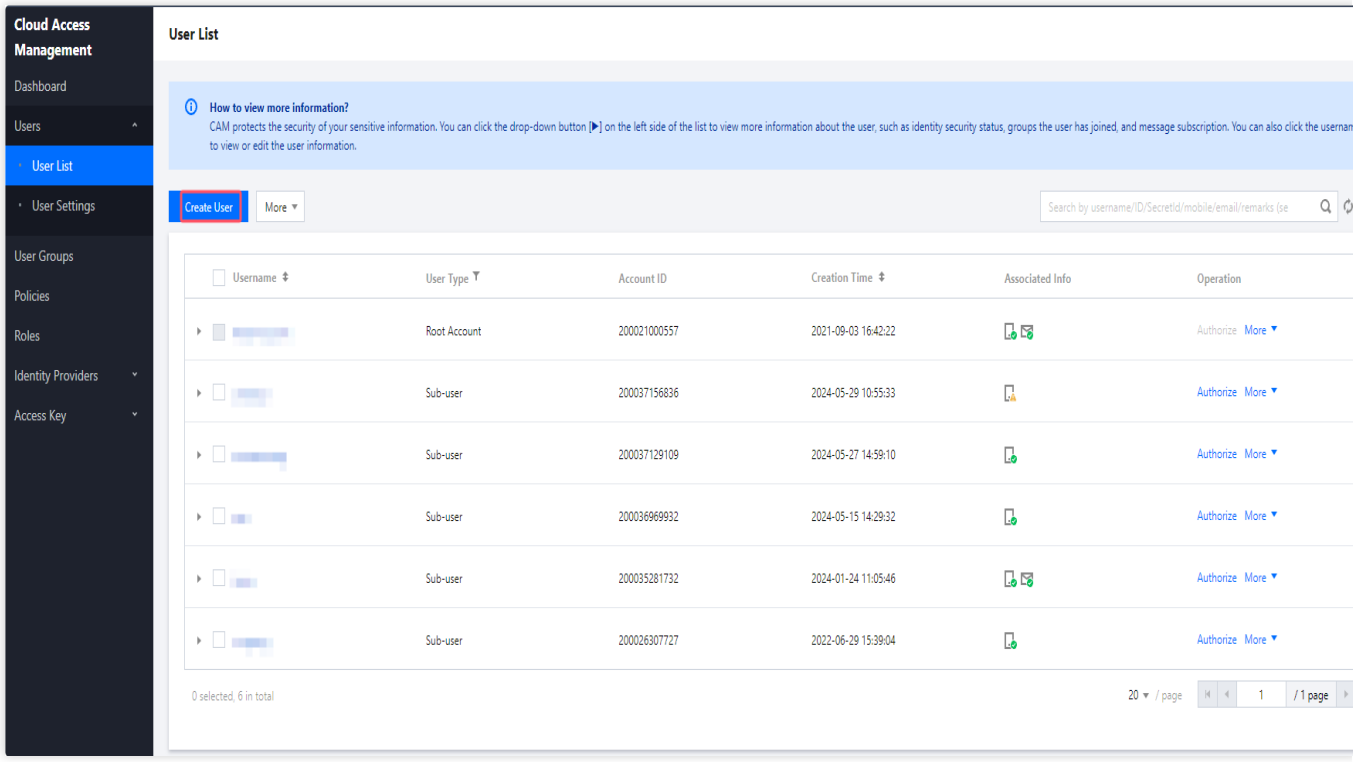
Concepts

Root account: A Tencent Cloud account
Sub-user: A user created and fully owned by a root account.
Collaborator: You can add another root account as a collaborator to your account. The added account becomes a sub-account of your account.
User group: Users that perform the same functions and can be bound with a permission policy for centralized access management.
Note:
For more information on the concepts and permissions, see User Types.

Directions

Step 1. Create a sub-user or user group

One or more sub-users can be created under each root account and can be associated with specific roles and policies. A sub-user has a unique ID and identity credential that can be used to log in to the Tencent Cloud console. It also has API access. You can log in to the CAM console to create a sub-user.



Note:

For detailed directions, see Creating Sub-user and Creating User Group.

Step 2. Add a policy to the sub-user or user group

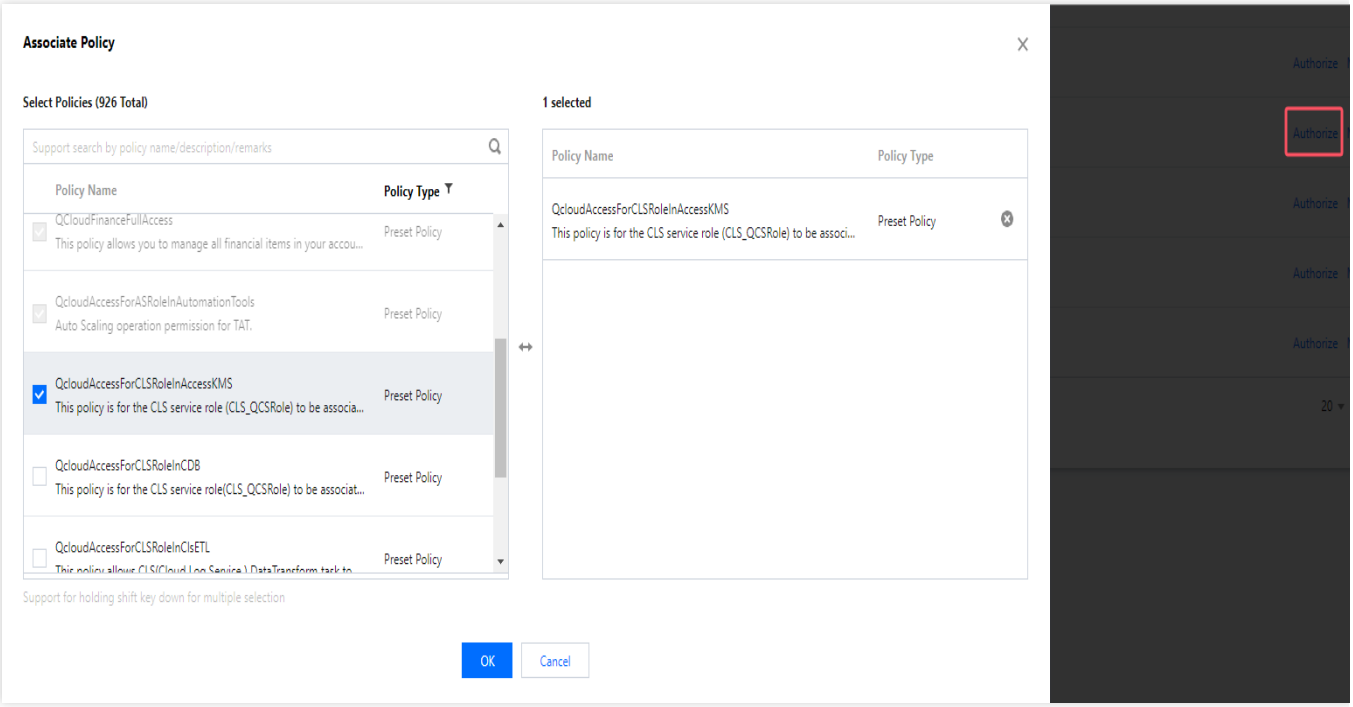
You can associate policies on the user/user group management page or policy management page. For detailed directions, see Authorization Management.

Method 1. Add a policy to a sub-user or user group

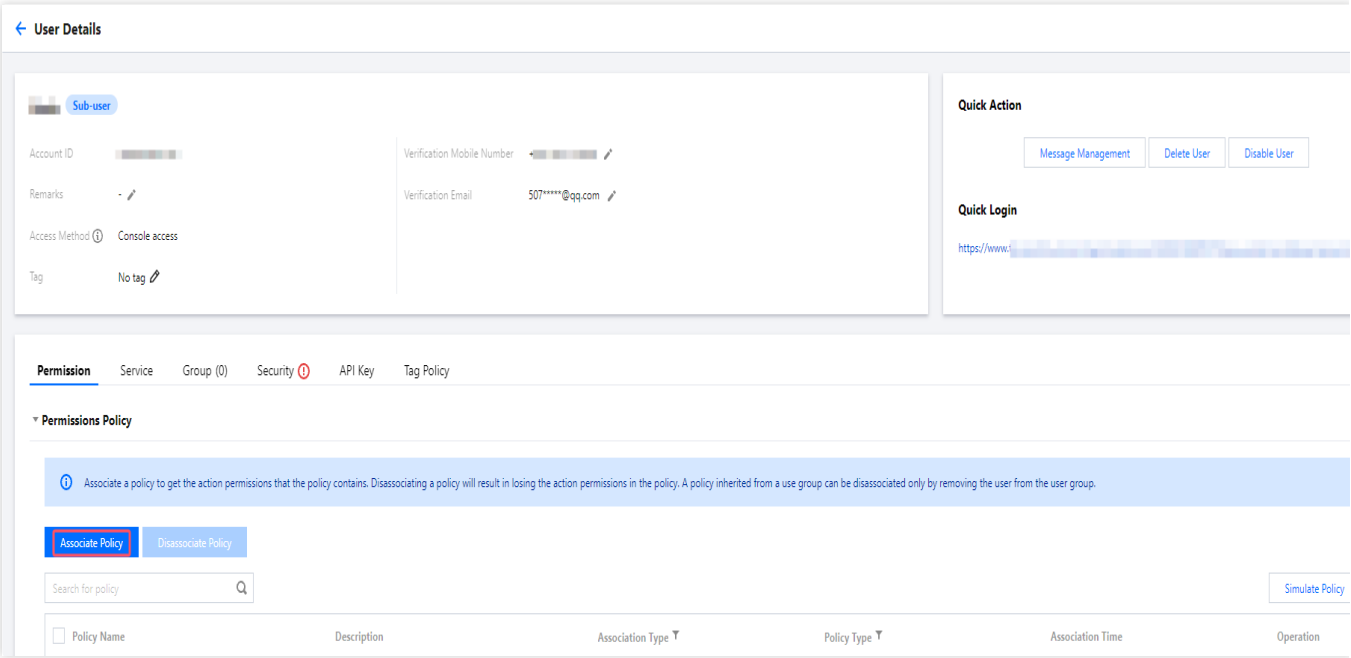
Method 2. Associate a policy with a user/user group

Go to the user/user group page and select the user/user group to which you want to add a policy.

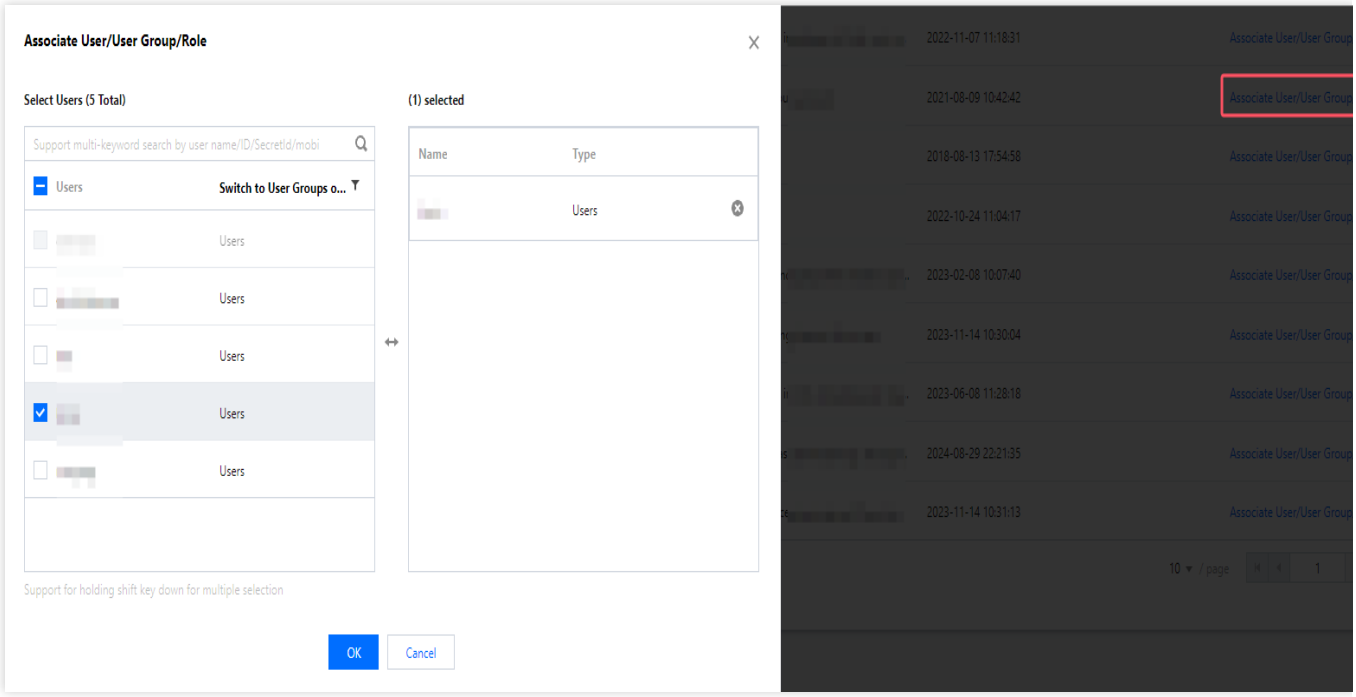
Select **Users > User List** or **User Groups** on the left sidebar of the CAM console. Find the user/user group to which you want to add a policy, click **Authorize** on the right, select a CSS policy, and click **OK**.



Select **Users > User List** or **User Groups** on the left sidebar and click the name of the user/user group to which you want to add a policy. Click **Associate Policy**, select a CSS policy, and click **OK**.



Select **Policies** on the left sidebar of the CAM console, find the policy you want to associate, and click **Associate User/User Group/Role** in the **Operation** column. Select the user/user group you want to associate the policy with, and click **OK**.



Addable policies

Preset policies: You can view all preset policies on the **Policies** page.

CSS preset policies include QcloudLIVEFullAccess (read and write policy) and QcloudLIVEReadOnlyAccess (read-only policy).

For a user to use tags, you need to associate QcloudTAGFullAccess (full read and write access by tag).

For a user to use real-time logs, associate QcloudCamFullAccess (full read/write access to CAM).

To use the screenshot & porn detection feature, associate QcloudAccessFoLVBRoleInSaveLiveScreenshottoCOS with your CSS service role to grant it access to COS.

Custom policy: Go to the **Policies** page, click **Create Custom Policy**, and select **Create by Policy Generator**. For more information, see Custom Policy.

Note:

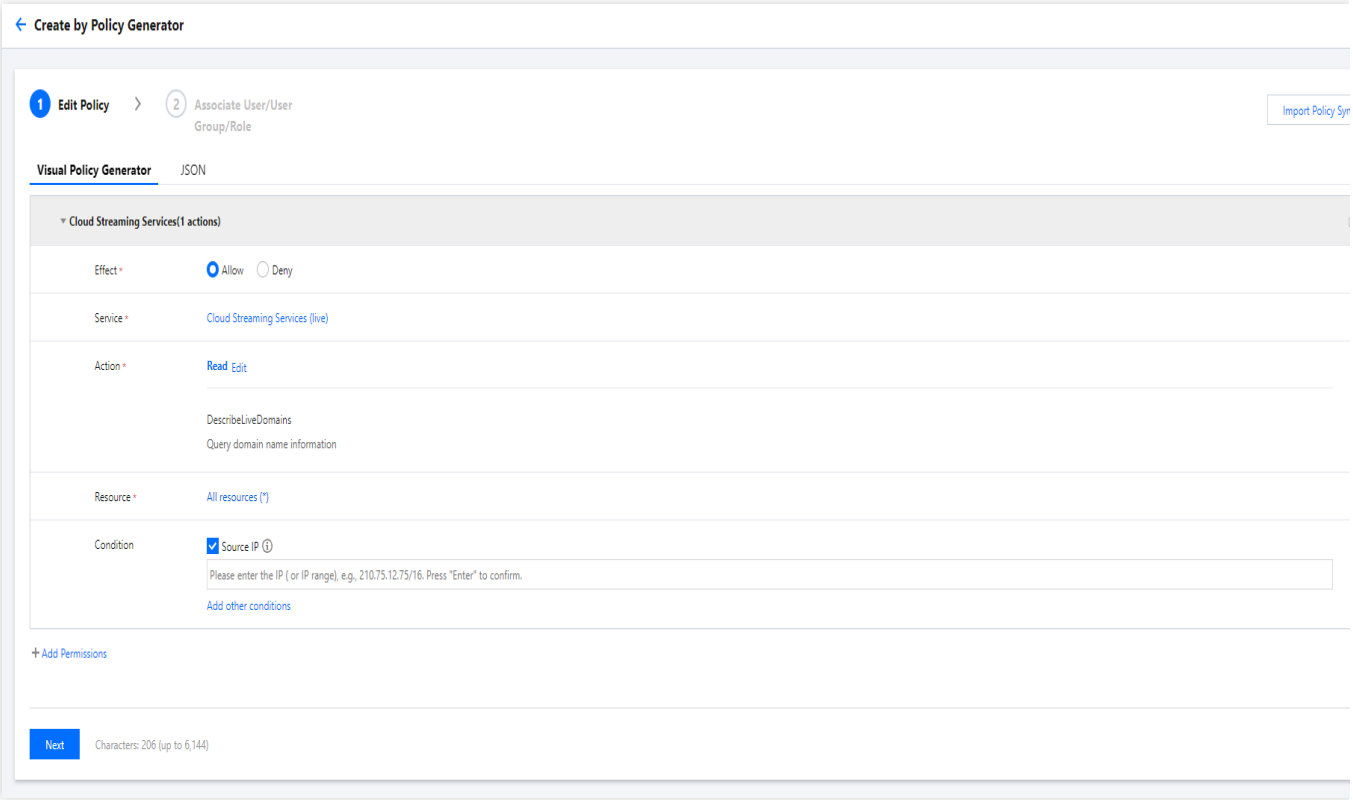
Currently, some APIs of CSS support resource-level authorization.

Example: If you want to allow a sub-user to use the **DescribeLiveDomains** API, follow the steps below to grant the permission.

1.1 Create a domain-level policy that allows access to the API: Go to the **Create by Policy Generator** page and complete the following settings:

Item	Required	Setting
Effect	Yes	Select Allow
Service	Yes	Select Cloud Streaming Services
Action	Yes	Select DescribeLiveDomains

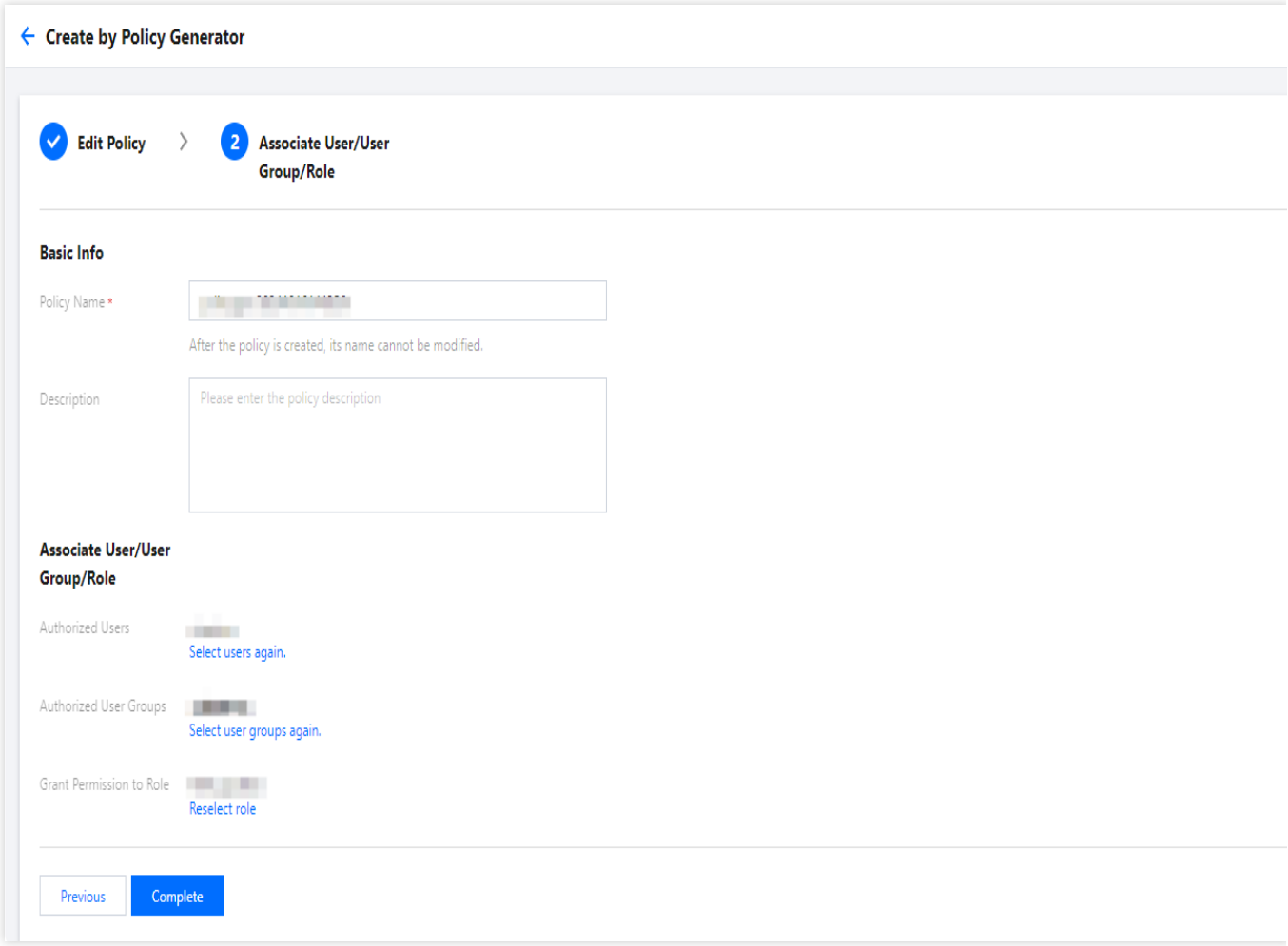
Resource	Yes	Select all resources or specific resources. Tencent Cloud services for which the authorization granularity is operation or service don't support six-segment resource descriptions; for them, select “All resources”. For Tencent Cloud services that support resource-level authorization, you can select specific resources. For the resource description method and authorization granularity of Tencent Cloud services, see CAM-Enabled Products.
Condition	No	Set the condition for the authorization to take effect. If you enter IP addresses, the API will be accessible only if a request is from the specified IP range. You can also add other conditions. For more information, see Conditions.



Note:

If you want to authorize multiple services, click **Add Permissions**.

1.2 Click **Next** to generate the policy. Then, associate it using either of the two methods above.



Step 3. Use a sub-account

You can now use the sub-user's account (the account ID and password) to call the API authorized (such as `DescribeLiveDomains`) and get the corresponding CSS data (such as all the domains under the current account).