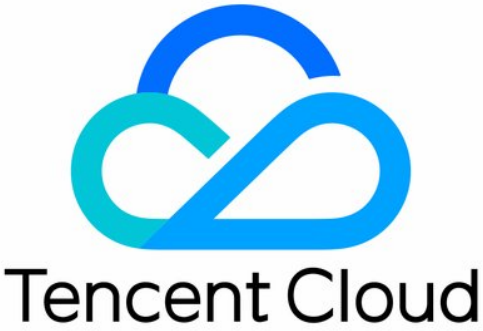
Cloud Infinite

Console Guide

Product Documentation



Contents

Console Guide
Overview

Last updated：2024-01-31 16:44:15

The CI console provides fast and convenient smart processing services for various types of data, such as images, videos, and files. It also allows you to easily manage buckets and monitor resources.
After you log in to the CI console, you will be redirected to the **Overview** page by default, where you can view the information of current CI service usage, including **resources and overall usage**, **month-to-date core data**, **alarm configuration**, **billing overview**, **help documentation**, and **quick entries**.

Resource and Overall Usage

This section displays the **number of buckets**, **month-to-date total traffic**, and **month-to-date read requests**.

Item	Description
Number of Buckets	Number of buckets for which the CI service is activated
Month-to-Date Total Traffic	Total amount of public network downstream traffic, private network traffic, and CDN origin-pull traffic in the current month
Month-to-Date Read Requests	Total number of GET and HEAD requests in the current month

Month-to-Date Core Data

This section displays the resource usage of various services, including **service traffic**, **image processing**, **media processing**, **content moderation**, **content recognition**, and **file processing**.

Alarm Configuration

This section displays the configuration of CI monitoring metrics, including the **number of current alarms** and **configured alarm policies**.

Billing Overview

This section displays the **month-to-date billing information** and the deduction status of each billable item in the **bills of the previous month**.

Note:

You can estimate the approximate amount payable from the 1st day of the current month to yesterday based on the month-to-date billing information.

Billable items marked with pay-as-you-go are postpaid.

Job and Workflow

Job

Last updated：2024-01-31 16:44:15

Overview

For files already in a bucket, you can create a job for media processing. Currently, the following jobs are supported: **audio/video transcoding**, **top speed codec transcoding**, **broadcast media format transcoding**, **video montage**, **voice/sound separation**, **text to speech**, **audio/video splicing**, **video frame capturing**, **video to animated image conversion**, **intelligent thumbnail**, **video enhancement**, **super resolution**, **audio/video segmentation**, **SDR to HDR**, **image processing**, **digital watermark extraction**, which can be created by template. You can use the preset templates provided by CI or customize templates. For more information, see Template.

Note:

Currently, jobs can process 3GP, ASF, AVI, DV, FLV, F4V, M3U8, M4V, MKV, MOV, MP4, MPG, MPEG, MTS, OGG, RM, RMVB, SWF, VOB, WMV, WEBM, MP3, AAC, FLAC, AMR, AWB, M4A, WMA, and WAV files. When initiating a media processing request, you must enter the complete file name and extension; otherwise, the format cannot be recognized and processed.

Currently, the job feature can only manipulate **existing files**. To manipulate files during **upload**, use the workflow feature.

After a job is created, feature fees will be charged. For billing details, see Media Processing Fees.

To use the media processing service, make sure that resources are available. Do not enable input image protection (as described in Configuring Buckets), hotlink protection (as described in Managing Domain Names), and other access control features.

Viewing Jobs

On the job page, you can view all jobs in different types for the **specified time period**, click **Status** to filter and view jobs in different statuses, search for jobs by job ID in the **search box**, and click **View** on the right of a job to view its following information:

Job information: Job ID, job status, queue ID, template ID, job creation time, and job end time.

Input information: Source video bucket, region, and storage path.

Destination information: Destination media address, bucket, region, and storage path.

Note:

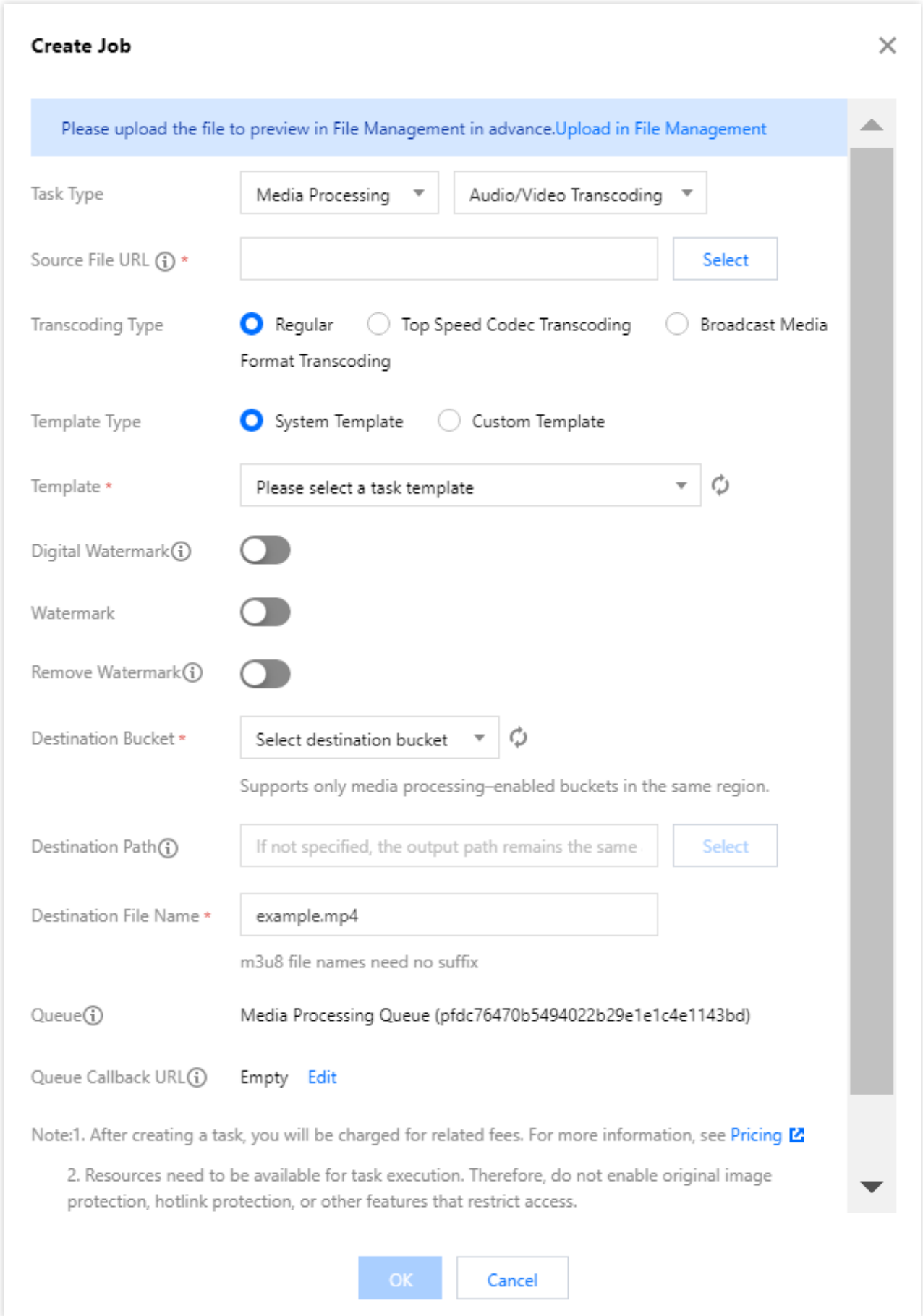
A job has six statuses: succeeded, failed, executing, pending, paused, and canceled.
You can query the records of jobs for the past month only.

Creating an Audio/Video Transcoding Job

The audio/video transcoding feature converts an audio/video file bitstream. It changes parameters of the source bitstream, such as codec, resolution, and bitrate, to adapt to different devices and network conditions.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Media Processing** > **Transcoding** > **Audio/Video Transcoding** as the job type, click **Create Job**, and configure as follows:



Source File URL: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.
Transcoding Type: Select **Regular**.
Template Type: Select **System Template** or **Custom Template**.
Template: Select a specified template.
Digital Watermark: You can add a blind watermark to the video during transcoding for copyright protection.
Watermark: Add an image or text watermark to the video during transcoding.
Remove Watermark: Select the image watermark and remove it.
Accelerated Transcoding: If you toggle on this option, the job is added to the accelerated transcoding queue and the transcoding speed can reach more than 5 times of the regular transcoding speed.
Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.
Destination File Name: Name of the destination file.
Destination Path: Path of the destination file.
Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating a TSC Transcoding Job

The top speed codec technology improves the subjective image quality of a video at the minimum bitrate. Compared with standard transcoding, it makes videos smaller and clearer and delivers a better visual experience with low network resource usage.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Transcoding** > **Audio/Video Transcoding** as the job type, click **Create Job**, select **Top Speed Codec Transcoding** as the transcoding type, and configure as follows:

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.
Transcoding Type: Select **Top Speed Codec Transcoding**.
Template: Select a custom template. If there are none, create one first.
Digital Watermark: You can add a blind watermark to the video during transcoding for copyright protection.
Watermark: Add an image or text watermark to the video during transcoding.
Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.
Destination Path: Path of the transcoded video.
Destination File Name: Name of the destination file.
Queue: Currently, only the default queue `queue-1` is supported.

Creating a Broadcast Media Format Transcoding Job

This feature processes special formats such as XAVC and Apple ProRes.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Transcoding** > **Audio/Video Transcoding** as the job type, click **Create Job**, select **Broadcast Media Format Transcoding** as the transcoding type, and configure as follows:

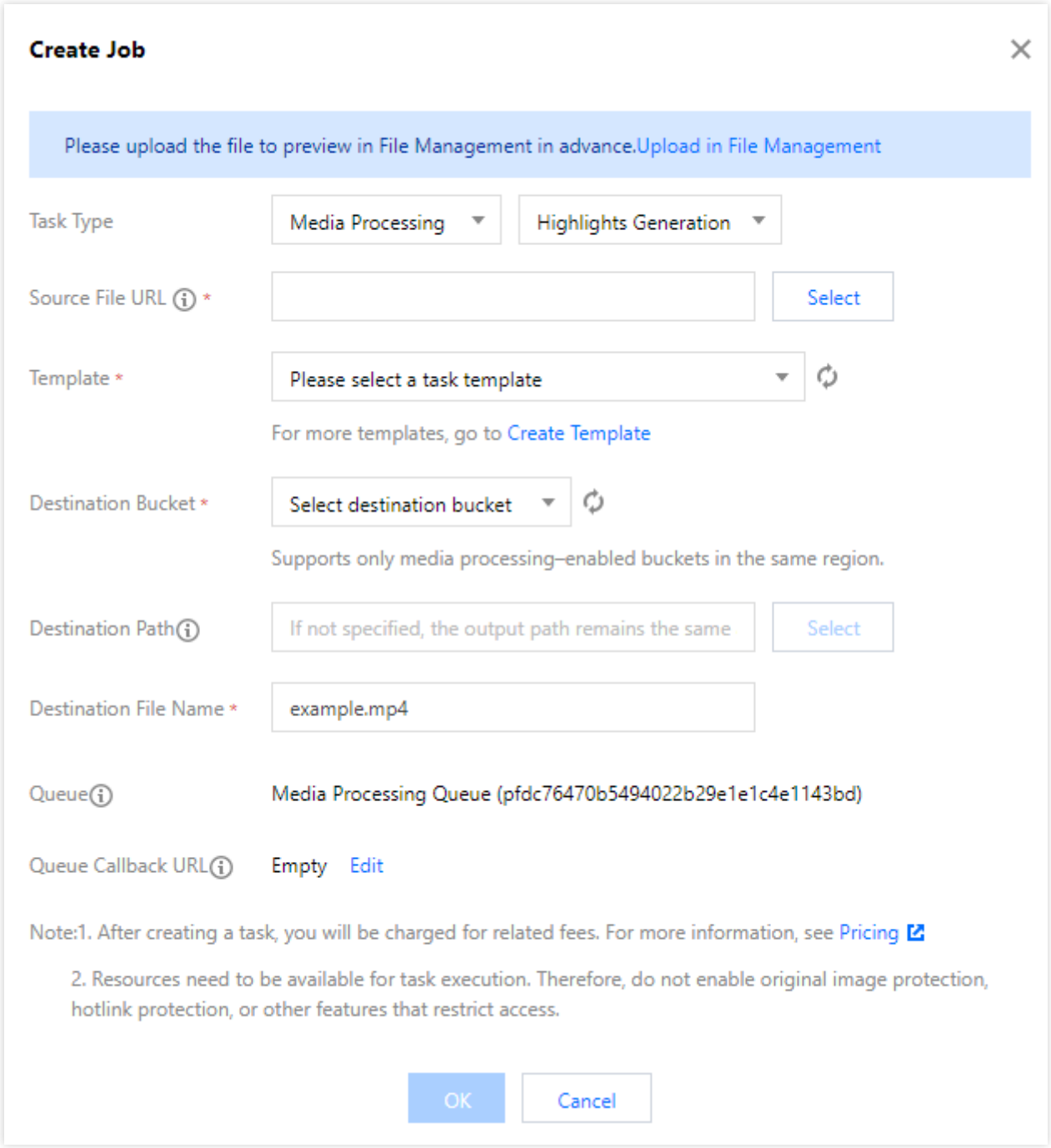
Source File URL: Enter the path of the source file, which cannot begin or end with `/`.
Transcoding Type: Select **Broadcast Media Format Transcoding**.
Template: Select a custom template. If there are none, create one first.
Digital Watermark: You can add a blind watermark to the video during transcoding for copyright protection.
Watermark: Add an image or text watermark to the video during transcoding.
Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.
Destination Path: Path of the transcoded video.
Destination File Name: Name of the destination file.
Queue: Currently, only the default queue `queue-1` is supported.

Creating an Video Montage Job

The video montage feature accurately extracts highlight segments from a video and outputs them as a new file for use in different scenarios, such as replay and preview.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Smart Editing** > **Video Montage** as the job type, click **Create Job**, and configure as follows:



Input Bucket Name: It is the current bucket by default.

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

Template: Select a custom template. If there are none, create one first.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Path of the destination file.

Destination File Name: Name of the destination file.

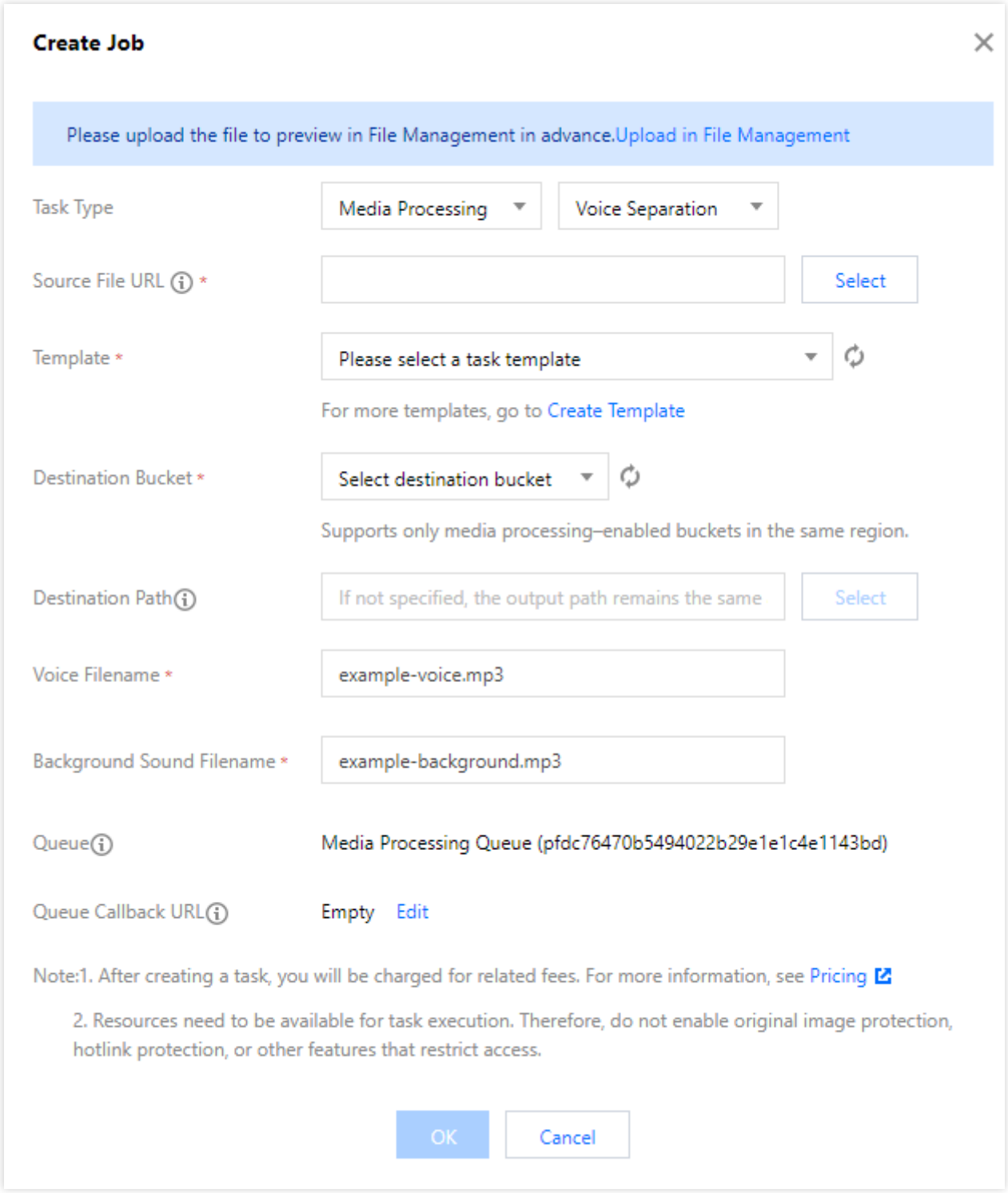
Queue: Currently, only the default queue `queue-1` is supported.

Creating a Voice/Sound Separation Job

The voice/sound separation feature separates the voice from the background sound in a video material to generate a new independent audio file. Then, you can apply artistic processing of other styles to the material without accompaniment and noise.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Smart Editing** > **Voice/Sound Separation** as the job type, click **Create Job**, and configure as follows:



Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

Template: Select a custom template. If there are none, create one first.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Path of the destination file.

Voice Filename: Name of the destination voice file.

Background Sound Filename: Name of the destination background sound file.

Queue: Currently, only the default queue `queue-1` is supported.

Creating a Text-to-Speech Job

The text to speech feature converts text into natural-sounding and smooth speeches for use in smart customer service and audiobook scenarios.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Smart Editing** > **Text to Speech** as the job type, click **Create Job**, and configure as follows:

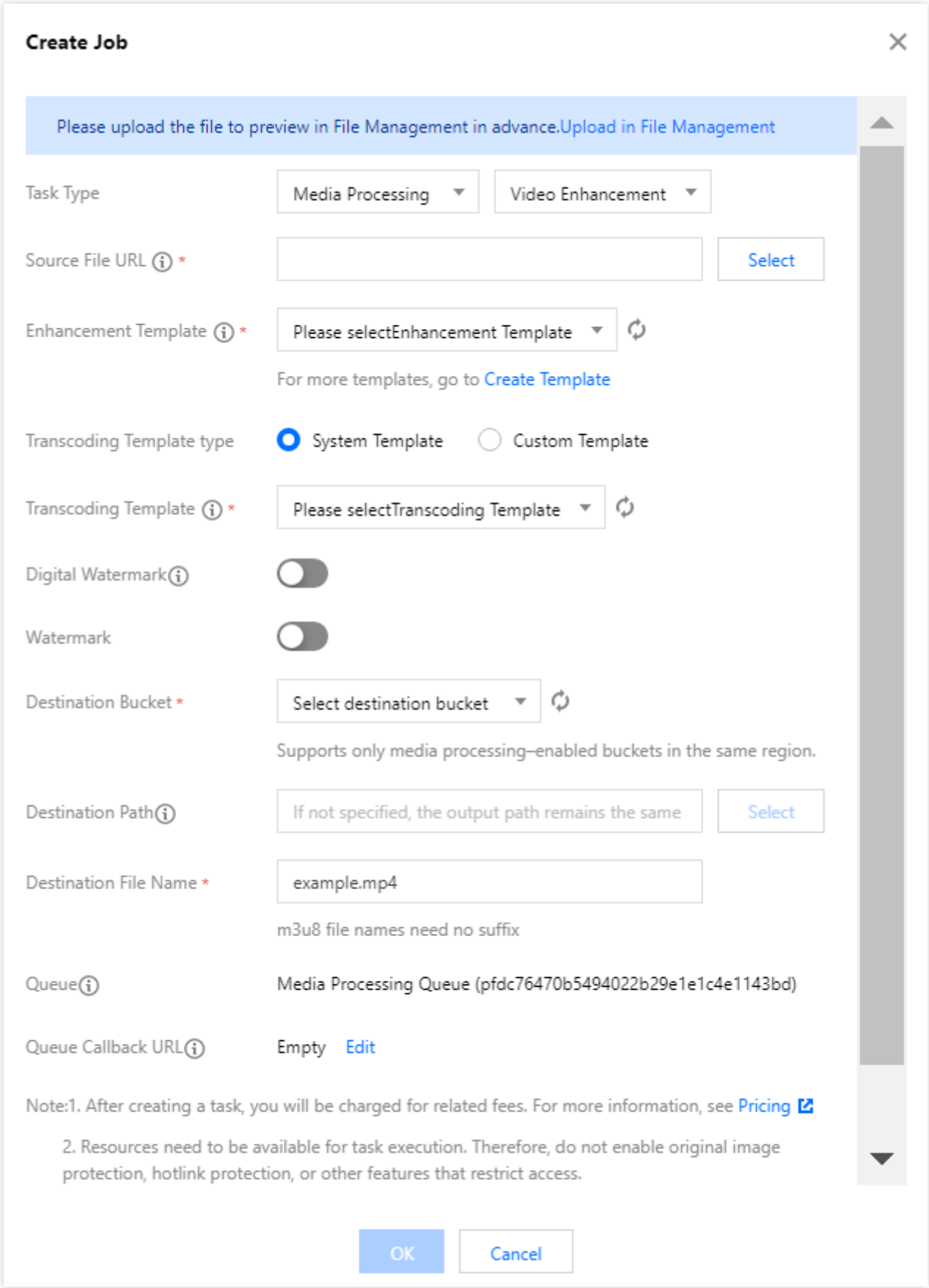
Source File URL: Enter the path of the source file, which cannot begin or end with `/` .
Template: Select a custom template. If there are none, create one first.
Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.
Destination Path: Path of the destination file.
Voice Filename: Name of the destination voice file.
Queue: Currently, only the default queue `queue-1` is supported.

Creating a Video Enhancement Job

Video enhancement is a video image quality improvement feature provided by CI. You can use it to enhance and beautify image colors and improve the image details.

Directions

1. Log in to the CI console and click **Bucket Management** to enter the bucket management page.
2. On the **Bucket Management** page, click the name of the desired bucket.
3. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
4. Select **Image Quality Optimization** > **Video Enhancement** as the job type, click **Create Job**, and configure as follows:



Note:

The input video must be shorter than 30 minutes.
Source File URL: Enter the path of the source file, which cannot begin or end with `/`.
Enhancement Template: Select a video enhancement template as needed.
Transcoding Template Type: Select **System Template** or **Custom Template**.
Transcoding Template: You can select a transcoding template and specify parameters such as resolution, bitrate, and format of the destination file.
Digital Watermark: You can add a blind watermark to the video during video enhancement for copyright protection.
Watermark: Add an image or text watermark to the video during video enhancement.
Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.
Destination Path: Storage path of the destination file.
Destination File Name: Name of the destination file.
Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating a Super Resolution Job

The super resolution feature reconstructs the details and local features of a video by recognizing its content and contour so as to generate a high-resolution video image through a series of low-resolution video images. It can be used in combination with video enhancement to remaster old videos.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Image Quality Optimization** > **Super Resolution** as the job type, click **Create Job**, and configure as follows:

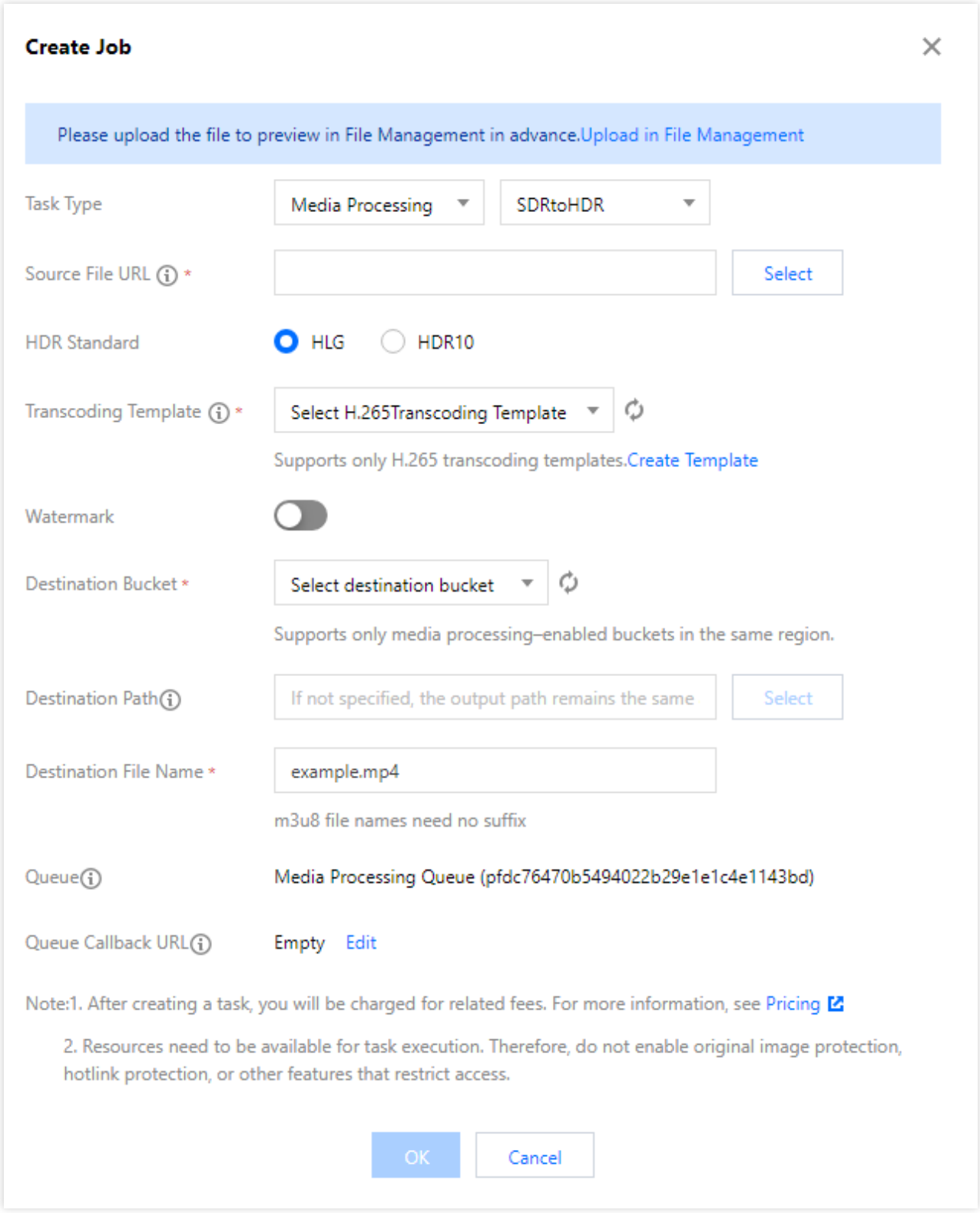
Source File URL: Enter the path of the source file, which cannot begin or end with `/`.
Super Resolution Template: Select the destination resolution template as needed.
Transcoding Template Type: Select **System Template** or **Custom Template**.
Transcoding Template: You can select a transcoding template and specify parameters such as resolution, bitrate, and format of the destination file.
Digital Watermark: You can add a blind watermark to the video during super resolution for copyright protection.
Watermark: Add an image or text watermark to the video during super resolution.
Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.
Destination Path: Storage path of the destination file.
Destination File Name: Name of the destination file.
Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating an SDR-to-HDR Job

SDR to HDR is a video dynamic range conversion feature provided by CI. You can use it to convert a standard dynamic range (SDR) video to a high dynamic range (HDR) video.

Directions

1. Log in to the CI console and click **Bucket Management** to enter the bucket management page.
2. On the **Bucket Management** page, click the name of the desired bucket.
3. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
4. Select **Image Quality Optimization** > **SDR to HDR** as the job type, click **Create Job**, and configure as follows:



Note:

The input video must be shorter than 30 minutes.

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

HDR Standard: Select HLG or HDR10.

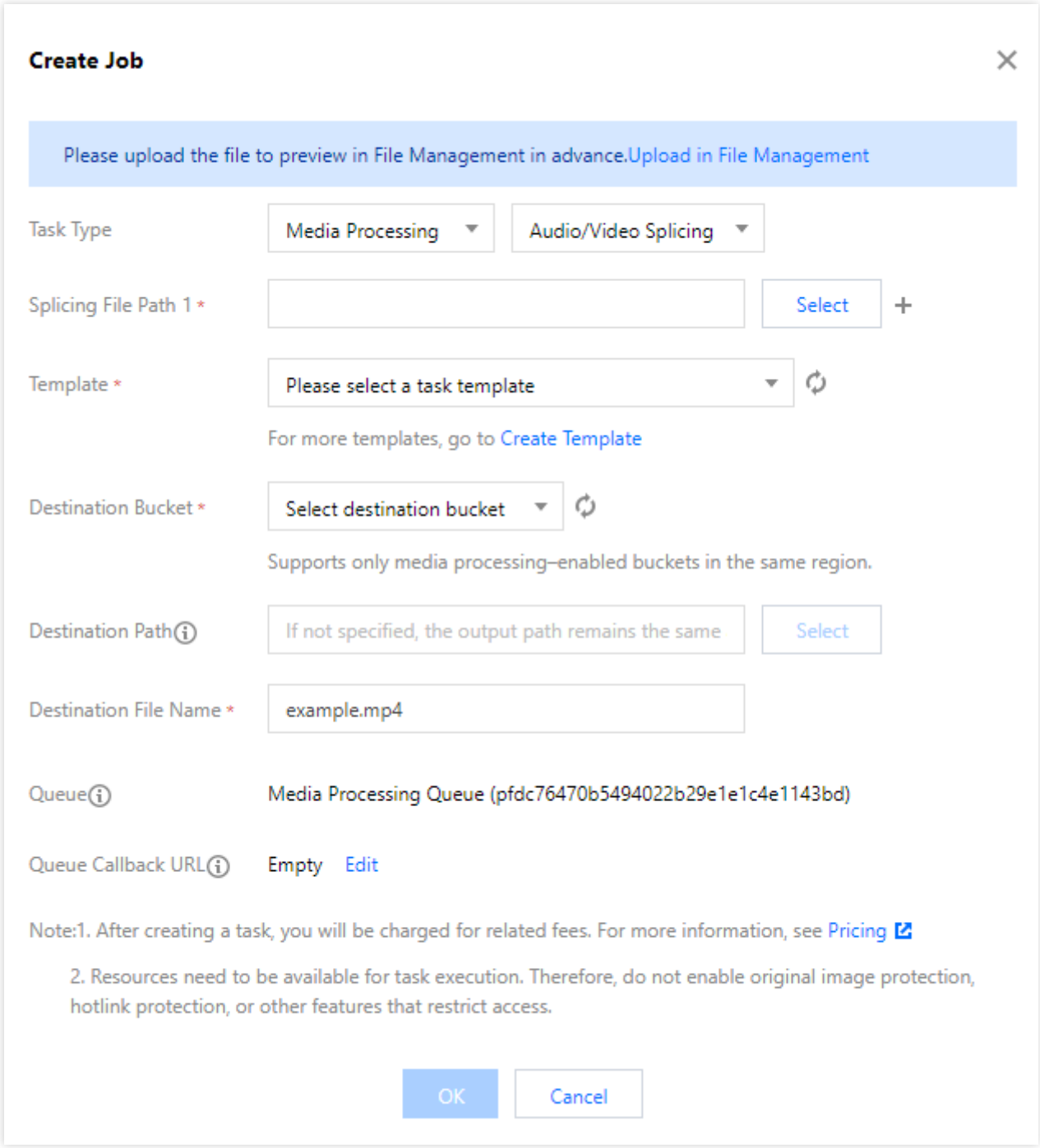
Transcoding Template: Select an H.265 transcoding template. If there are no templates, create an audio/video transcoding template and select H.265 as the encoding format. For more information on how to create a template and configure parameters, see Custom Template.
Watermark: Add an image or text watermark as needed.
Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.
Destination Path: Storage path of the destination file after the SDR to HDR conversion is completed.
Destination File Name: Name of the destination file.
Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating an Audio/Video Splicing Job

The video/audio splicing feature adds the specified video/audio segment at the beginning or end of a video/audio file to generate a new one.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Transcoding** > **Audio/Video Splicing** as the job type, click **Create Job**, and configure as follows:



Source File URL: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.

Template: Select a created audio/video splicing template.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the destination file.

Destination File Name: Name of the destination file.

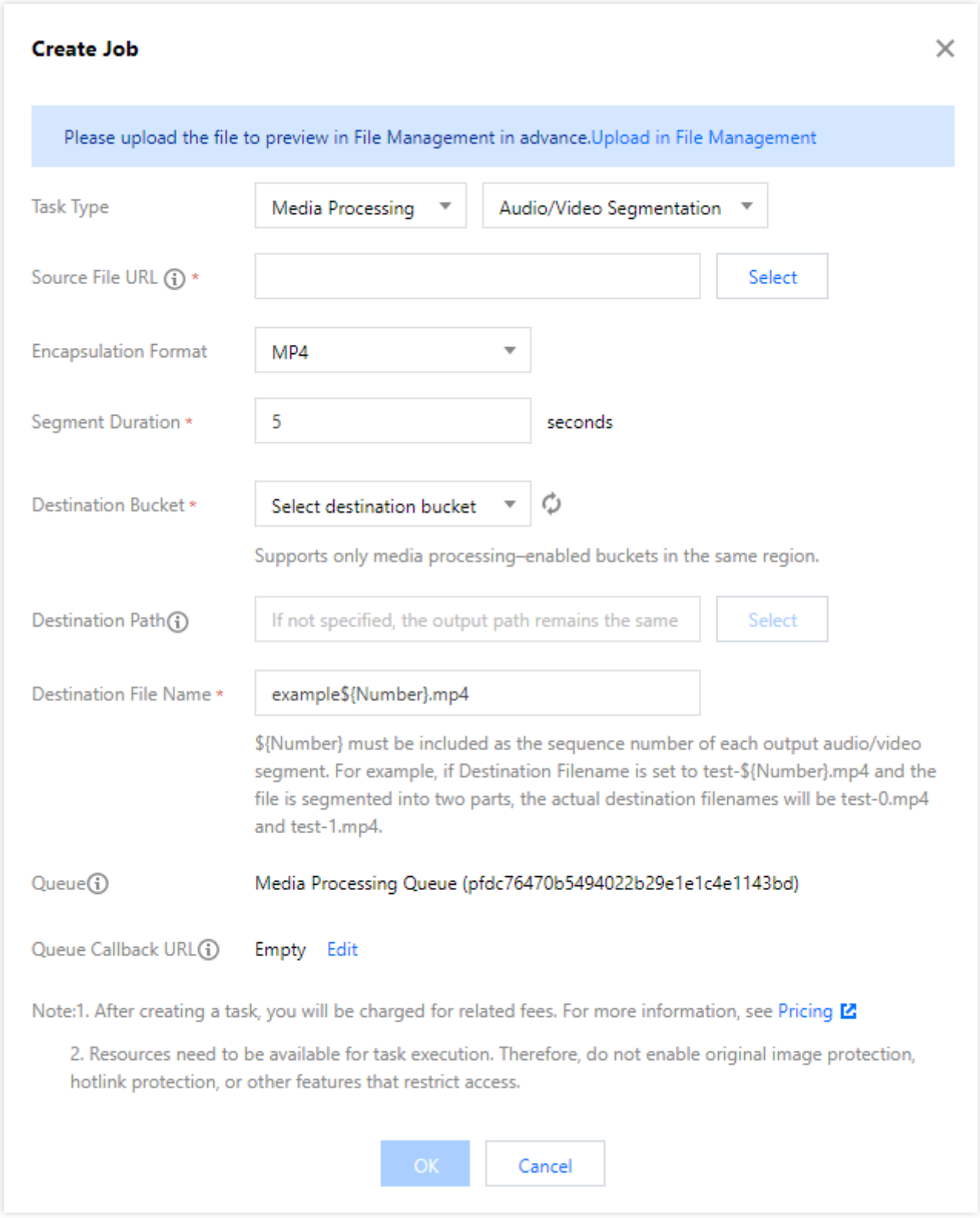
Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating an Audio/Video Segmentation Task

The audio/video segmentation feature can divide long and large audio/video files into several segments and remux the segments at the same time.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Transcoding** > **Audio/Video Segmentation** as the job type, click **Create Job**, and configure as follows:



Source File URL: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.

Segment Duration: Specify the duration of the output segment.

Container Format: Select the container format for the output audio/video.

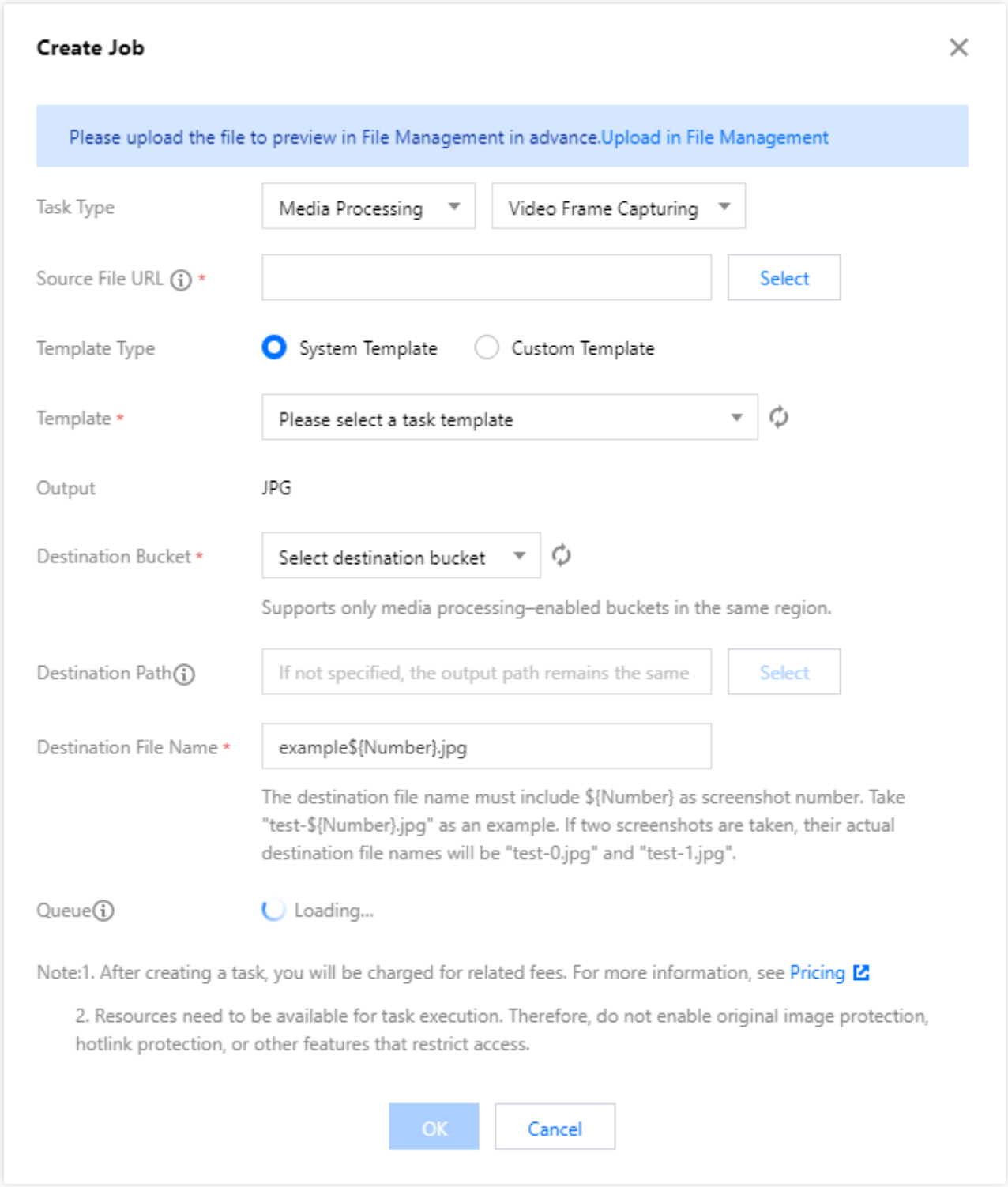
Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.
Destination Path: Storage path of the destination file.
Destination File Name: Name of the destination file.
Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating a Video Frame Capturing Job

Video frame capturing is a screencapturing feature provided by CI to capture the frames of a video at specified time points. After the job is enabled in the console, the output screenshots are in JPG format by default. If you enable captured frame compression, screenshots can be output in HEIF or TPG format.
Note:
A video frame capturing job can be created by template. You can customize the frame capturing start time, frame capturing interval, captured frames, destination image size, and destination format (captured frame compression needs to be enabled for this option) in a custom video frame capturing template.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Transcoding** > **Video Frame Capturing** as the job type, click **Create Job**, and configure as follows:



Source File URL: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.

Template Type: Select **System Template** or **Custom Template**. For more information, see Template.

Template: Select the specified template.

Output: If the video frame capturing job is enabled in the console, screenshots in JPG format will be output by default. If captured frame compression is used, screenshots in HEIF or TPG format can be output. If you use the video frame

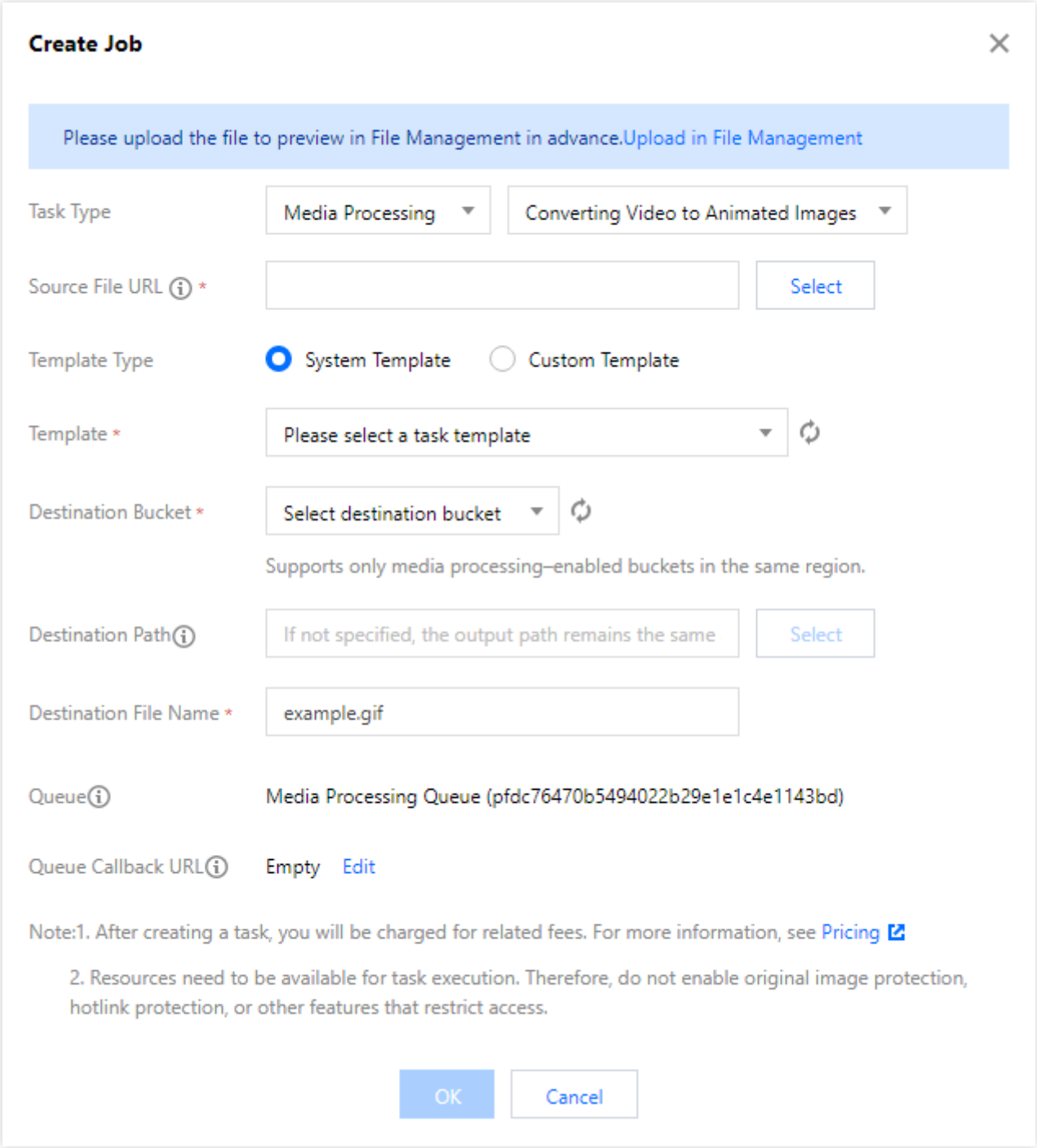
capturing API, you can choose to output JPG or PNG screenshots. For more information, see GenerateSnapshot in the API documentation.
Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.
Destination Path: Storage path of the video screenshots.
Destination File Name: Name of the output file. Note that as more than one files are output by **video frame capturing**, the destination file name must contain the ${Number} parameter as the sequence number of the screenshot. For example, if the destination file path is set to `test-${Number}.jpg` and the job captures two screenshots, the actual names of the destination files will be `test-0.jpg` and `test-1.jpg` .
Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating a Video-to-Animated Image Conversion Job

You can use the video to animated image conversion feature to convert a video to animated images.
Note:
A video-to-animated image conversion job can be created by template. You can customize the transcoding start time, transcoding duration, frame extraction method, destination animated image frame rate, destination animated image size, and destination format in a custom video-to-animated image conversion template.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Transcoding** > **Video-to-Animated Image Conversion** as the job type, click **Create Job**, and configure as follows:



Source File URL: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.

Template Type: Select **System Template** or **Custom Template**. For more information, see Template.

Template: Select the specified template.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the animated images.

Destination File Name: Name of the destination file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating an Intelligent Thumbnail Job

The intelligent thumbnail feature intelligently analyzes the quality, brilliance, and content relevance of video frames by understanding the video content with Tencent Cloud's advanced AI technologies. Then, it extracts optimal frames to generate thumbnails to make the content more engaging. |

Note:

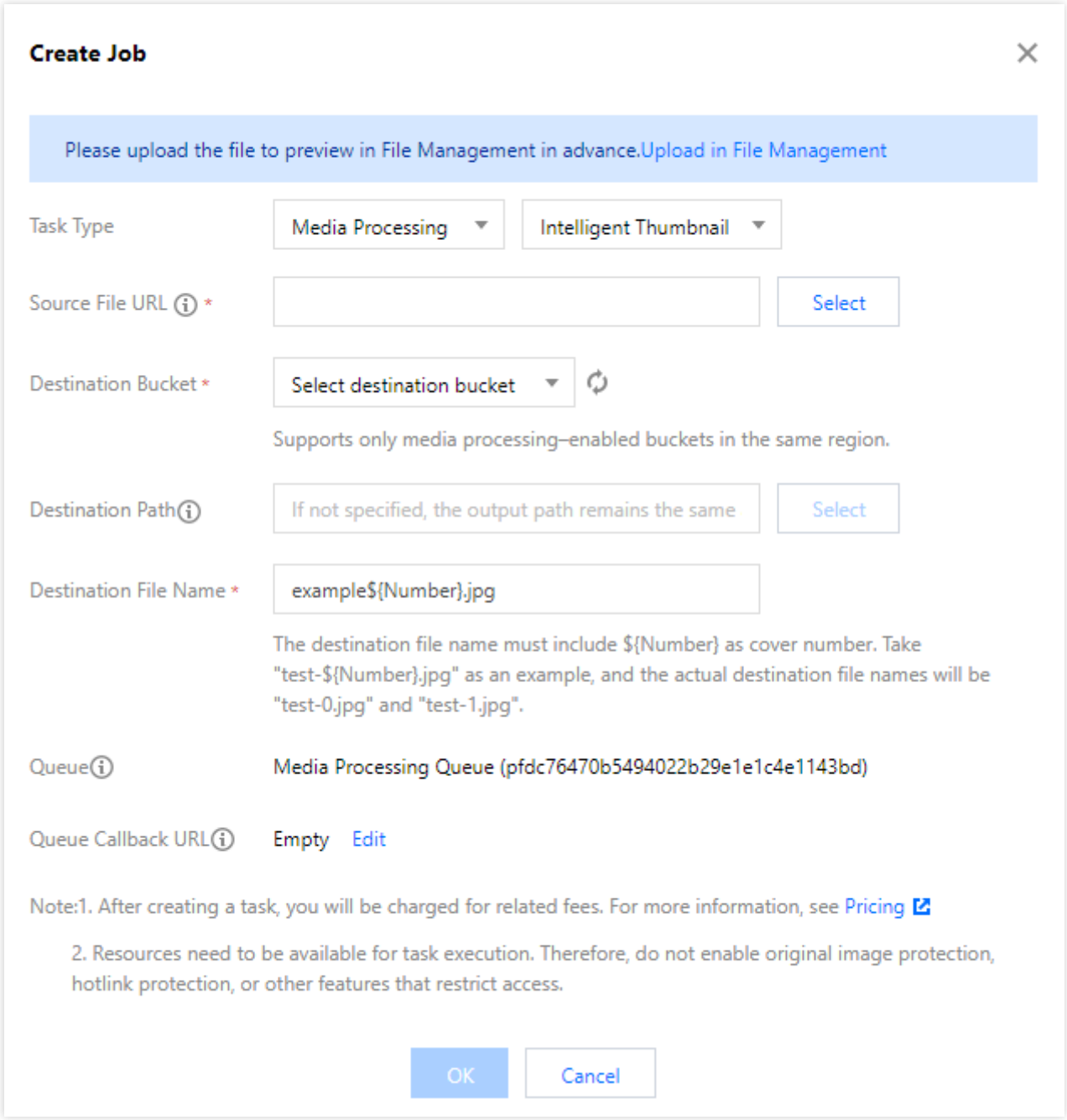
The intelligent thumbnail feature is a paid service and billed by the video duration. For billing details, see Billing Overview.

Three optimal keyframes will be output through intelligent analysis of each video file.

CI also provides an API for creating jobs, which can be configured based on parameters. For more information, see Submitting Audio/Video Transcoding Job in the API documentation.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Smart Editing** > **Intelligent Thumbnail** as the job type, click **Create Job**, and configure as follows:



Source File URL: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the smart thumbnails.

Destination File Name: Name of the destination file. Note that as more than one files are output by **video frame capturing**, the destination file name must contain the ${Number} parameter as the sequence number of the screenshot. For example, if the destination file path is set to `test-${Number}.jpg` and the job captures two screenshots, the actual names of the destination files will be `test-0.jpg` and `test-1.jpg`.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating a Digital Watermark Adding Job

This feature can embed an invisible watermark into a video for copyright protection.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Copyright Protection** > **Digital Watermark Adding** as the job type, click **Create Job**, and configure as follows:

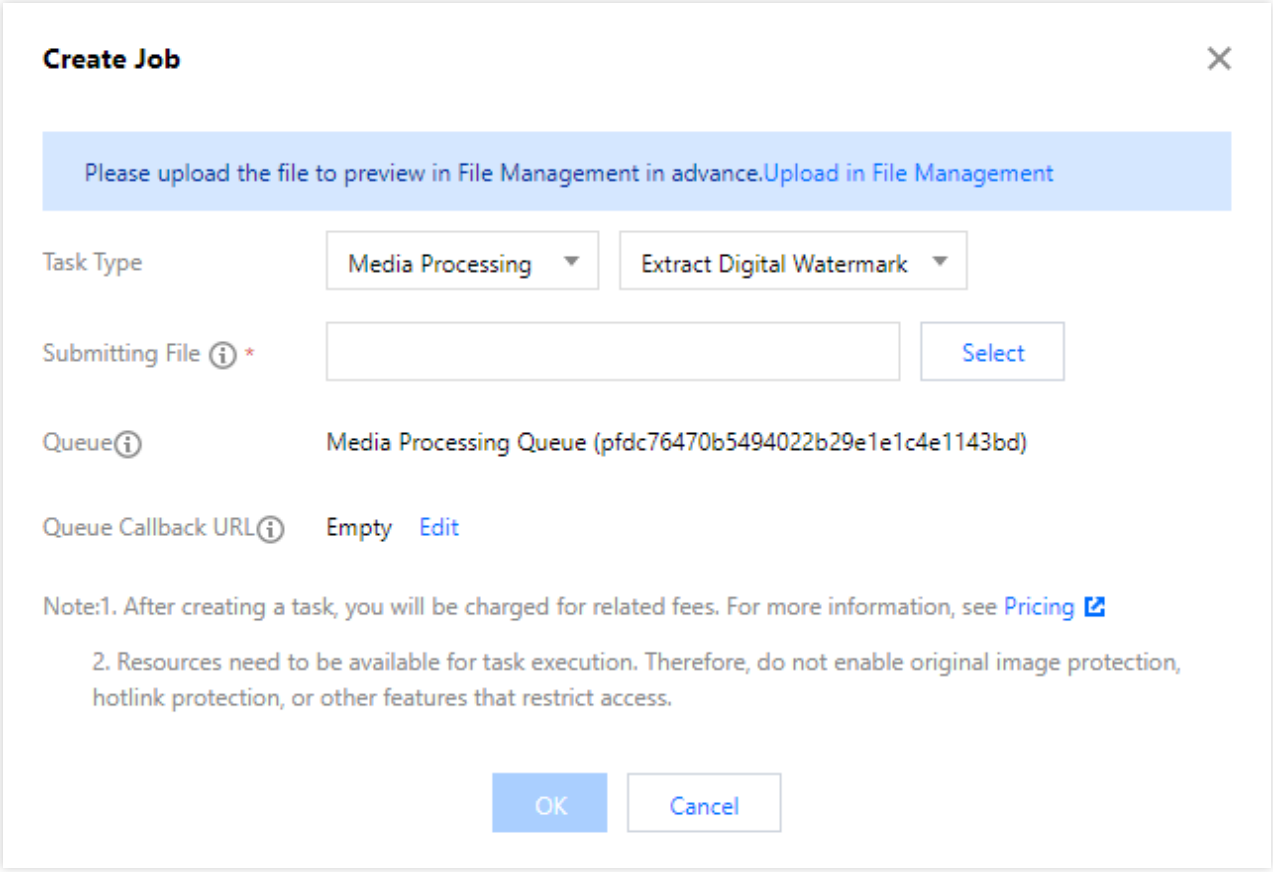
Source File URL: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.
Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.
Digital Watermark Content: Enter the custom digital watermark content for copyright traceability.
Destination Path: Storage path of the smart thumbnails.
Destination File Name: Name of the destination file.
Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating a Digital Watermark Extraction Job

You can use the CI's media processing service to extract the digital watermark from a watermarked video.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Media Processing** tab at the top.
5. Select **Copyright Protection > Digital Watermark Extraction** as the job type, click **Create Job**, and configure as follows:



Source File: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.
Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Creating an Image Processing Job

Image processing supports flexible image editing, such as rotation, cropping, transcoding, and scaling. It provides multiple image downsizing solutions like Guetzli compression, TPG transcoding, and HEIF transcoding, as well as diversified copyright protection solutions like image/text/blind watermarking. This meets your image processing needs in different business scenarios.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click the name of the desired bucket.
4. Click **Data Processing Workflow** > **Job** on the left sidebar, and select the **Image Processing** tab at the top.
5. Click **Create Job**, select **Image Processing** as the job type, and configure as follows:

Source File URL: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.

Template: Select the specified template.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the image processing result.

Destination File Name: Name of the destination file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see Queue.

Workflow
Workflow

Last updated：2024-01-31 16:44:15

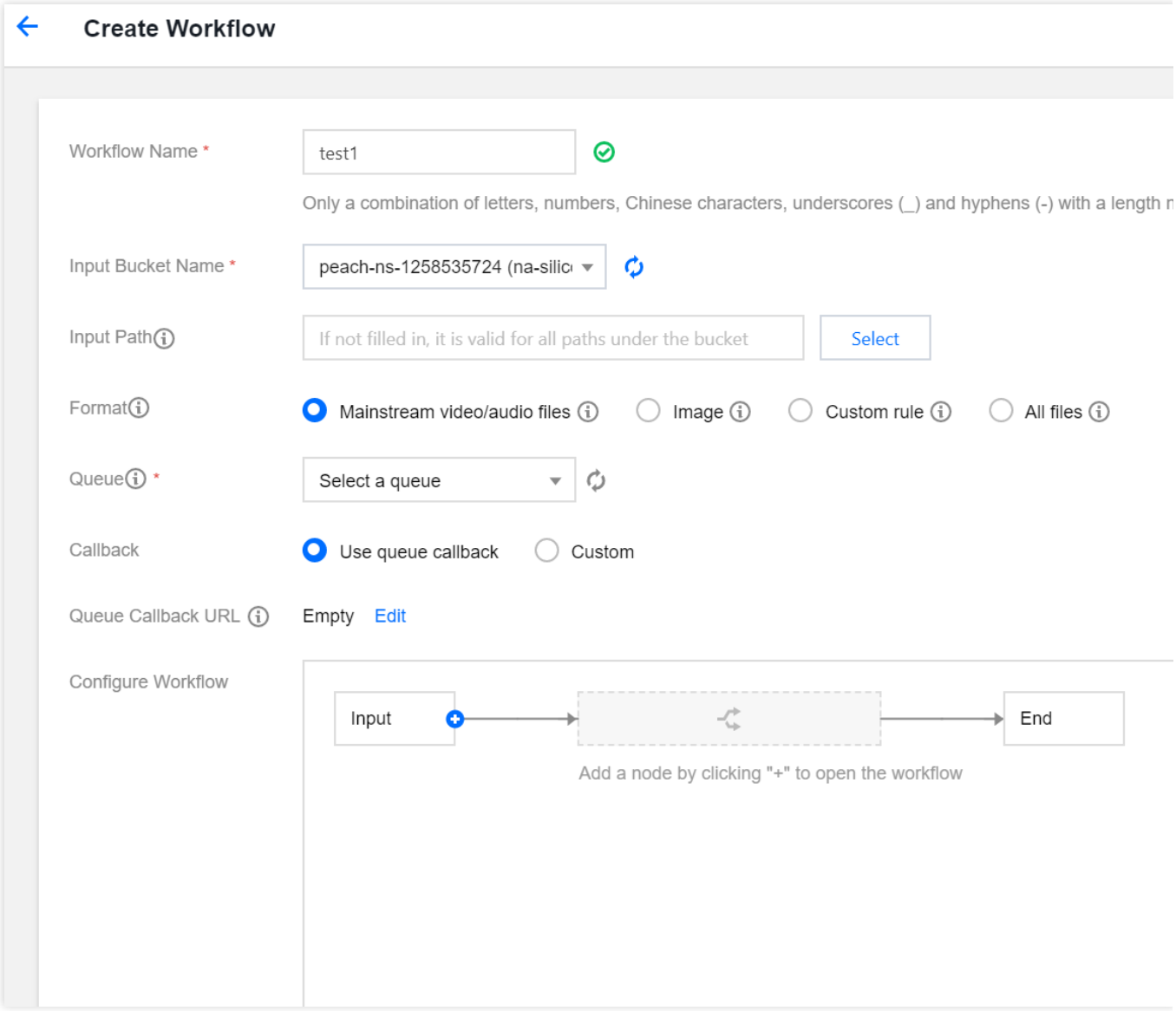
Overview

With a media processing workflow in CI, you can quickly and flexibly create video processing flows as needed. A workflow is bound to a path of an input bucket. When a video file is **uploaded** to the path, the media workflow will be **automatically triggered** to perform the specified operation, with the processing result automatically saved to the specified path of the destination bucket.
You can use a data processing workflow to implement the following features: **audio/video transcoding (including top speed codec transcoding and broadcast media format transcoding)**, **video frame capturing**, **video-to-animated image conversion**, **intelligent thumbnail**, **audio/video splicing**, **voice separation (also known as voice/sound separation)**, **text to speech**, **speech recognition**, **highlights generation (also known as video montage)**, **adaptive multi-bitrate**, **SDR to HDR**, **video enhancement**, **super resolution**, **audio/video segmentation**, **custom function**, and **image processing**.
Note:
Currently, workflows can process 3GP, ASF, AVI, DV, FLV, F4V, M3U8, M4V, MKV, MOV, MP4, MPG, MPEG, MTS, OGG, RM, RMVB, SWF, VOB, WMV, WEBM, MP3, AAC, FLAC, AMR, M4A, WMA, and WAV files. When initiating a media processing request, you must enter the complete file name and extension; otherwise, the format cannot be recognized and processed.
Currently, the workflow feature can manipulate existing files and files being uploaded. To perform media processing operations on existing data in the cloud, use the batch processing job feature as described in Triggering Job (Workflow).

Directions

Creating workflow

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
4. Click **Job and Workflow** on the left sidebar and select the **Workflow Management** tab at the top of the page.
5. Click **Create Workflow**.
6. On the **Create Workflow** page, configure the following items:



Workflow Name: It is required and can contain up to 128 letters, digits, underscores (_), and hyphens (-).
Input Bucket Name: It is the current bucket by default.
Input Path: It is optional and must start and end with `/`. If it is not specified, the workflow will be triggered for all paths in the input bucket. After the media workflow is enabled, when a video file is uploaded to this path, the workflow will be automatically triggered.
Format: Select the default audio/video/image file filter rule or a custom workflow rule. You can also select all files to process all objects in the bucket.
Queue: It is required. When you activate the service, the system will automatically create a user queue for you. When you submit a job, the job will be arranged in the queue first and executed in sequence according to the priority and order of submission.
Callback: You can use the queue callback, i.e., callback URL bound to the queue. To modify it, go to the corresponding queue list.

Configure Workflow: Click **+** on the right to add any of the following nodes: **audio/video transcoding (including top speed codec transcoding and broadcast media format transcoding)**, **video frame capturing**, **video-to-animated image conversion**, **intelligent thumbnail**, **audio/video splicing**, **voice separation**, **highlights generation**, **HLS adaptive multi-bitrate**, **SDR to HDR**, **video enhancement**, **super resolution**, **audio/video segmentation**, **custom function**, and **image processing**. You need to configure at least one job node in a workflow and set the destination bucket, filename (see Workflow Variable Description), path, and job template for each job node. For more information on templates and how to set them, see Template.

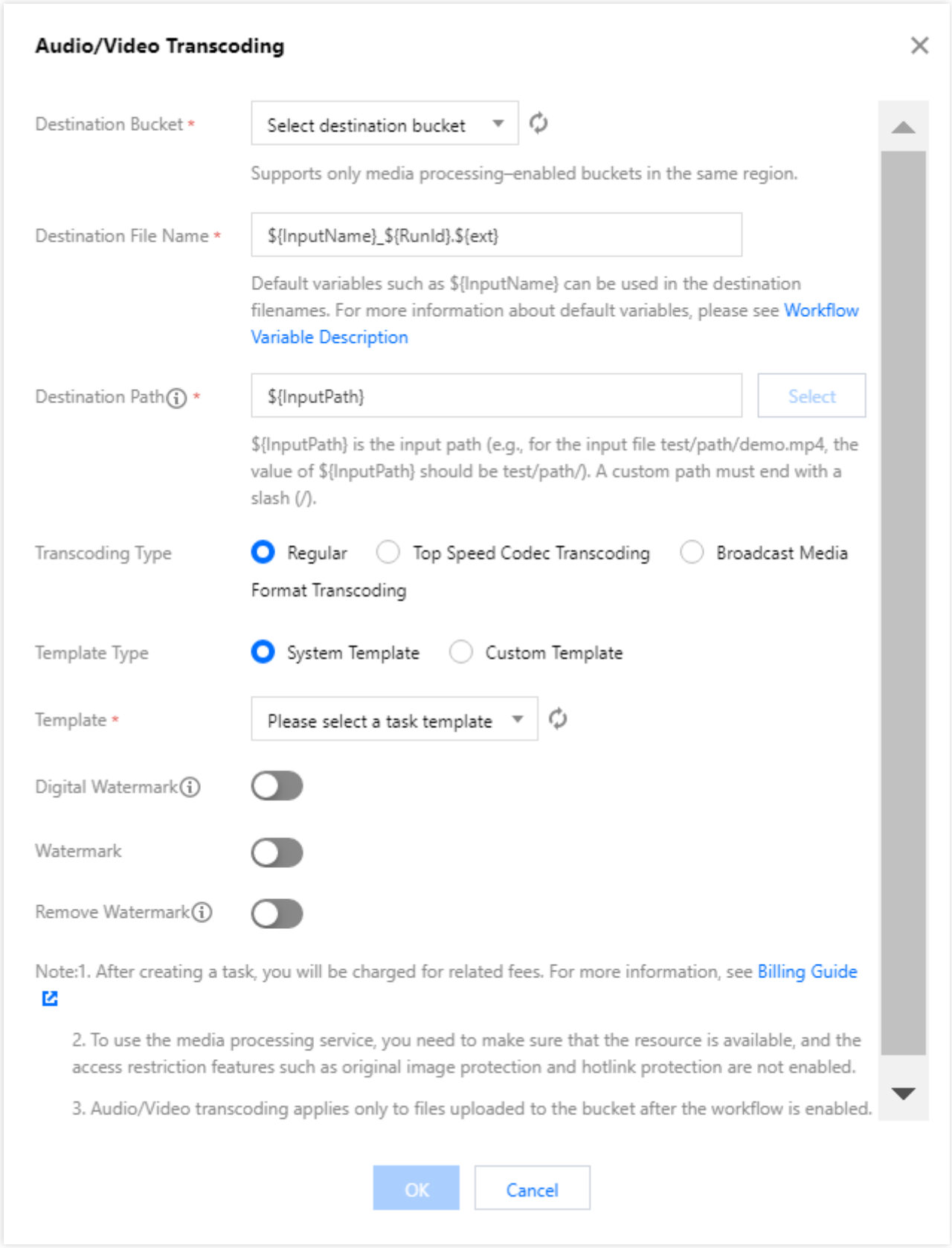
Audio/Video transcoding

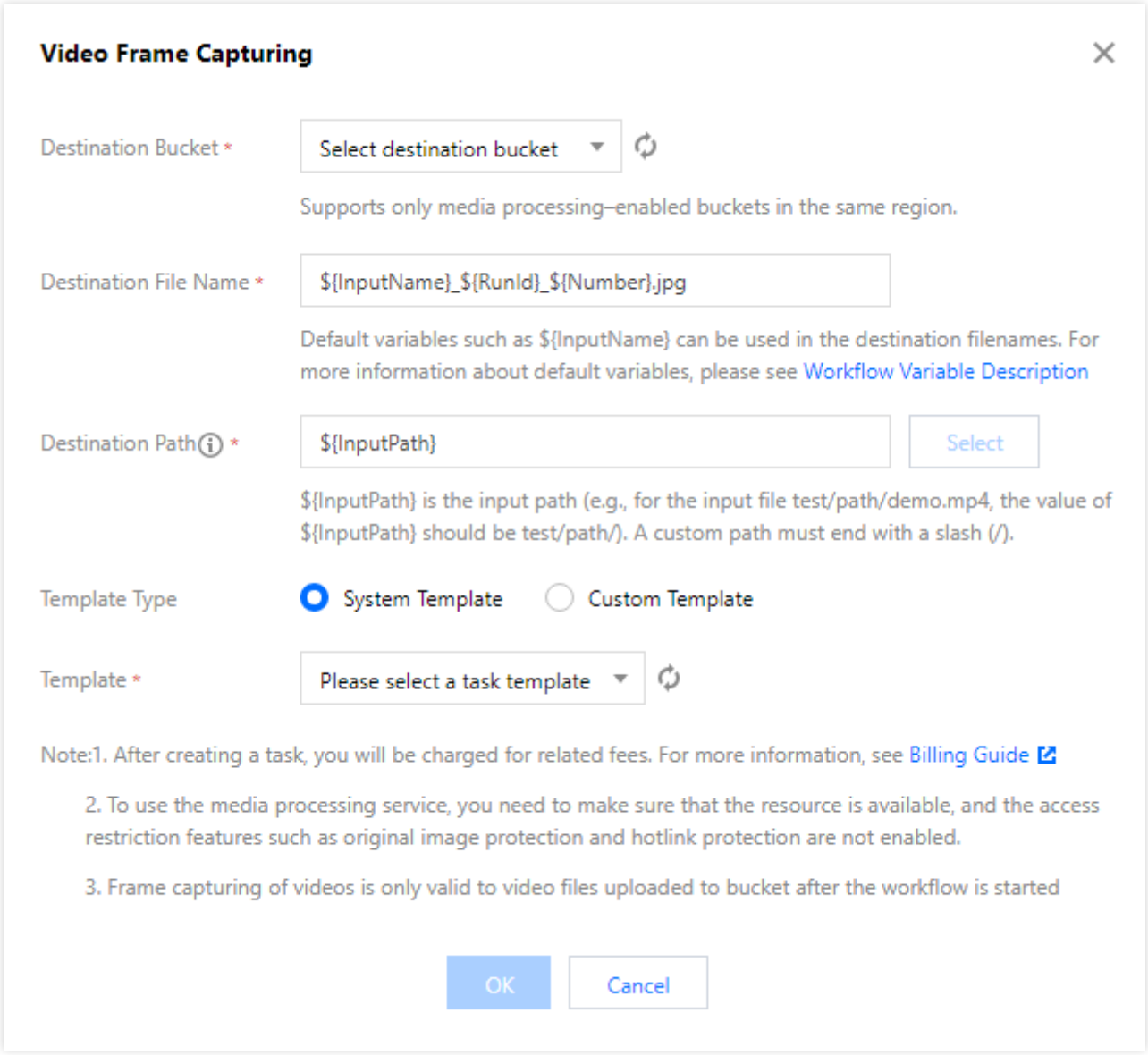
Video frame capturing

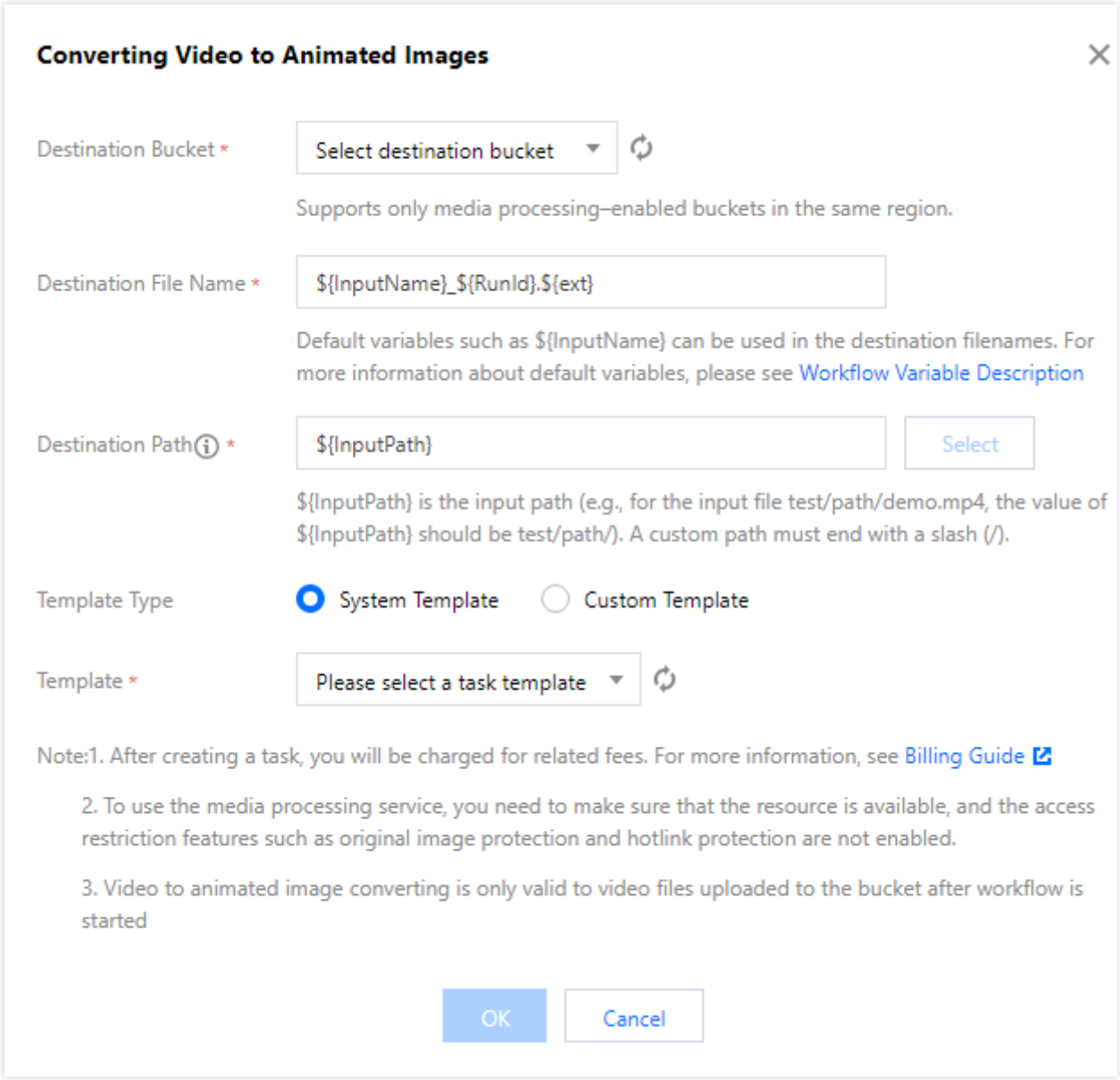
Video-to-animated image conversion

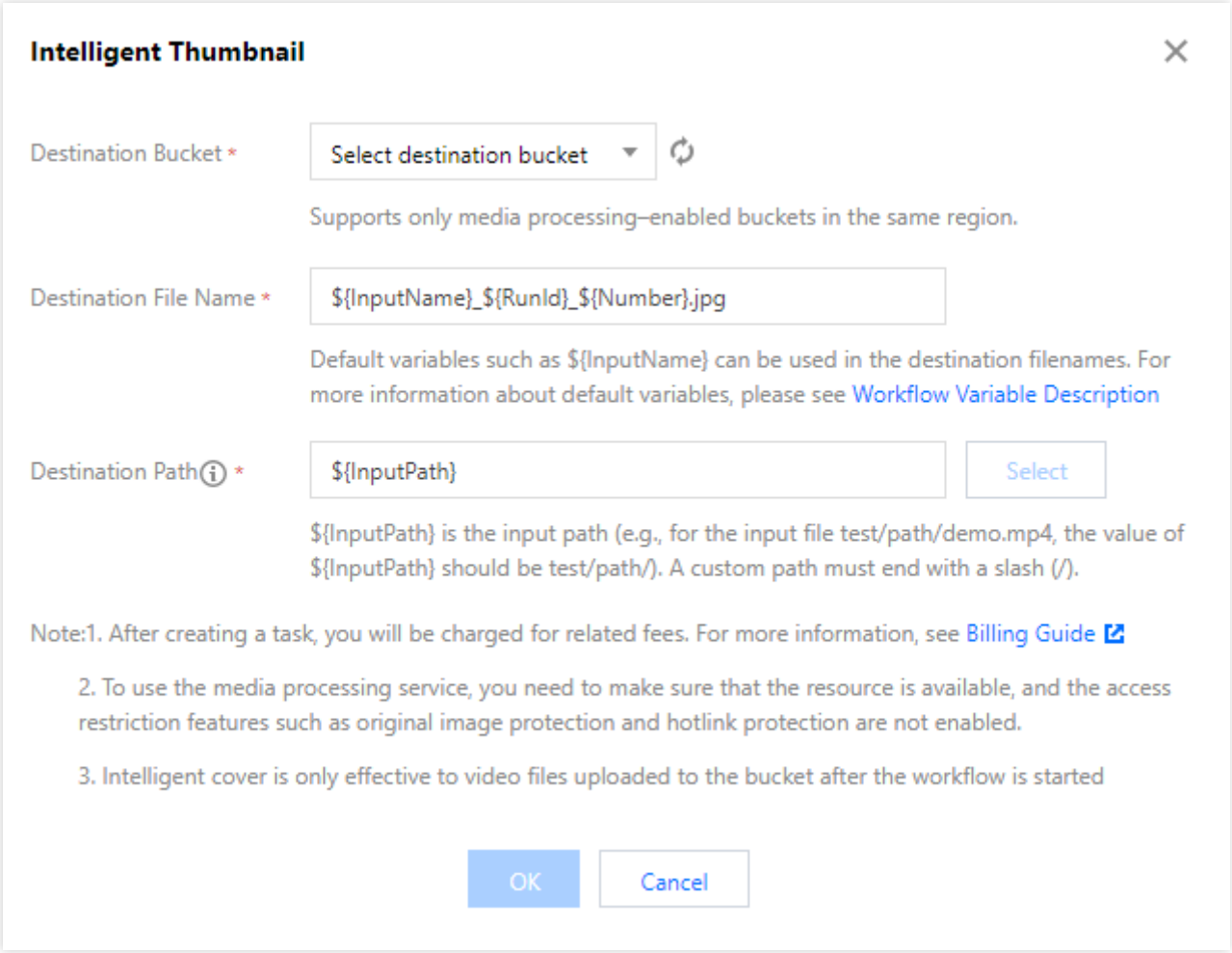
Intelligent thumbnail

Audio/Video splicing

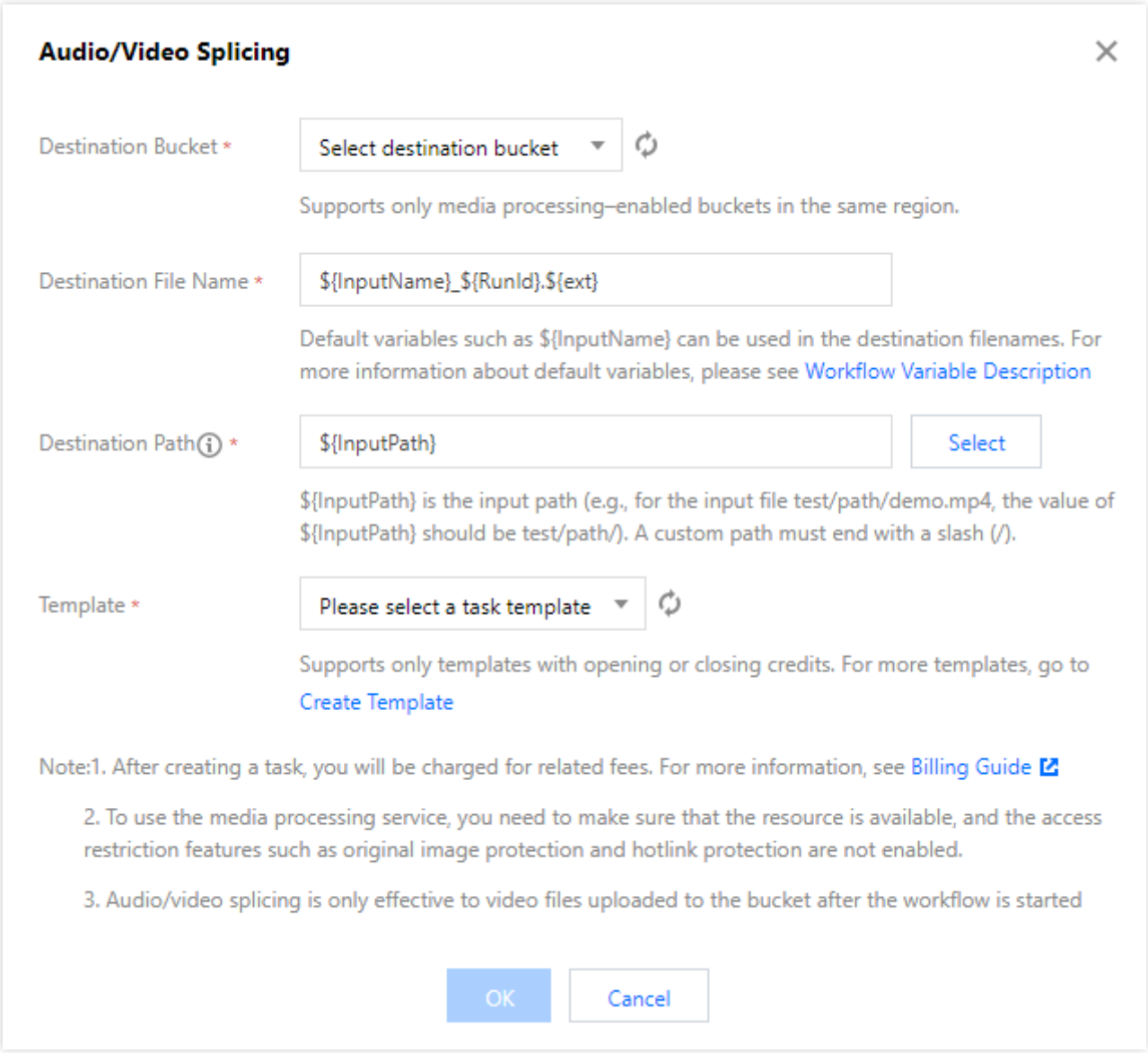








Description: The intelligent thumbnail feature understands the video content with the aid of Tencent Cloud's advanced AI technologies to intelligently extract three optimal frames.



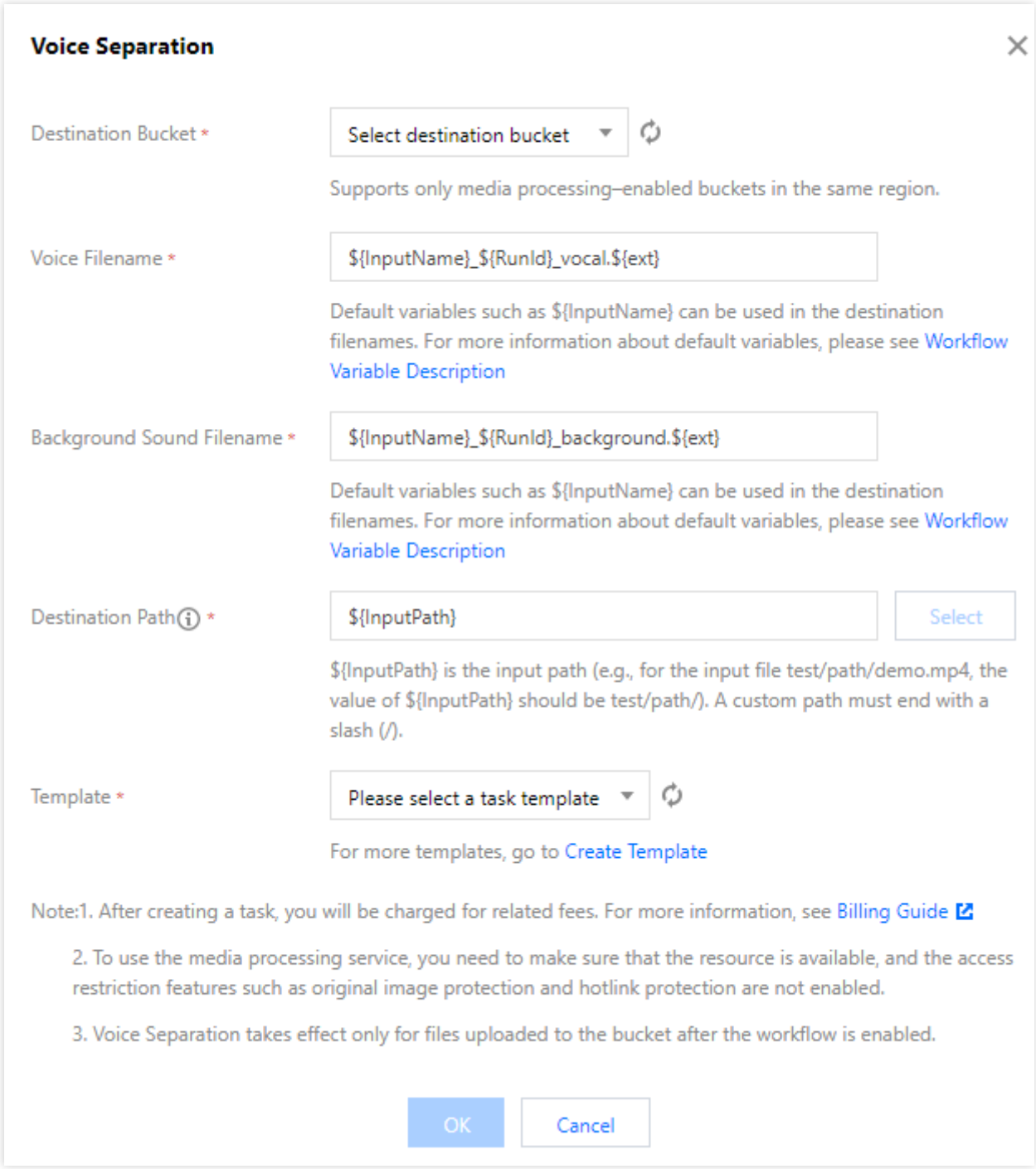
Voice separation

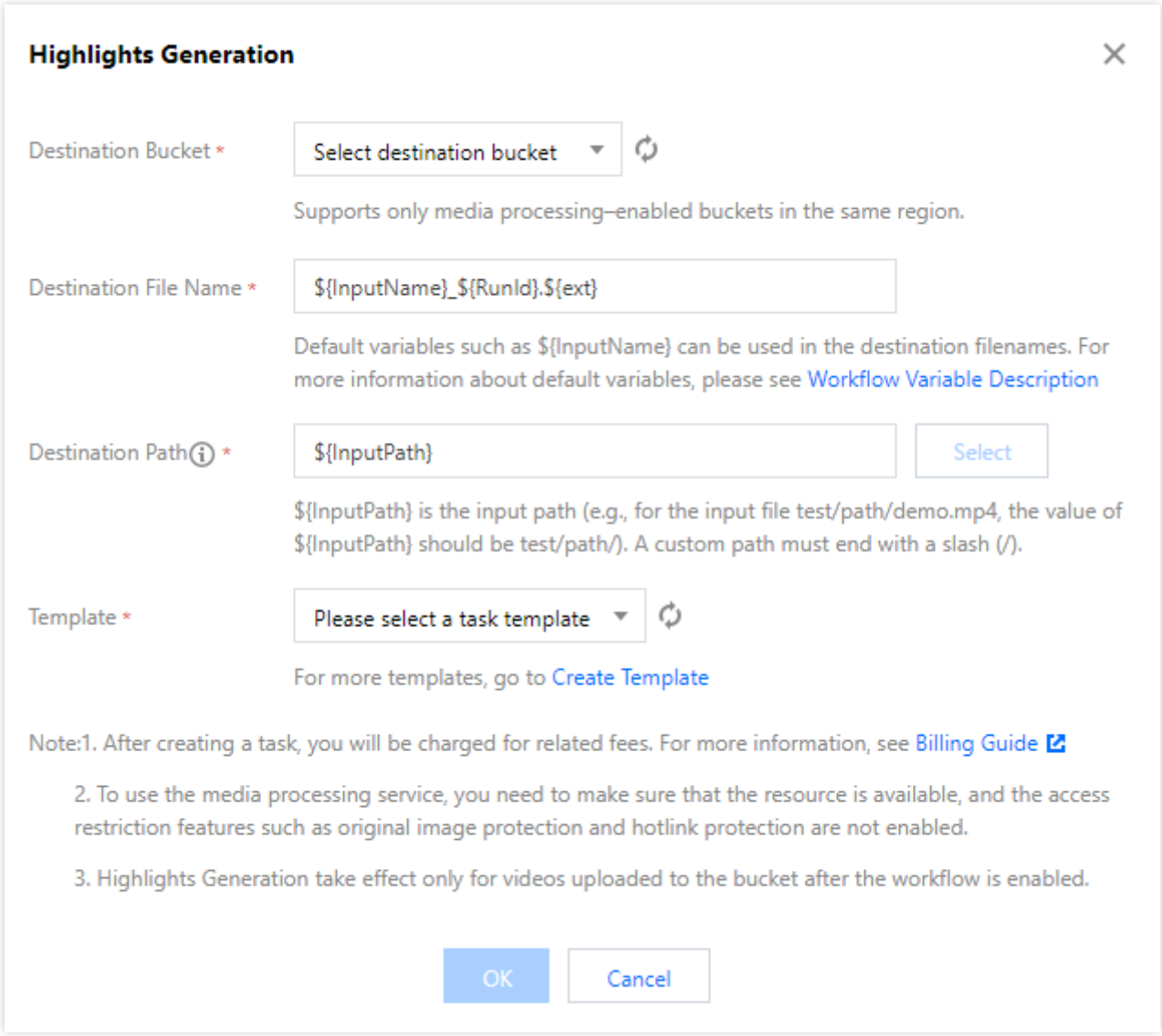
Highlights generation

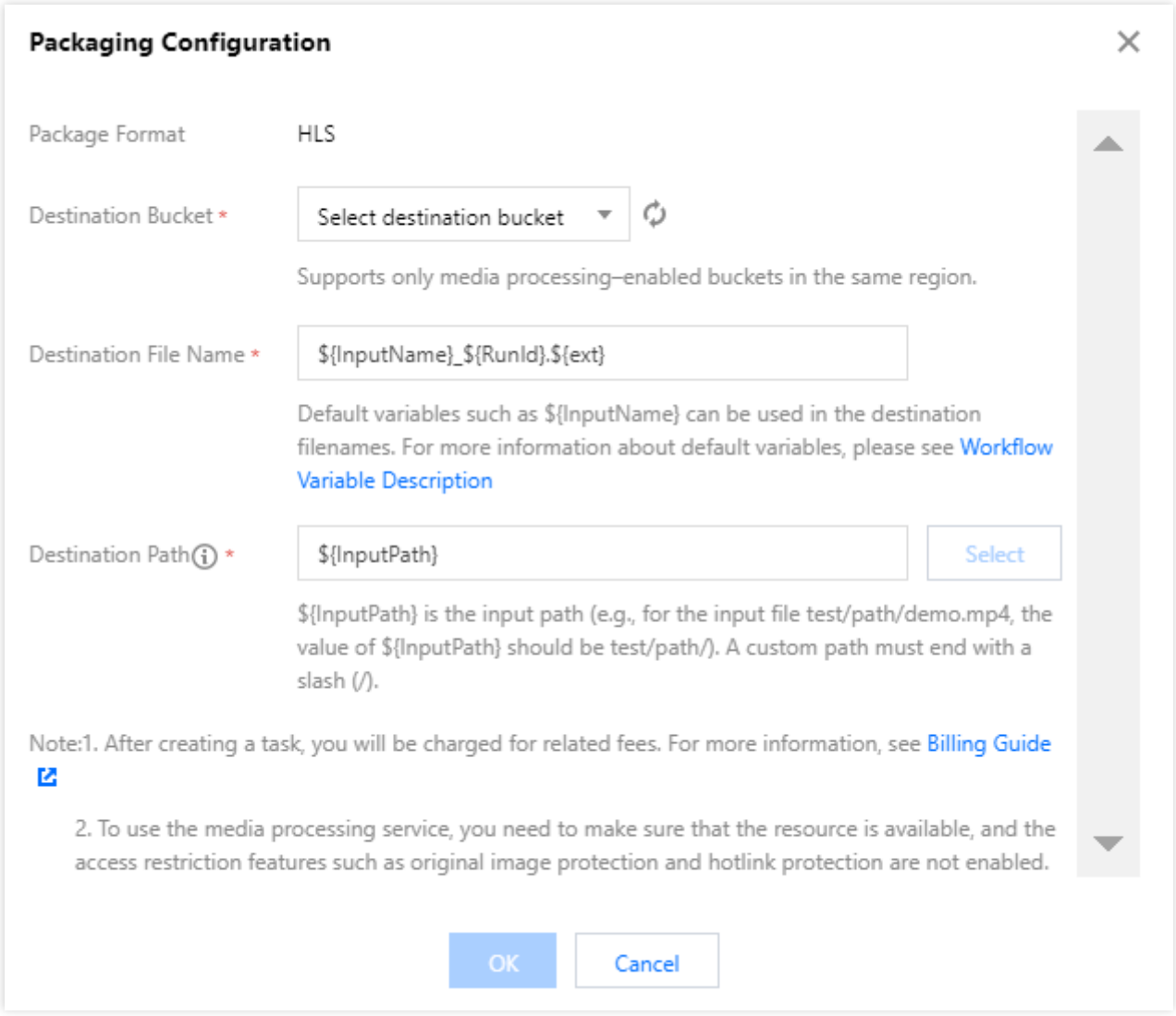
Adaptive bitrate streaming

SDRtoHDR

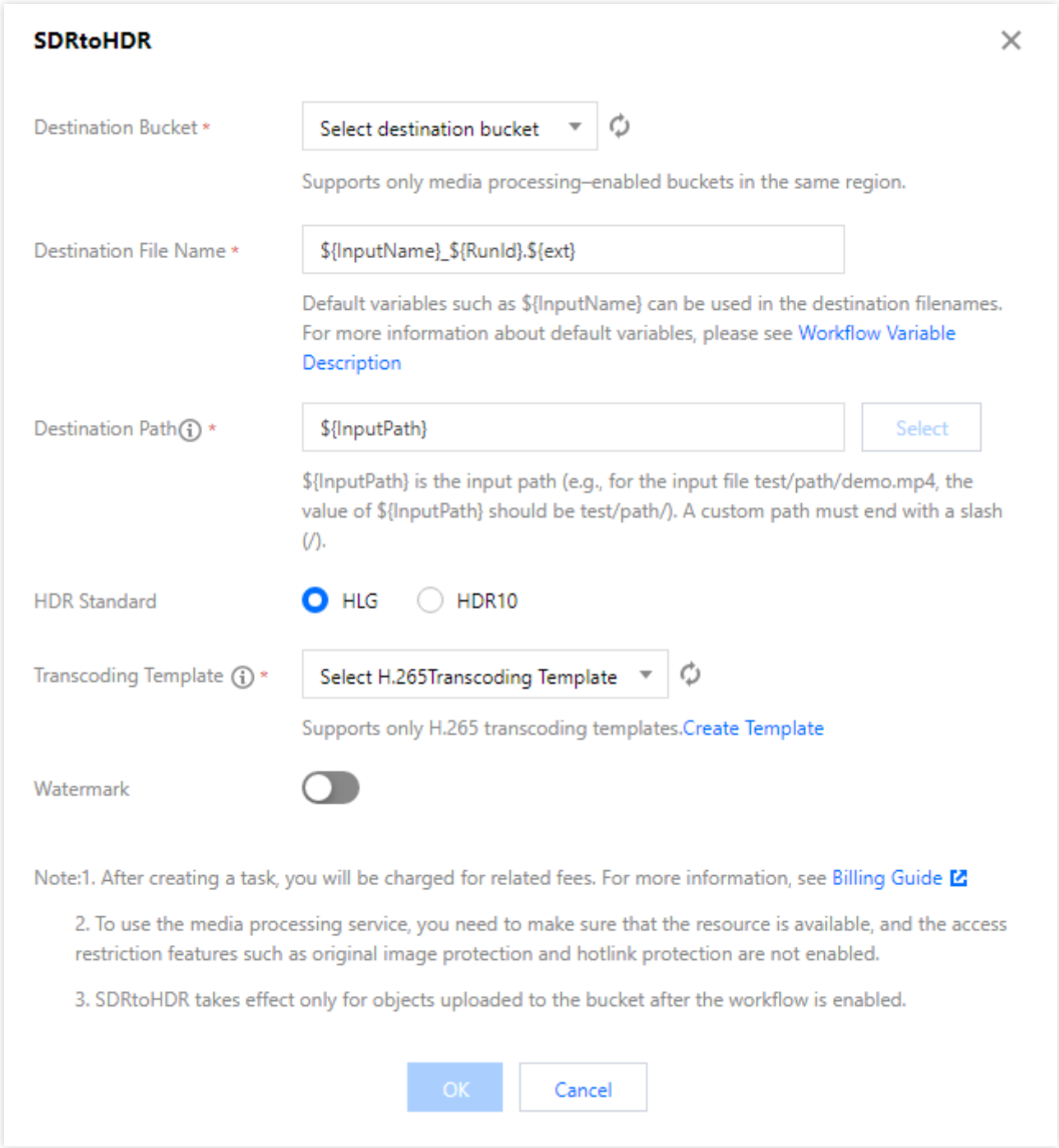
Video enhancement







Description: The HLS adaptive multi-bitrate feature encapsulates multiple files with multiple bitrates and audio tracks into one HLS or DASH multi-bitrate adaptive video file.



Super resolution

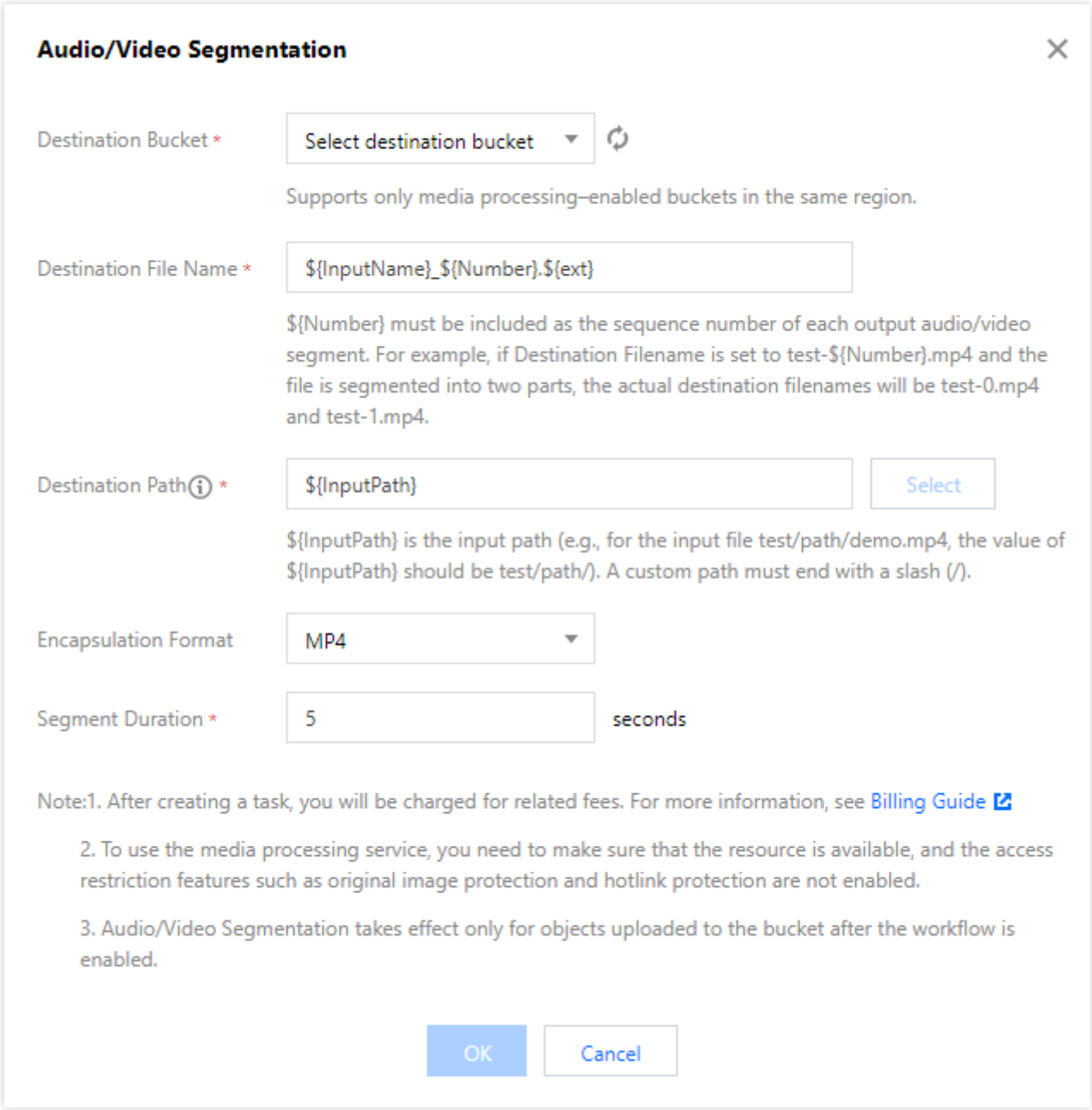
Audio/Video segmentation

Text to speech

Speech recognition

Custom function

Image processing



7. After confirming that the configuration is correct, click **Save**.

Workflows are disabled by default. To enable a workflow, click the toggle in the **Enable** column. Once enabled, the workflow will take effect in five minutes. Then, it will automatically perform media processing operations on video files uploaded subsequently. After processing files, it will output the new generated files to the specified file path.

Managing workflow

You can view the list of created workflows on the workflow management page.

The workflow list displays the names, IDs, input paths, creation times, and statuses of workflows. You can search for workflows by name and ID to view, edit, or delete specified workflows.

Enable: Once a workflow is enabled, video files uploaded to the specified path in the input bucket will be automatically processed according to the workflow configuration. You can click the toggle again to pause the workflow.

Note:

Workflows are disabled by default. To enable a workflow, click the toggle in the **Enable** column. Once enabled, the workflow will take effect in five minutes.

Details: You can view the configuration details of the current workflow.

Execution Instance: You can view the workflow execution status and time by time.

More:

Click **More** > **Edit** in the **Operation** column to enter the **Edit Workflow** page, where you can modify the workflow configuration.

Click **More** > **Delete** in the **Operation** column to delete the workflow.

Note:

You cannot edit or delete an enabled workflow.

Viewing workflow execution instance

An execution instance will be generated after a workflow is executed for each video file. The execution instance page displays the source file address, workflow execution status, and execution time.

1. Go to the workflow management page and click **Workflow Instance** in the **Operation** column of the target workflow to enter the execution instance list page.
2. On the execution instance page, click **Details** in the **Operation** column of the target instance.
3. On the **Workflow Instance Details** page, you can view the job ID, execution status, start time, and end time of each workflow node.

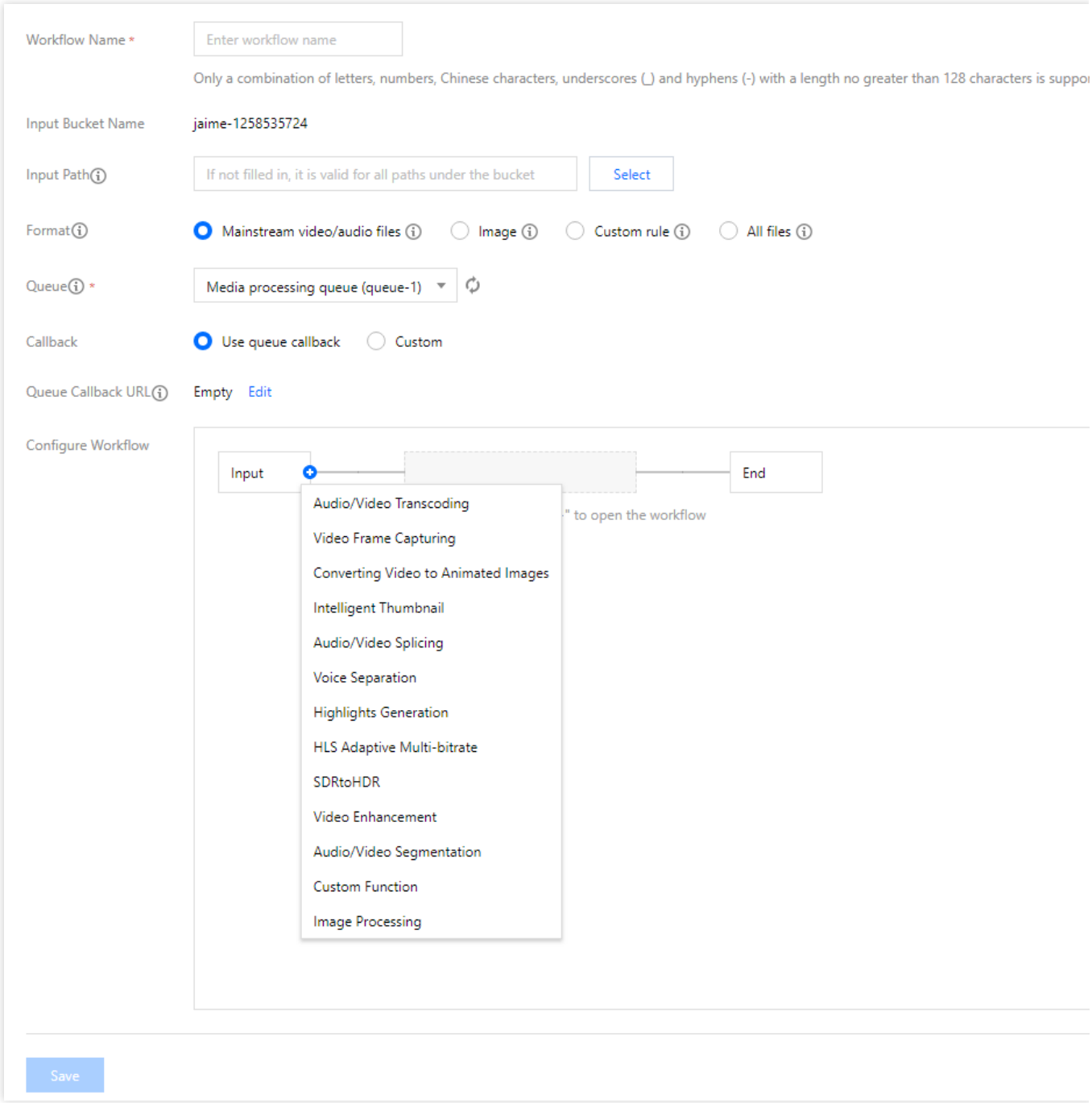
Testing workflow

After a workflow is created, it can be automatically triggered for files uploaded to the specified bucket or manually triggered for existing files in the bucket.

1. Go to the workflow management page, find the target workflow, and click **Test** to quickly verify the workflow.
2. During the test, select the file for which to trigger the workflow and click **OK** to immediately trigger and execute the workflow.

You can view the workflow execution status on the workflow execution instance page.

You can view the workflow execution status on the execution instance page.



Workflow Variable Description

Workflows support rendering destination file names and URLs with the following variables:

Variable Name	Description
InputName	Filename of the input file (without file extension)
InputNameAndExt	Filename of the input file (with file extension)

InputPath	File input path
RunId	Execution instance ID
Ext	Destination file format
Number	Destination file number

Sample

If the names of your input files are `test1.mp4` and `test2.mp4`, and you want to convert them to the FLV format (the final filenames will be `test1.flv` and `test2.flv`), then set the parameter format of the destination filename to `${InputName}.${Ext}`.
If the parameter format of the destination filename is set to `${InputNameAndExt}_${RunId}.${Ext}`:
When the workflow generates two instances (`000001` and `000002`) during execution, the final filenames will be `test1.mp4_000001.flv` and `test2.mp4_000002.flv`.

Batch Data Processing

Last updated：2024-01-31 16:44:15

Overview

CI supports batch processing of files stored in COS. You can specify a workflow or an independent job node as the operation of batch data processing.

Directions

Creating batch data processing job

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
4. On the left sidebar, click **Job and Workflow** > **Batch Data Processing**.
5. Click **Create Batch Data Processing Job** to enter the creation page.
6. On the **Create Workflow** page, configure the following items:

Job Name: It is required and can contain up to 128 letters, digits, underscores (_), and hyphens (-).
Input Bucket Name: It is the current bucket by default.
Scope: Determine the data scope for batch processing, which is the current bucket file list by default.
Time: Select the default audio/video/image file filter rule or a custom workflow rule. You can also select all files to process all objects in the bucket.
Prefix: Scan files with the specified prefix to perform operations specified in the processing settings.
Processing Type: Set operations for data within the specified range. You can select a workflow or independent node. For configurations for independent nodes, see Job.
Select Workflow: Select the workflow to be executed.

Viewing batch data processing job result

1. Go to the batch data processing page and click **Execution Result** in the **Operation** column of the target workflow.
2. If the processing type is workflow, clicking **Execution Result** will redirect you to **Execution Record** > **Workflow Execution Result**.
3. If the processing type is independent node, clicking **Execution Result** will redirect you to **Execution Record** > **Job Result**.

Template

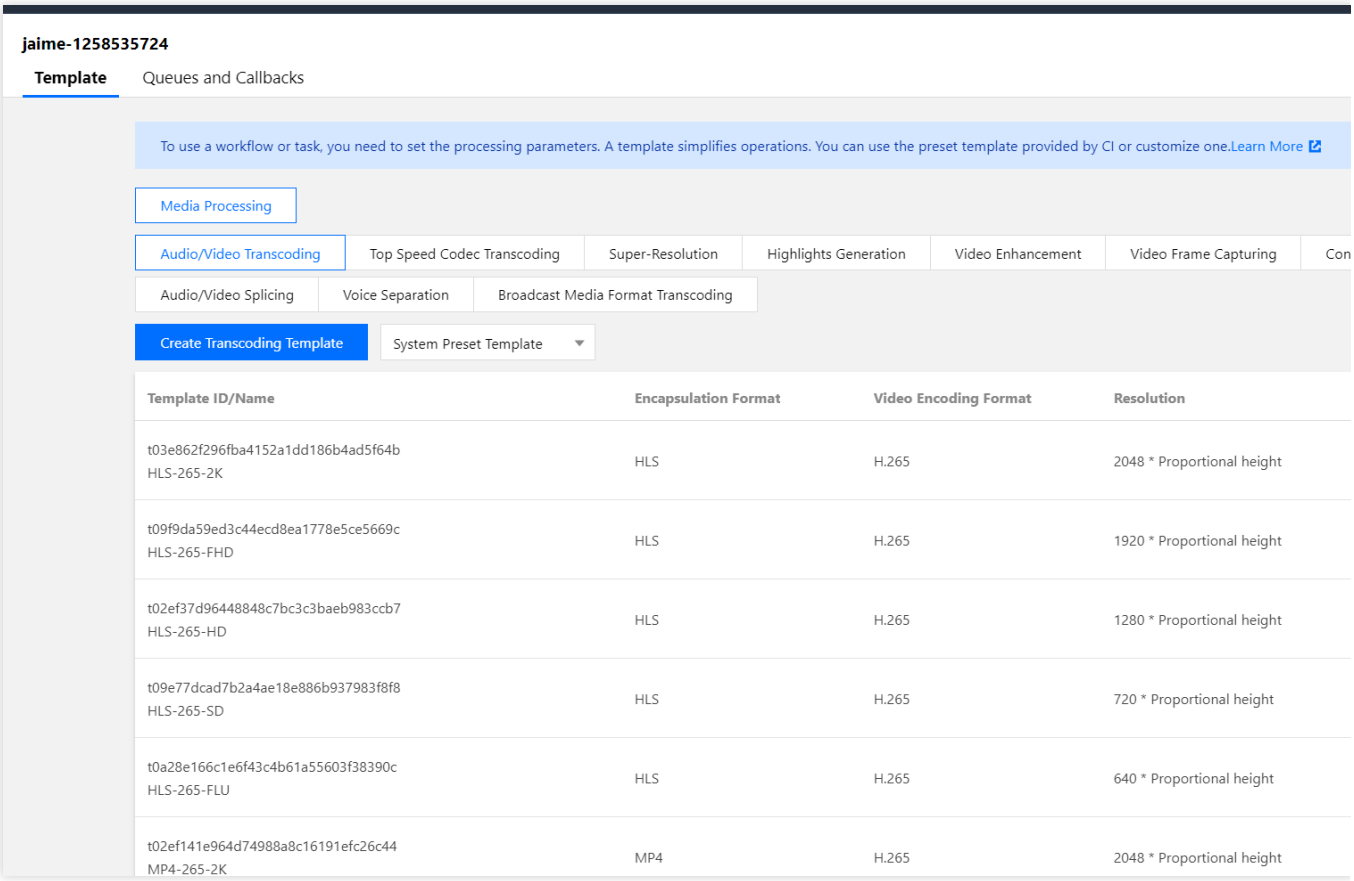
Last updated：2024-03-04 09:37:42

Overview

When using the media processing feature, you usually need to set a series of parameters, which can be combined through a template. This **simplifies your operations** and allows you to reuse the configured parameters with no need to enter them repeatedly.
For media processing features such as audio/video transcoding, audio/video splicing, video frame capturing, and video-to-animated image conversion, you need to specify a template when creating a job or workflow in CI. The template page provides **preset templates**, and you can also **customize templates** based on your business needs.

Preset Templates

The CI system combines common parameters in advance into preset templates, so that you can use them directly. When creating a job or workflow, you can select such a template by the template name.
On the bucket management page, click **Job and Workflow** > **Template Configuration** to view templates of different processing types. Click **View** on the right of a template to view its detailed information.



Note:

Currently, the system provides 15 **audio/video transcoding**, three **video frame capturing**, and 18 **video-to-animated image conversion** preset templates.

You can only view the information of preset templates but cannot edit or delete them.

Preset templates for audio/video transcoding

Template ID	Template Name	Container Format	Video Encoding Format	Resolution	Video Bitrate
t0e2b9f4cd25184c6ab73d0c85a6ee9cb5	H264-MP4-LD-360P	MP4	H.264	640 * proportionally scaled	512 Kbps
t0876739cd865042d1957d73c78f0484fb	H264-MP4-SD-480P	MP4	H.264	720 * proportionally scaled	1024 Kbps
t0852e7ff4acd4484e99ba104f3840d3cb	H264-MP4-HD-720P	MP4	H.264	1280 * proportionally scaled	2000 Kbps

t04df9eb0c373c4a8780ec894ce05469a7	H264-MP4-FHD-1080P	MP4	H.264	1920 * proportionally scaled	3500 Kbps
t09d027135634d47048e5a30dc1e19ee90	H264-MP4-2K	MP4	H.264	2048 * proportionally scaled	4800 Kbps
t0e634622e8dfb49339ba478d60ddc7188	H264-HLS-LD-360P	M3U8	H.264	640 * proportionally scaled	512 Kbps
t0fa5bdbf58bb348e88bf73fae5d674fdf	H264-HLS-SD-480P	M3U8	H.264	720 * proportionally scaled	1024 Kbps
t09d0f419921e44ed98190f355ec9fd629	H264-HLS-HD-720P	M3U8	H.264	1280 * proportionally scaled	2000 Kbps
t080ae8a06f9074f3daa46201078f8d4b1	H264-HLS-FHD-1080P	M3U8	H.264	1920 * proportionally scaled	3500 Kbps
t0ab68939cef0f40d19c4a135df540239f	H264-HLS-2K	M3U8	H.264	2048 * proportionally scaled	4800 Kbps
t0e165bef65ed24d568eeecc8661248af6	H264-FLV-LD-360P	M3U8	H.264	640 * proportionally scaled	512 Kbps
t057d0410c32444e48b9220f9571e6097a	H264-FLV-SD-480P	M3U8	H.264	720 * proportionally scaled	1024 Kbps
t00daf332ba39049f8bfb899c1ed0134b0	H264-FLV-HD-720P	M3U8	H.264	1280 * proportionally scaled	2000 Kbps
t0d41905a814434c8a81897ecb54d53a32	H264-FLV-FHD-1080P	M3U8	H.264	1920 * proportionally scaled	3500 Kbps

t0e287e59454b94a8983ba78a6a30ee864	H264-FLV-2K	M3U8	H.264	2048 * proportionally scaled	4800 Kbps

Preset templates for video frame capturing

Template ID	Template Name	Frame Capturing Start Time	Frame Capturing Interval	Max Frame Count Per Video	Output Image Size
t01d40e440761448fc8c538fb8d5a5b81e	snapshot_320 * 180_1	0s	2s	5	320 * 180 px
t0a60a2bc71a4b40c7b3d7f7e8a2779a81	snapshot_640 * 360_2	0s	10s	5	640 * 360 px
t07740e32081b44ad7a0aea03adcffd54a	snapshot_1280 * 720_3	0s	10s	5	1280 * 720 px

Preset templates for video-to-animated image conversion

Template ID	Template Name	Transcoding Start Time	Transcoding Duration	Frame Extraction Method	O Ar Im Fr Ra
t04373959a69c04d47b62fd214dd13d8e9	gif_320 * 180_1	0s	600s	Only keyframes are extracted	Ac
t0341b0ab2b8a340ff826e9cb4f3a7baea	gif_320 * 180_2	0s	600s	One frame is extracted every 10s	Ac (0
t046b1d8e5bdf842c6a58d8028b48eafee	gif_320 * 180_3	0s	600s	Ten frames are extracted per second	Ac (1

t0ef2077f215864c018a2fca73614ceca6	gif_640 * 360_4	0s	600s	Only keyframes are extracted	Ac
t0d21406ca737a40869973a37a5daa349a	gif_640 * 360_5	0s	600s	One frame is extracted every 10s	Ac (0
t0878a9c9c1f054cb5bca68b8b06e556c2	gif_640 * 360_6	0s	600s	Ten frames are extracted per second	Ac (1
t0dae821708cea4ba5b3e271810ac80a21	gif_1280 * 720_7	0s	600s	Only keyframes are extracted	Ac
t03fef67ad94d2466b9c0c89252ed72e87	gif_1280 * 720_8	0s	600s	One frame is extracted every 10s	Ac (0
t030a64e9f9f5a4f53a9ef64bb7ce490b5	gif_1280 * 720_9	0s	600s	Ten frames are extracted per second	Ac (1
t03b0e9eca4fc34e2cba9da89d9c7c13a2	webp_320 * 180_1	0s	60s	Only keyframes are extracted	Ac
t016fcddf6bc3c44b793e9b7b07119b4ee	webp_320 * 180_2	0s	600s	One frame is extracted every 10s	Ac (0
t0bf1f1ce6d2404b258c0f81fbb9aaece1	webp_320 * 180_3	0s	600s	One frame is	Ac (1

				extracted every 10s	
t098d6d3fcfd2c45309a408594a42559f6	webp_640 * 360_4	0s	60s	Only keyframes are extracted	Ac
t0169a6a9c2eec4b51972eb63bafcbf08d	webp_640 * 360_5	0s	600s	One frame is extracted every 10s	Ac (0
t0ef9ba537011e4876b8777aebc19d10a5	webp_640 * 360_6	0s	600s	One frame is extracted every 10s	Ac (1
t02743d344b5e74c579e50e9e135b432b8	webp_1280 * 720_7	0s	60s	Only keyframes are extracted	Ac
t0dd27c136ff2741538bec96981e058868	webp_1280 * 720_8	0s	600s	One frame is extracted every 10s	Ac (0
t00ad05235d67a45a9a697b553052b7346	webp_1280 * 720_9	0s	600s	One frame is extracted every 10s	Ac (1

Custom Template

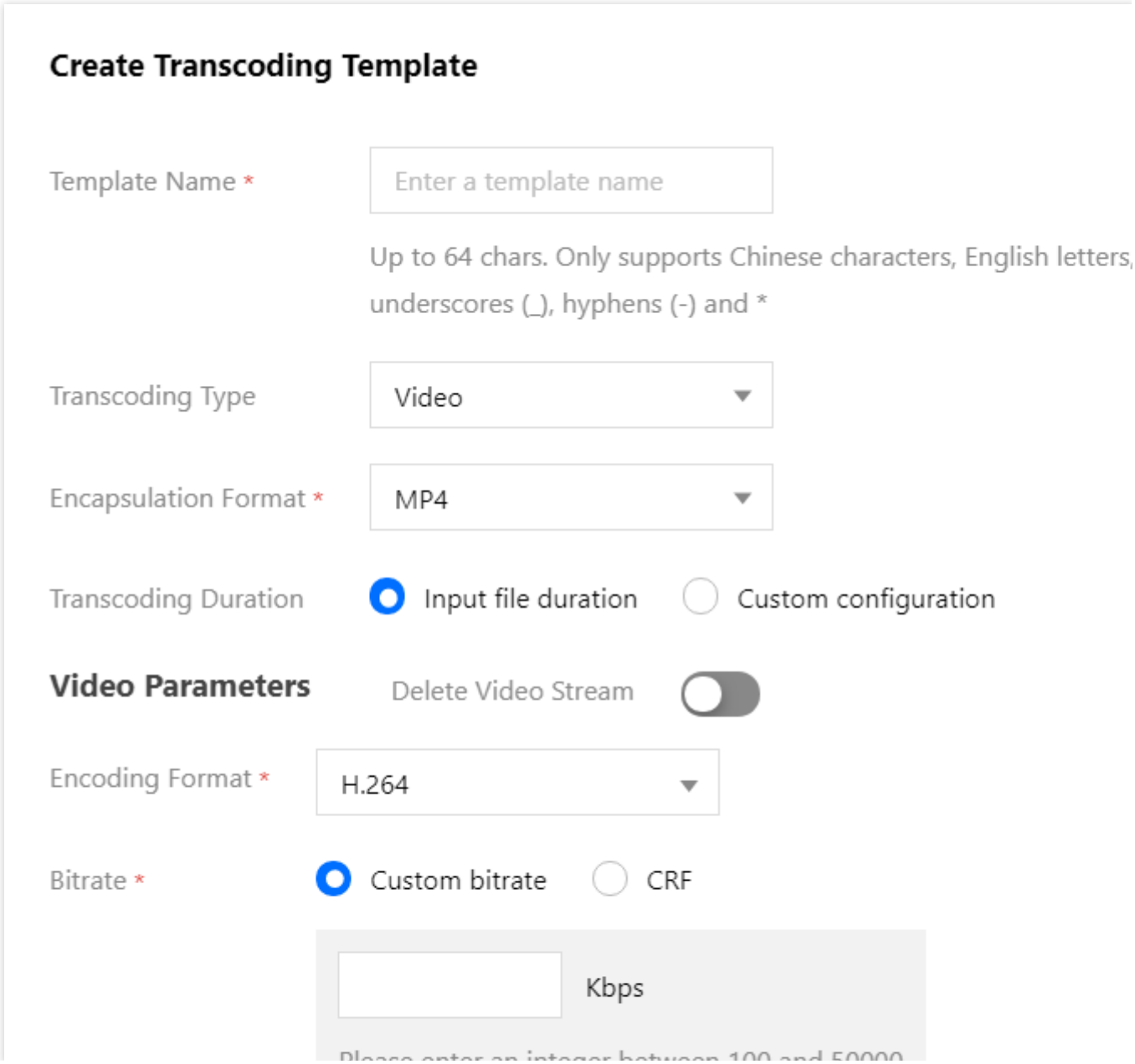
If preset templates cannot meet your needs, use custom templates. Currently, you can create custom templates for **audio/video transcoding**, **top speed codec transcoding**, **broadcast media format transcoding**, **image processing**, **highlights generation (also known as video montage)**, **voice separation (also known as voice/sound separation)**, **video enhancement**, **super resolution**, **video frame capturing**, **video-to-animated image conversion**, **video watermark**, and **audio/video splicing**.

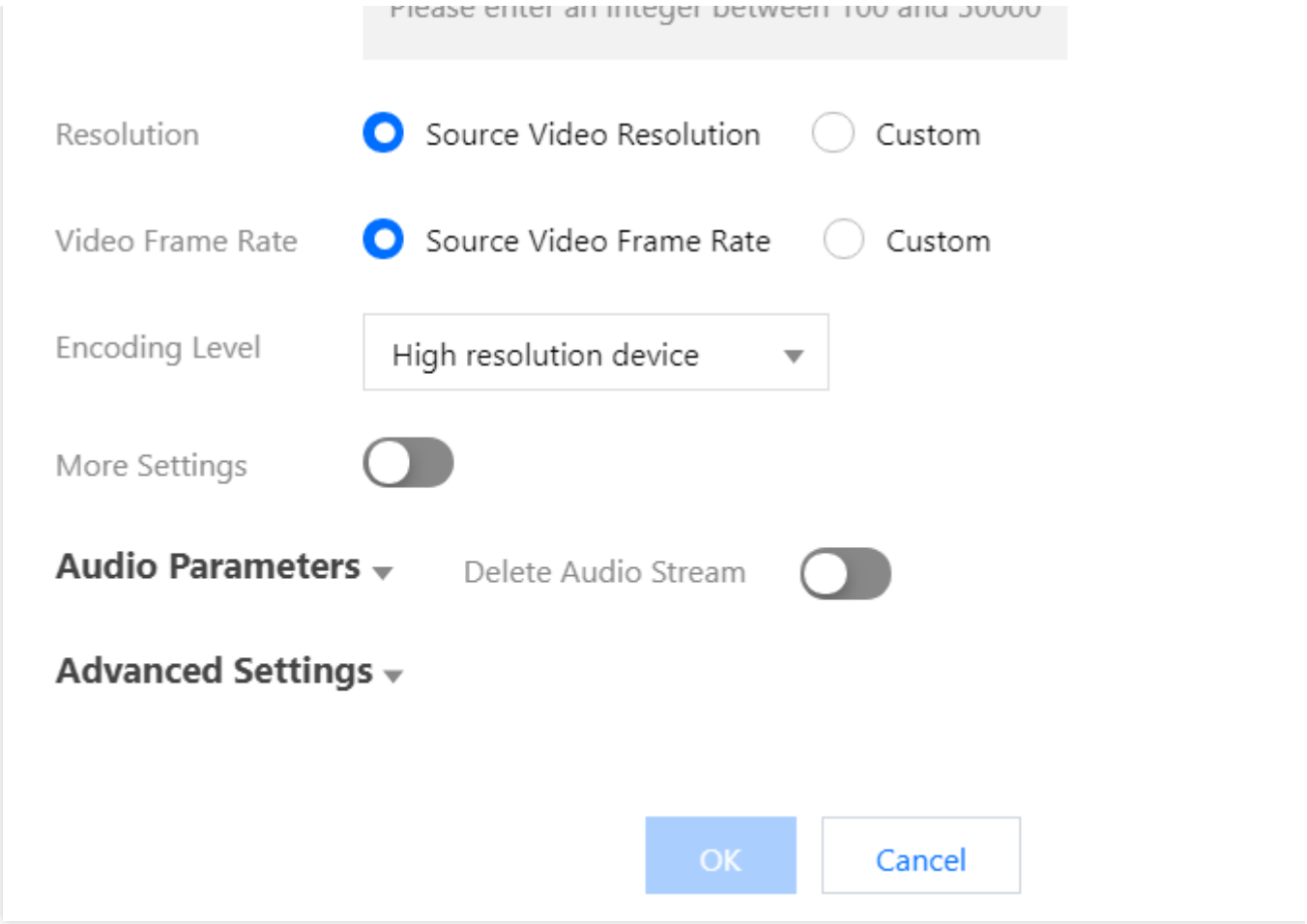
Audio/Video transcoding

The audio/video transcoding feature converts an audio/video file bitstream. It changes parameters of the source bitstream, such as codec, resolution, and bitrate, to adapt to different devices and network conditions. You can customize the template parameters in a custom audio/video transcoding template.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
4. On the left sidebar, click **Data Processing Workflow** > **Common Configuration** and select the **Template** tab at the top to enter the template configuration page.
5. Select **Audio/Video Transcoding** and click **Create Transcoding Template**.
6. In the **Create Transcoding Template** pop-up window, configure the following items:





</br>

The configuration information of the audio/video transcoding template is as follows:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Container Format: Supported formats include MP4, FLV, HLS, TS, and MKV.

Transcoding Duration: You can select the input video duration or customize the duration.

Video Parameters

Encoding Format: Convert the input video to the selected encoding format.

Bitrate: Customize the bitrate or adjust the bitrate through CRF.

Resolution: Control the frame size of the output video.

Video Frame Rate: Set the frequency in frames at which a bitmap image appears continuously on the display.

Encoding Level: Control the compression ratio of the video.

Audio Parameters: Customize audio parameters as needed.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

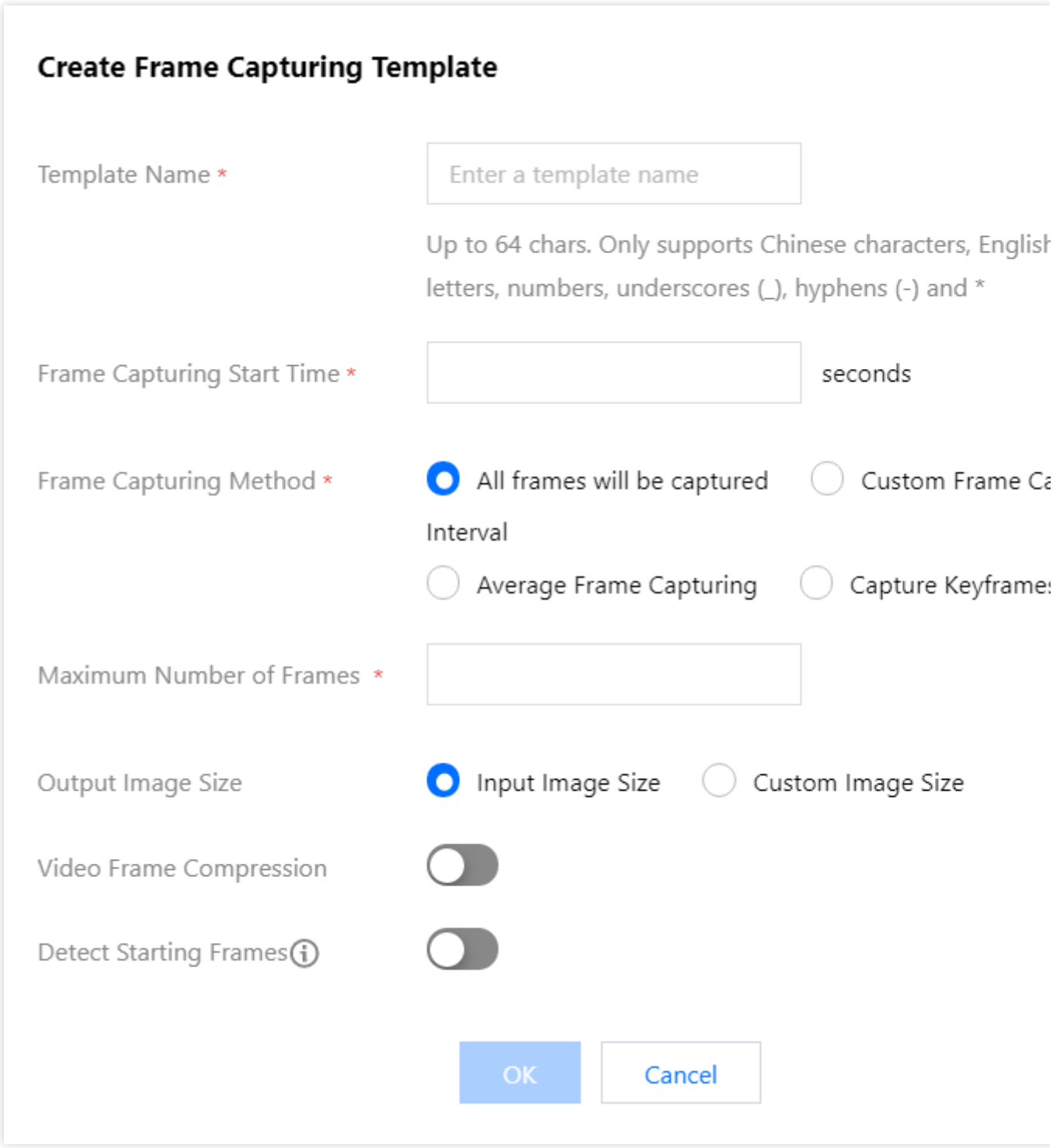
You can apply the audio/video transcoding template when creating a job or workflow in CI.

Video frame capturing

CI's video frame capturing feature captures the frames of a video at specified time points. The output screenshots are in JPG format. You can customize the template name, frame capturing start time, frame capturing interval, captured frames, and output image size and format in a custom video frame capturing template.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
4. On the left sidebar, click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
5. Select **Video Frame Capturing** and click **Create Video Frame Capturing Template**.
6. In the **Create Video Frame Capturing Template** pop-up window, configure the following items:



The configuration information of the video frame capturing template is as follows:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Frame Capturing Start Time: You can select any time point within the full video length.

Frame Capturing Method

All frames will be captured by default: Every video frame will be captured.

Custom Frame Capturing Interval: Frames will be captured at specified time intervals from the frame capturing start time to the end of the video.

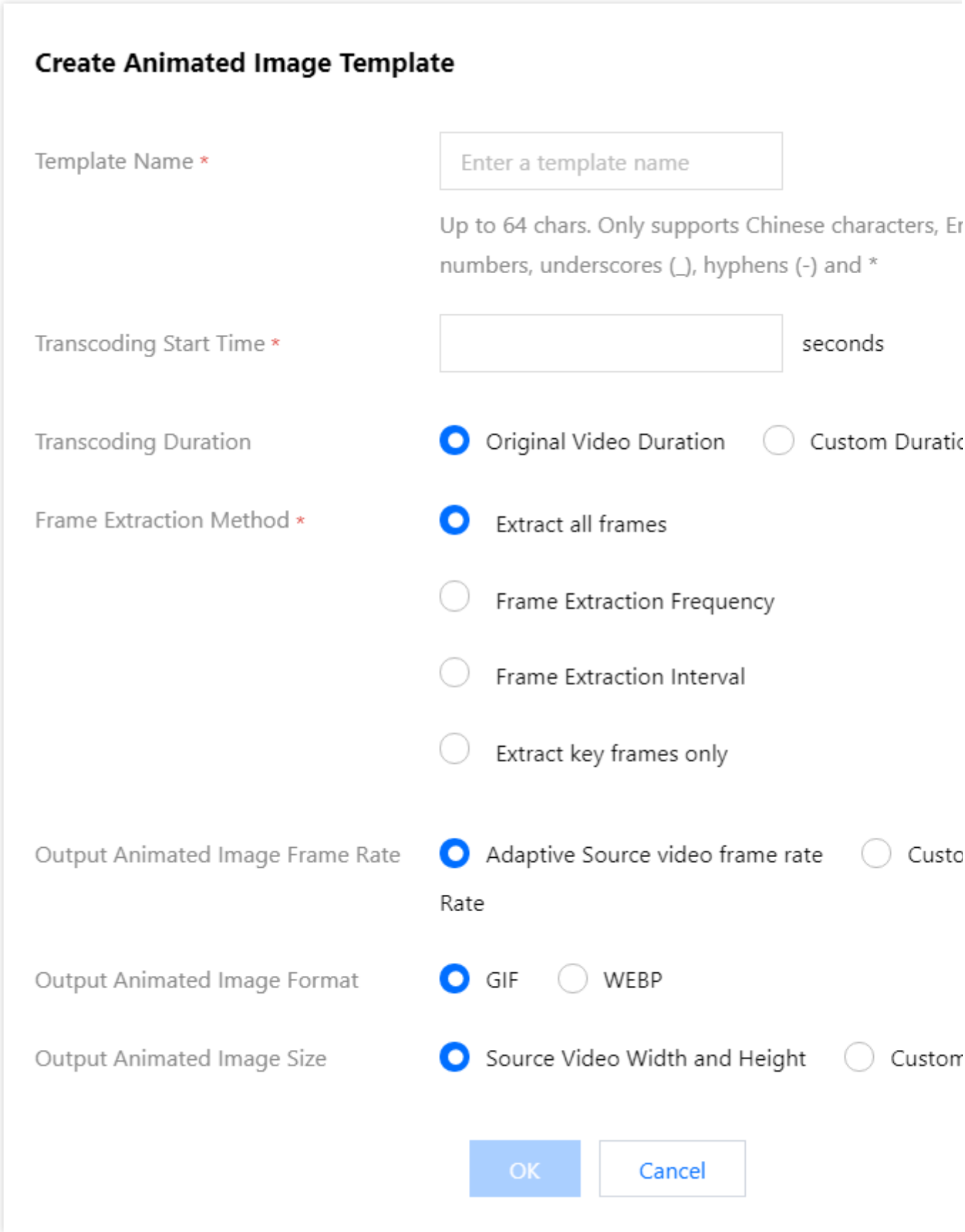
Even Frame Capturing: Frames will be captured at even intervals calculated based on the specified **number of captured frames** from the frame capturing start time to the end of the video.
Capture Keyframes: Keyframes will be captured based on the specified **number of captured frames** from the frame capturing start time to the end of the video.
Max Frame Count Per Video: This parameter is required if you select **All frames will be captured by default**, **Custom Frame Capturing Interval**, or **Capture Keyframes** as the frame capturing method.
Captured Frames: This parameter is required if you select **Even Frame Capturing** as the frame capturing method. Frames will be captured at even intervals calculated based on the specified number of frames captured from the frame capturing start time to the end of the video.
Output Image Size: The default output screenshot size is the same as that of the input video image. If you select custom image size, you must enter an integer between 128 and 4096 for the width and height respectively.
7. Click **OK**.
After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list. You can click **Preview** to view the position and dimensions of the watermark in videos of three common resolutions and quickly adjust the template.
Note:
You can apply the video frame capturing template when creating a job or workflow in CI.

Video-to-animated image conversion

The video-to-animated image conversion feature converts a video to animated images. You can customize the template name, transcoding start time, transcoding duration, frame extraction method, output animated image frame rate, and output animated image size in a custom video-to-animated image conversion template.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
4. On the left sidebar, click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
5. Select **Video-to-Animated Image Conversion** and click **Create Video-to-Animated Image Conversion Template**.
6. In the **Create Video-to-Animated Image Conversion Template** pop-up window, configure the following items:



The configuration information of the video-to-animated image conversion template is as follows:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Transcoding Start Time: You can select any time point within the full video length.
Transcoding Duration: It specifies the duration of video transcoding after the **transcoding start time**. You can select **Original Video Duration** or **Custom**.
Frame Extraction Method
Extract all frames: Every video frame will be extracted.
Frame Extraction Frequency: You can set the number of frames to be extracted per second (an integer between 1 and 50).
Frame Extraction Interval: Frame will be extracted at the specified intervals in seconds.
Extract key frames only: The system will intelligently identify and extract the optimal set of frames based on AI understanding of the video content and output them as an animated image.
Output Animated Image Frame Rate: If **Adaptive** is selected, the system will automatically select an appropriate frame rate based on the settings of the above parameters. You can also select **Custom Playback Frame Rate** to restrict the frame rate to 1–60 FPS.
Output Animated Image Format: The output animated image is in GIF format by default. If you select the WEBP format, you need to select the animated image quality, which ranges from 1 to 99 and is 75 by default.
Output Animated Image Size: The default output animated image size is the same as that of the input video. If you select custom width and height, you must enter an integer between 128 and 4096 for the width and height respectively.
7. Click **OK**.
After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.
Note:
You can apply the video-to-animated image conversion template when creating a job or workflow in CI.

Highlights generation

The highlights generation feature automatically extracts highlights from a video. You can use a custom template to set the highlights generation template name and specify the maximum duration, resolution, and format of the output highlight video.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
4. On the left sidebar, click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
5. Select **Highlights Generation** and click **Create Highlights Generation Template**.
6. In the **Create Highlights Generation Template** pop-up window, configure the following items:
Note:
Currently, highlights generation can be used only for landscape, food, street, and vlog scenarios and will support more scenarios in the future. If you want to customize this feature, contact us for assistance.

The configuration information of the highlights generation template is as follows:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Container Format: Supported formats include MP4, FLV, HLS, TS, and MKV.

Highlight Video Duration: You can select the duration of the complete output highlight video after automatic analysis or customize the duration.

Video Parameters

Encoding Format: Convert the input video to the selected encoding format.

Bitrate: Customize the bitrate or adjust the bitrate through CRF.

Resolution: Control the frame size of the output video.

Video Frame Rate: Set the frequency in frames at which a bitmap image appears continuously on the display.

Audio Parameters: Customize audio parameters as needed.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can apply the highlights generation template when creating a job or workflow in CI.

Video enhancement

The video enhancement feature uses AI to improve the video quality and enhance the video colors and details visually.

Directions

1. Log in to the CI console and click **Bucket Management** on the left sidebar to enter the bucket list.
2. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
3. Click **Job and Workflow** > **Template Configuration** on the left to enter the template configuration page.
4. Select **Video Enhancement** and click **Create Video Enhancement Template**.
5. In the **Create Video Enhancement Template** window, configure the following items:

Note:

Currently, video enhancement supports color and detail enhancement. Other features will be provided in the future.

The input video for enhancement must be shorter than 30 minutes.

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Color Enhancement: Customize the color enhancement parameters or select automatic system analysis for color enhancement.

Detail Enhancement: Customize the detail enhancement parameters or select automatic system analysis for detail enhancement.

6. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Super resolution

The super resolution feature reconstructs a series of low-resolution images through AI technologies to generate a high-resolution image.

Directions

1. Log in to the CI console and click **Bucket Management** on the left sidebar to enter the bucket list.
2. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
3. Select the **Data Processing Workflow** > **Common Configuration** tab on the left and click **Template** at the top to enter the template configuration page.
4. Select **Super Resolution** and click **Create Super Resolution Template**.
5. In the **Create Super Resolution Template** window, configure the following items:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).
Version: Select **Basic** or **Enhanced**. The latter delivers greater image quality restoration effects.
Target Resolution: Select the output resolution.
Target Zoom: Zoom the output video to the selected target resolution.

6. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Top speed codec transcoding

The top speed codec transcoding feature improves the subjective image quality of a video at the minimum bitrate. Compared with regular audio/video transcoding, it outputs smaller files and clearer video images and delivers a better visual experience with guaranteed low network resource usage. You can customize parameters such as codec, resolution, and bitrate in a custom top speed codec transcoding template.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
4. Click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
5. Select **Top Speed Codec Transcoding** and click **Create Top Speed Codec Transcoding Template**.
6. In the **Create Top Speed Codec Transcoding Template** pop-up window, configure the following items:

The configuration information of the top speed codec transcoding template is as follows:
Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).
Container Format: Supported formats include MP4 and HLS.
Transcoding Duration: You can select the input video duration or customize the duration.

Video Parameters

Encoding Format: Convert the input video to the selected encoding format.
Bitrate: Customize the bitrate or adjust the bitrate through CRF.
Resolution: Control the frame size of the output video.

Video Frame Rate: Set the frequency in frames at which a bitmap image appears continuously on the display.

Audio Parameters: Customize audio parameters as needed.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can apply the top speed codec transcoding template when creating a job or workflow in CI.

Broadcast media format transcoding

This feature processes special formats such as XAVC and ProRes.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
4. On the left sidebar, click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
5. Select **Broadcast Media Format Transcoding** and click **Create Broadcast Media Format Transcoding Template**.
6. In the **Create Top Speed Codec Transcoding Template** pop-up window, configure the following items:

The configuration information of the broadcast media format transcoding template is as follows:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Container Format: Supported formats include MXF.

Transcoding Duration: You can select the input video duration or customize the duration.

Video Parameters

Encoding Format: Convert the input video to the selected encoding format.

Preset Encoder Configuration: Select the default values of encoder parameters such as sample rate.

Bitrate: Customize the bitrate or adjust the bitrate through CRF.

Resolution: Control the frame size of the output video.

Video Frame Rate: Set the frequency in frames at which a bitmap image appears continuously on the display.

Audio Parameters: Customize audio parameters as needed.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

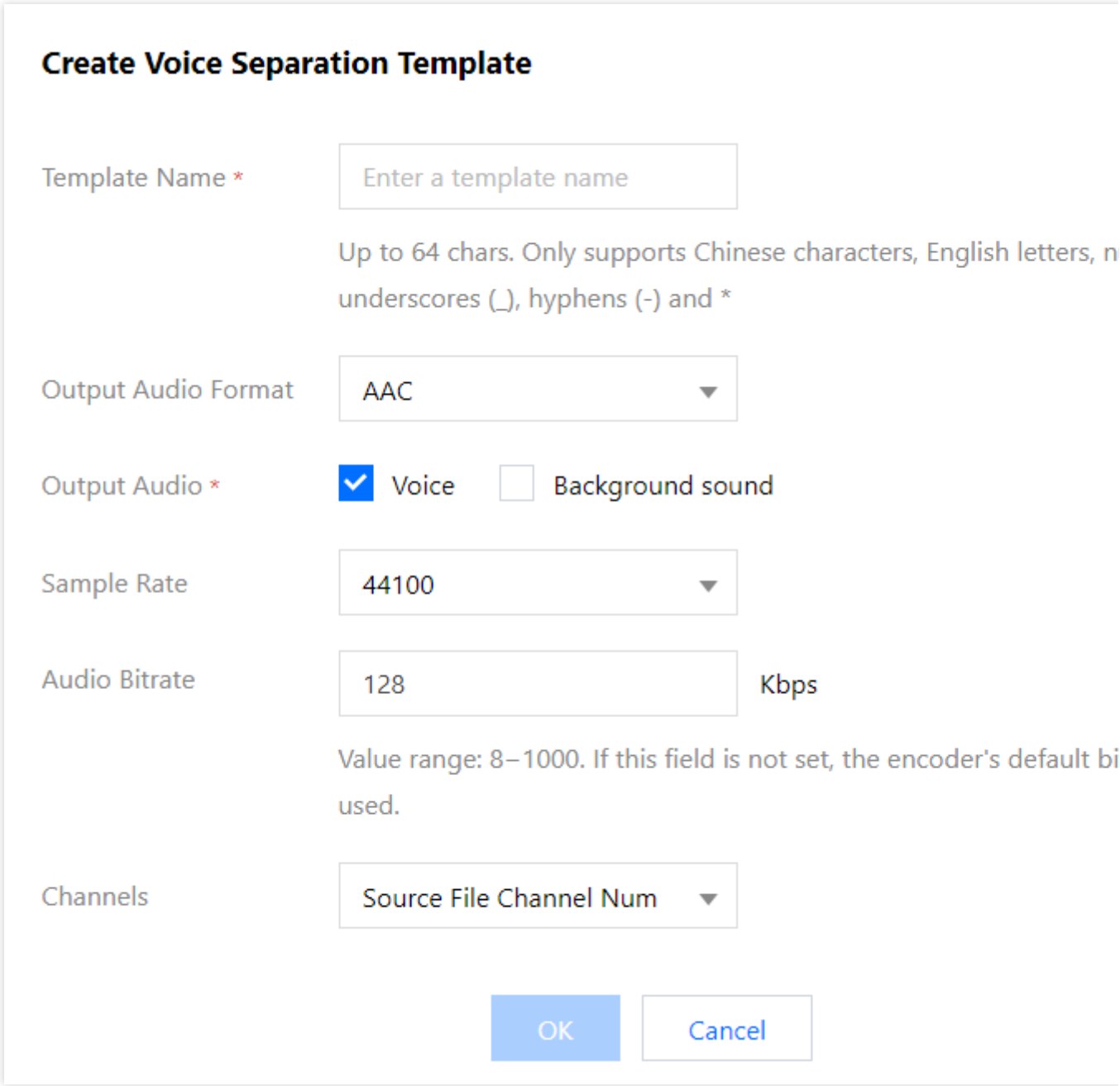
You can apply the top speed codec transcoding template when creating a job or workflow in CI.

Voice separation

You can separate the same audio file into a voice file and a background sound file for subsequent video editing and playback.

Directions

1. Log in to the CI console and click **Bucket Management** on the left sidebar to enter the bucket list.
2. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
3. On the left sidebar, click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
4. Click **Voice Separation** > **Voice Separation Template**. In the **Create Voice Separation Template** pop-up window, configure the following items:



5. In the **Create Voice Separation Template** window, configure the following items:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Output Audio Format: Supported formats include MP3, AAC, AMR, and FLAC.

Output Audio: Specify to output voice or background sound.
Audio Parameters: Customize audio parameters as needed.
6. Click **OK**.
After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Text to speech

The text to speech feature converts text to natural-sounding and smooth speeches through advanced deep learning technology.

Directions

1. Log in to the CI console and click **Bucket Management** on the left sidebar to enter the bucket list.
2. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
3. On the left sidebar, click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
4. Click **Text to Speech** > **Text-to-Speech Template**. The configuration information of the text-to-speech template is as follows:
5. In the **Create Text-to-Speech Template** window, configure the following items:
Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).
Voice: Select the desired voice.
Processing Mode: Select async or sync processing based on the text length.
Output Audio Format: Supported formats include MP3, AAC, WAV, and PCM.
Volume: Adjust the volume level.
Speech Speed: Adjust the speech speed of the output audio.
6. Click **OK**.
After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Speech recognition

The speech recognition feature can convert speeches in English and Chinese to text.

Directions

1. Log in to the CI console and click **Bucket Management** on the left sidebar to enter the bucket list.
2. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
3. On the left sidebar, click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
4. Click **Speech Recognition** > **Speech Recognition Template**. The configuration information of the speech recognition template is as follows:
5. In the **Create Speech Recognition Template** window, configure the following items:
Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).
Recognition Engine: Select the needed recognition engine.
Sound Channels: Select the number of channels.

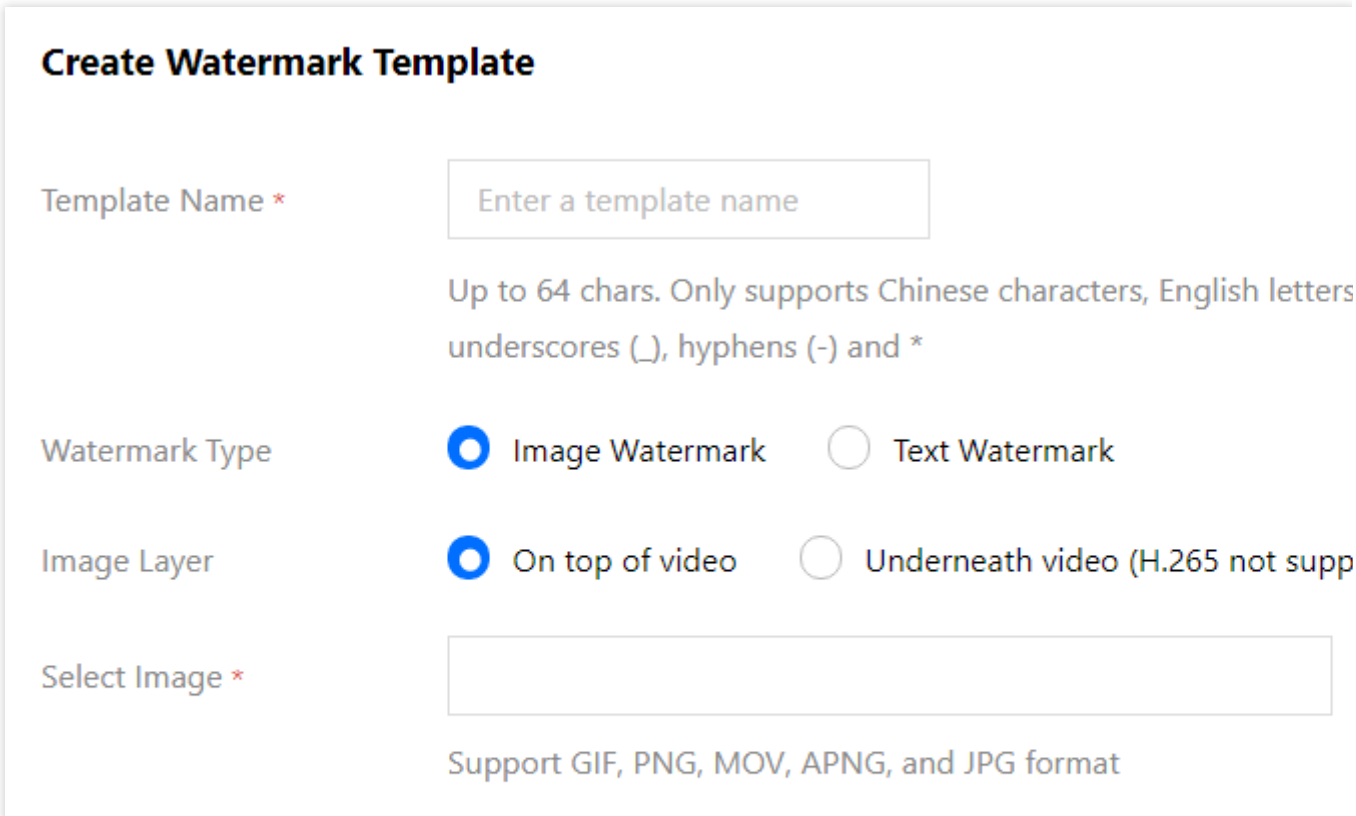
Speaker Separation: Specify whether to automatically distinguish between different speakers when marking the content.
Recognition Result: Select **Common text** or **Word-level text**.
Filter Restricted Words: Specify whether to filter restricted words.
Smart Number Conversion: Specify whether to convert numbers to Arabic numerals.
Output File Type: Select **srt** or **txt**.
6. Click **OK**.
After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

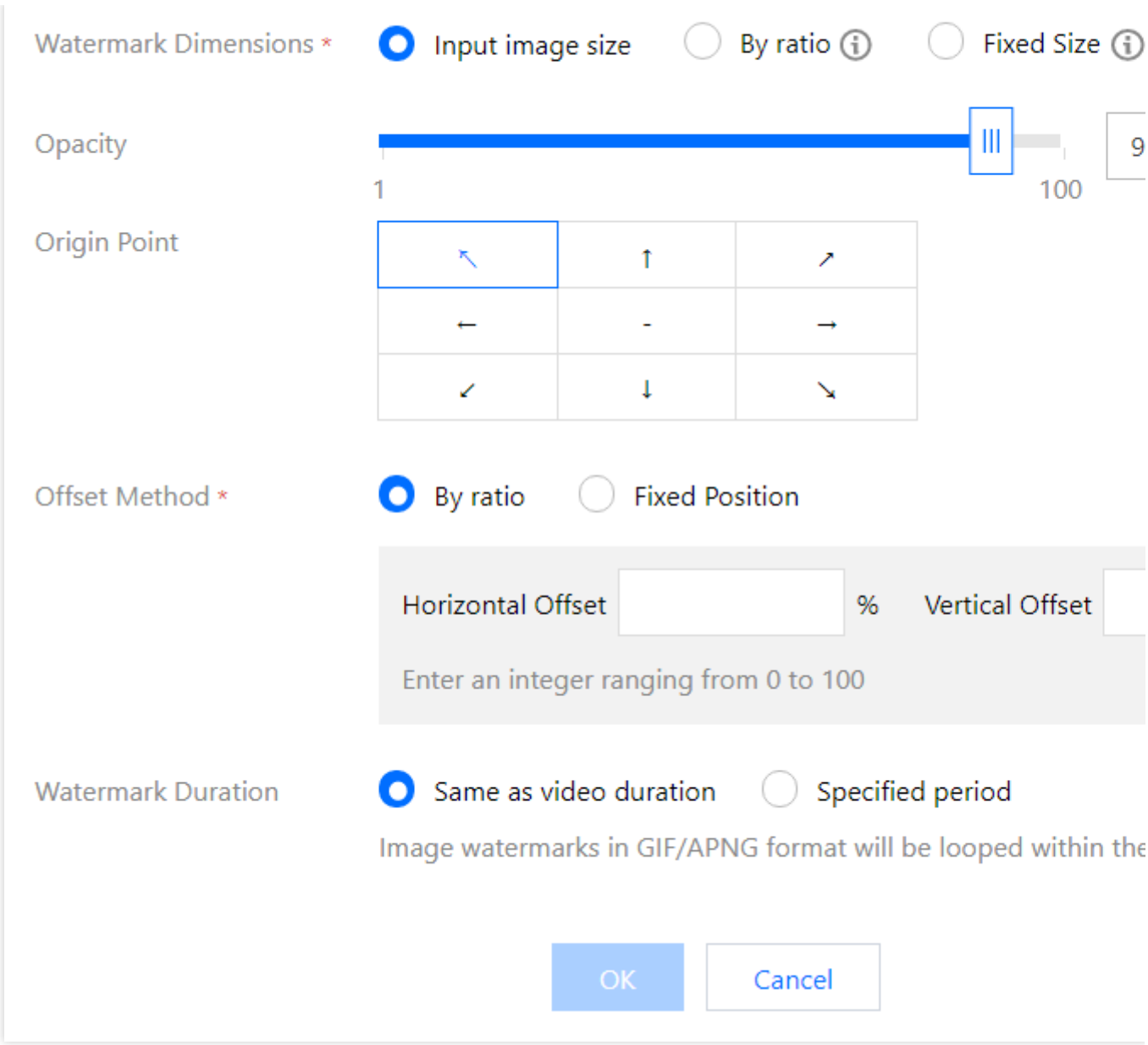
Video watermark

The video watermark feature adds a text or image watermark to a video during transcoding.
Note:
Currently, you can add up to three watermarks in the console or five via API at a time. To add more watermarks, contact us for assistance.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
4. On the left sidebar, click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
5. Select **Video Watermark** and click **Create Video Watermark Template**.





6. In the **Create Video Watermark Template** window, configure the following items:

Common parameters

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Watermark Type: Select image or text watermark.

Origin Point: Select the top-left, top-right, bottom-left, or bottom-right corner.

Opacity: Select a value between 1% and 100%.

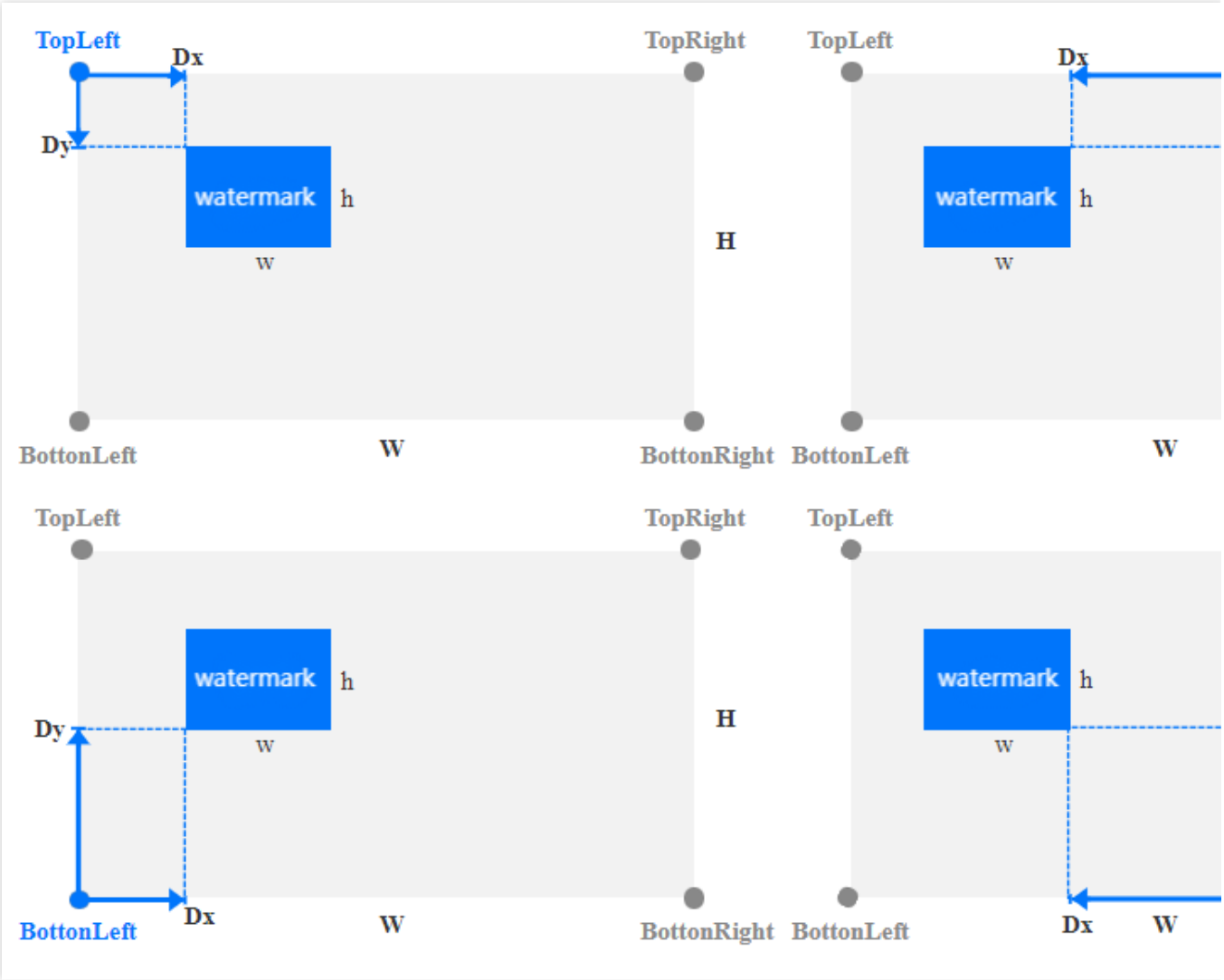
Offset Method: The watermark offset is based on the origin point. You can select offset by ratio or fixed position.

Watermark Duration: Select **Same as video duration** or **Specified period**. If you select the latter, you can set the watermark start time and end time. If you set the start time only, the watermark will be displayed until the video ends by default.

Image watermark parameters

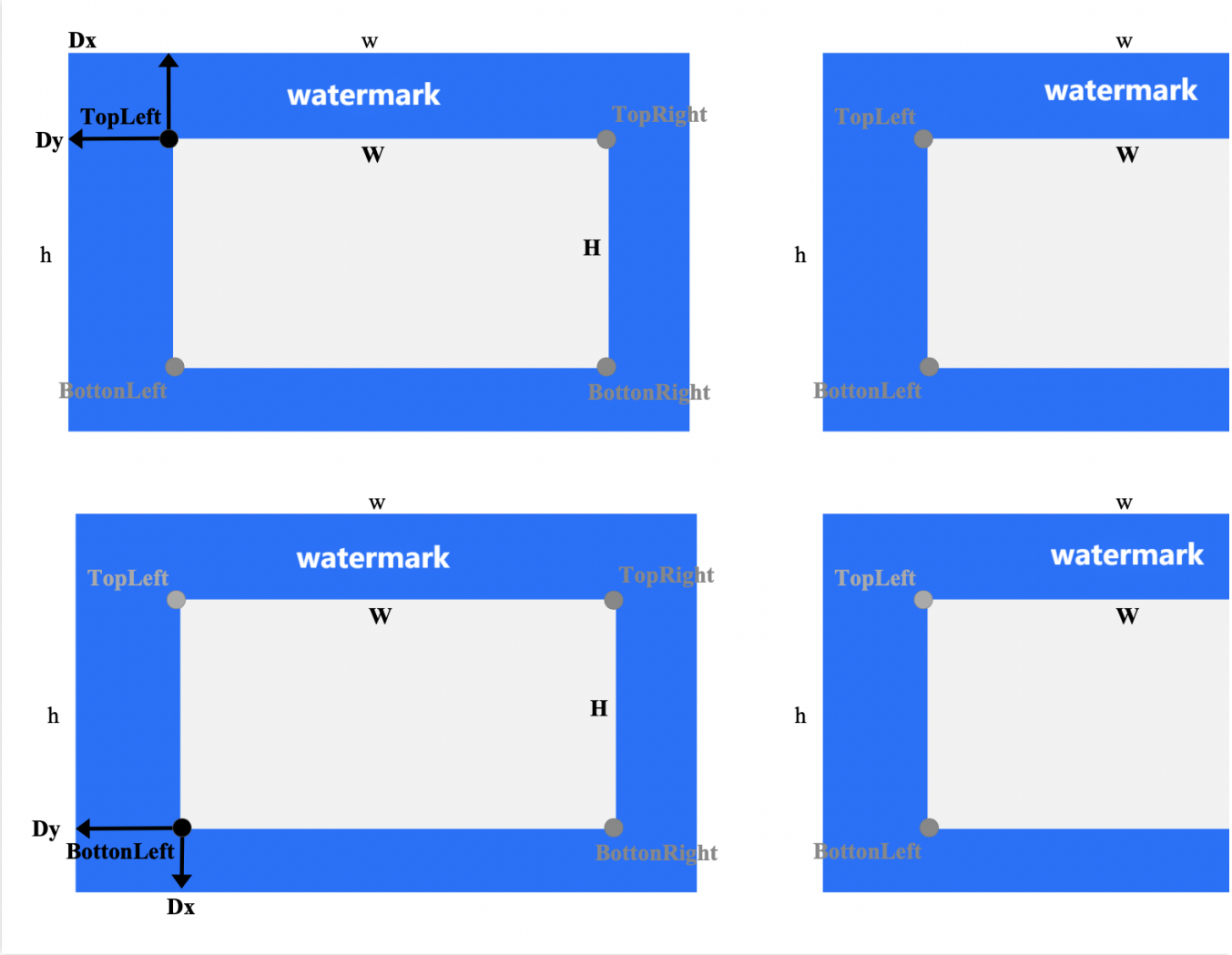
Select Image: If you select image watermark, you need to select its source. Currently, only a watermark image in the same bucket can be selected. If the bucket doesn't have desired images, you need to upload a new one.

Image Layer: Select whether to place the image on top of or underneath the video.
If the image is placed on top of the video, the effect is as shown below:



Watermark Dimensions:
Input image size: The original watermark image size will be retained without any processing. Note that if the watermark image is larger than the video image, the watermark cannot be completely displayed.
By ratio: You can set the percentage (1–100) of only the width or height or both of them. If the width or height is not set, it will be scaled proportionally. Suppose the width ratio is `a` and height ratio is `b`, then the watermark width will be `w = W * a`, and the watermark height will be `h = H * b` (here, `W` and `H` are the video width and height respectively).
Fixed size: You can specify the watermark width and height between 8 and 4096 px.
Offset Method:
By ratio: You can set the percentage (0–100) of the width or height. Suppose the horizontal offset ratio is `a` and the vertical ratio is `b`, then the horizontal offset will be `Dx = W * a`, and the vertical offset will be `Dy = H * b` (here, `W` and `H` are the video width and height respectively).

Fixed position: Select a value between 0 and 4096 px. The horizontal offset is `Dx`, and the vertical offset is `Dy`.
If the image is placed underneath the video (as the background), the effect is as shown below:



Watermark Dimensions:
Input image size: The original watermark image size will be retained without any processing. Note that if the watermark image is smaller than the video image, the watermark cannot be completely displayed.
By ratio: You can set the percentage (100–300) of only the width or height or both of them. If the width or height is not set, it will be scaled proportionally. Suppose the width ratio is `a` and height ratio is `b`, then the watermark width will be `w = W * a`, and the watermark height will be `h = H * b` (here, `W` and `H` are the video width and height respectively).
Fixed size: You can specify the watermark width and height between 8 and 4096 px.
Offset Method:
By ratio: You can set the percentage (-300–0) of the width or height. Suppose the horizontal offset ratio is `a` and the vertical ratio is `b`, then the horizontal offset will be `Dx = W * a`, and the vertical offset will be `Dy = H * b` (here, `W` and `H` are the video width and height respectively).
Fixed position: Select a value between -4096 and 0 px. The horizontal offset is `Dx`, and the vertical offset is `Dy`.

Text watermark parameters

Watermark Text: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Font Size: Select a value between 5 and 100 px.

Font: Select Ariblk, Arial, Ahronbd, Helvetica, or HelveticaNeue.

Font Color: It is in the format of `0xRRGGBB` .

7. Click **OK**.

After successfully creating the template, you can **preview**, **view**, **edit**, or **delete** it in the custom template list. You can click **Preview** to view the position and dimensions of the watermark in videos of three common resolutions and quickly adjust the template.

Note:

You can apply the video watermark template when creating an audio/video transcoding job or workflow in CI.

Audio/Video splicing

The video/audio splicing feature adds the specified video/audio segment at the beginning or end of a video/audio file to generate a new one.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.
4. On the left sidebar, click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
5. Select **Audio/Video Splicing** and click **Create Audio/Video Splicing Template**.
6. In the **Create Audio/Video Splicing Template** pop-up window, configure the following items:
7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can apply the audio/video splicing template when creating a job or workflow in CI.

Image processing

The image processing feature supports flexible image editing, such as rotation, cropping, transcoding, and scaling. It provides multiple image downsizing solutions like Guetzli compression, TPG transcoding, and HEIF transcoding, as well as diversified copyright protection solutions like image/text/blind watermarking. This meets your image processing needs in different business scenarios.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Click **Manage** in the **Operation** column on the right of the target bucket to enter the bucket management page.

4. On the left sidebar, click **Job and Workflow** > **Template Configuration** to enter the template configuration page.
5. Select **Image Processing** and click **Create Image Processing Template**.
6. In the **Create Image Processing Template** pop-up window, configure the following items:
7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can apply the image processing template when creating a job or workflow in CI.

Queue

Last updated：2024-01-31 16:44:15

Overview

When you activate the media processing service, the system will **automatically create** a user queue (queue-1) for you. When you submit a job, the job will be arranged in the queue first and executed in sequence according to the priority and order of submission. You can also set a **callback rule** to stay up to date with the job or workflow progress, and the system will send the processing result and status information to the specified address.

Note:

Currently, CI supports only one queue. If you want more concurrencies of a single queue, submit a ticket for assistance.

Enabling or Pausing a Queue

You can enable or pause a queue in its **Operation** column.

Directions

1. Log in to the CI console and click **Bucket Management** to enter the bucket management page.
2. Click the name of the desired bucket.
3. On the left sidebar, click **Task and Workflow**. Then, select the **Queues and Callbacks** tab.
4. In the **Media Processing Queue** column, enable or pause the queue.

Note:

After a queue is paused, you cannot use the job and workflow features on the console.

After the queue is paused, jobs in it will stop.

Setting a Callback Rule

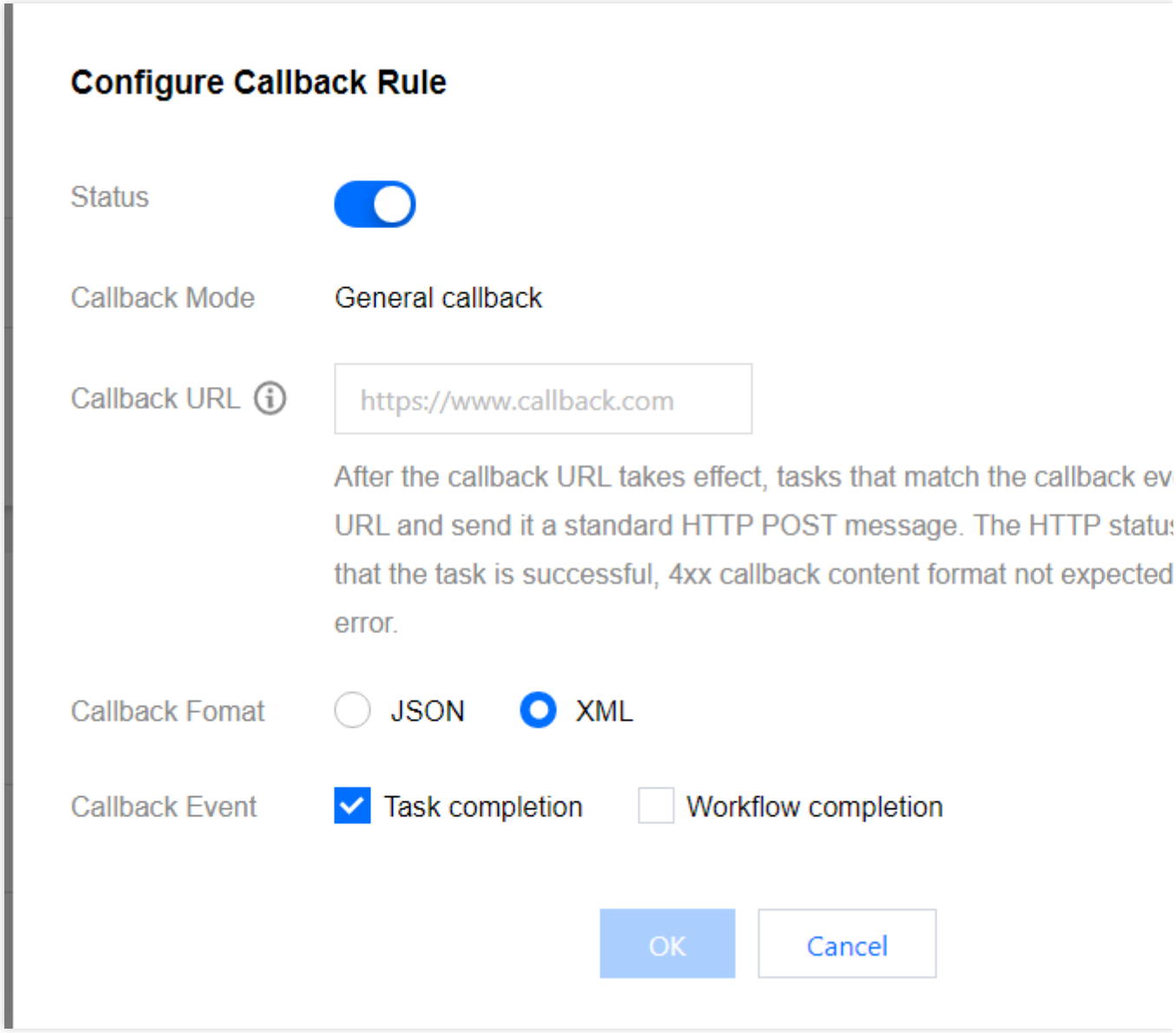
CI supports user-defined callback URLs. After an event is completed, the system sends an HTTP POST request whose body contains notification content to a user-defined callback URL. You can use the configured callback URL to learn about the processing progress and status of the event so that you can perform other operations as needed.

Directions

1. Log in to the CI console and click **Bucket Management** to enter the bucket management page.
2. Click the name of the desired bucket.

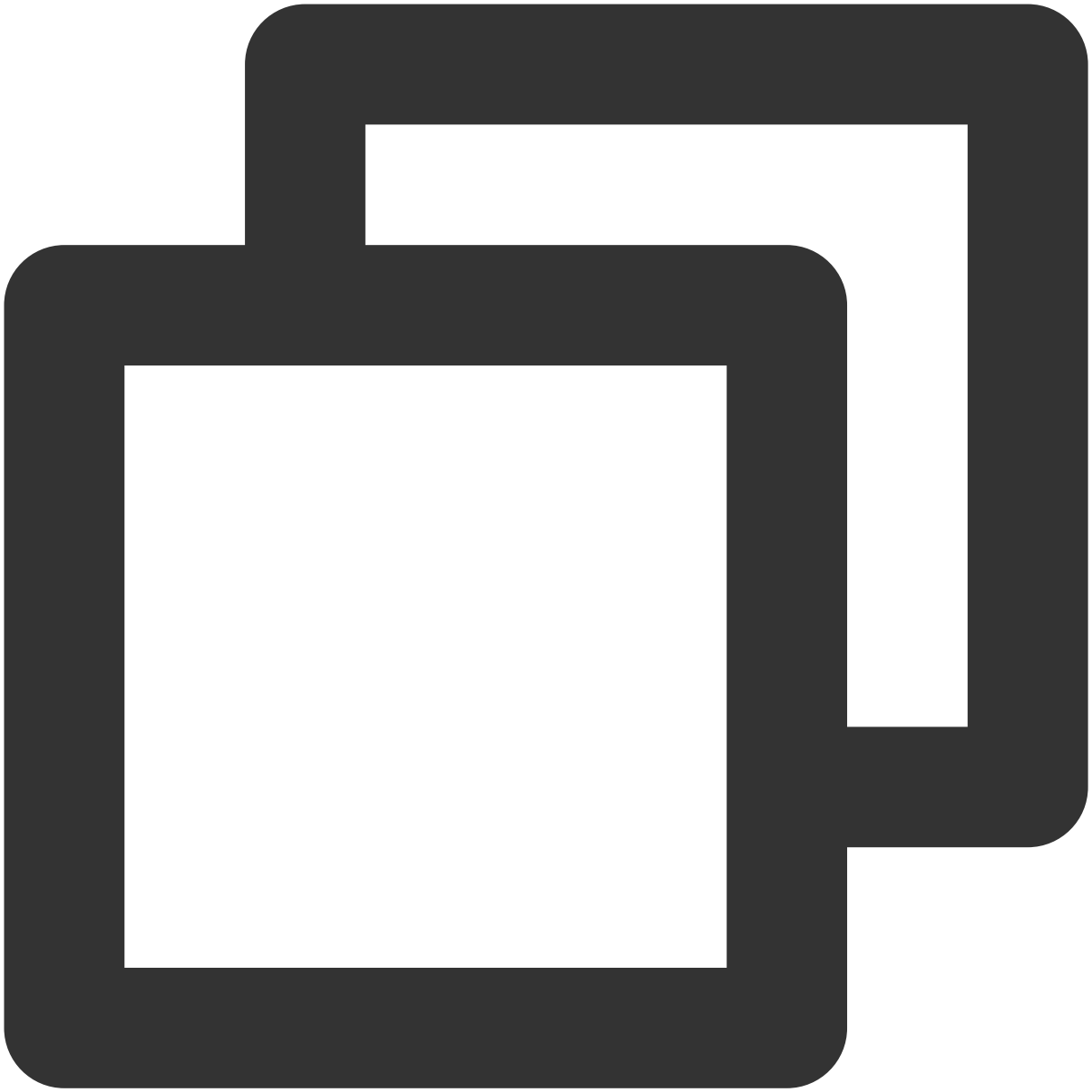
3. On the left sidebar, click **Task and Workflow**. Then, select the **Queues and Callbacks** tab.
4. Click **Configure Callback Rule**.
5. In the pop-up window, click the current status to enable or disable callback.

When enabling callback, you need to specify a URL for the system to send HTTP requests or select a TMDQ-CMQ message queue. For more information on callback, see **Callback content**.



Callback content

After a job is completed, the system will send the following callback content to the configured callback URL:



```
<Response>
  <JobsDetail></JobsDetail>
  <NonExistJobIds></NonExistJobIds>
</Response>
```

The nodes are described as follows:

Parameter	Description	Type
JobsDetail	Job details. Same as the Response.JobsDetail node in the `CreateMediaJobs` API.	Container

NonExistJobIds	List of non-existing job IDs queried. If all jobs exist, this parameter is not returned.	String

Bucket Management
Configuring Buckets

Last updated：2024-01-31 16:44:15

CI is a data processing platform based on COS. You can use CI features only after binding or creating a COS bucket. The bucket management page provides the **bucket binding**, **bucket creation**, **bucket unbinding**, and **bucket search** features.

Prerequisites

You need to log in to the CI Console and click **Bucket Management** on the left sidebar to enter the bucket list page.

Binding Bucket

You can bind an existing COS bucket in the following steps:
1. Click **Bind Bucket** to pop up the bucket binding dialog box.
Note:
During the binding, you need to create a preset service role, grant it CI-related permissions, and complete service authorization as prompted.
2. Click the COS bucket to be bound and select whether to enable CDN acceleration.
Note:
Binding a COS bucket is essentially to enable the image processing service for it.

Creating Bucket

You can create a bucket in the following steps:
1. Click **Bind Bucket** to pop up the bucket binding dialog box.
2. Select **Create** as the adding method, enter the custom bucket name, select the bucket region, access permission, and whether to enable CDN acceleration, and click **OK** to quickly create a bucket. The configuration items are as detailed below:
Note:
The new bucket can also be queried in the COS Console. If you want to configure the bucket in a more detailed manner, please go to the COS Console.

There can be up to 200 buckets in total in all regions under one account, but the numbers of directories and files in a bucket are not limited.

Bucket Name

A bucket name can contain up to 50 digits, lowercase letters, and hyphens.

The bucket name must be unique in all projects under the same `APPID` .

Region

The storage service can be used in multiple regions. For the available regions, please see Regions and Domain Names. You can select the bucket region when creating a bucket, and once selected, it cannot be changed. To make access faster, we recommend you select an available region near your users.

Access Permission

Three types of bucket access permissions are available by default, i.e., "Private Read/Write", "Public Read/Private Write", and "Public Read/Write". If needed, you can modify the access permission in the COS Console subsequently.

Private Read/Write: only the creator of the bucket and authorized accounts can read/write the objects in the bucket, while others cannot.

Public Read/Private Write: anyone (including anonymous visitors) has read permission to the objects in the bucket, but only the bucket creator and authorized accounts have write permission to them.

Public Read/Write: anyone (including anonymous visitors) has read/write permission to the objects in the bucket, which is not recommended.

CDN Acceleration

CDN acceleration is disabled by default. You can enable/disable it as needed. After it is enabled, you can relay files on Tencent Cloud CDN nodes to make the access faster.

Unbinding Bucket

If you no longer use a bucket, you can unbind it.

Click **Unbind** in the "Operation" column on the right of the target bucket to pop up the bucket unbinding dialog box.

Click **OK** to unbind it.

Note:

Currently, CI **does not allow** you to delete buckets. Once unbound, a bucket will be deleted from the CI's bucket list, but it and all its contents will be retained in COS. You can go to the COS Console to view it in the bucket list.

Searching for Bucket

If you want to query a bucket bound to CI, you can select **Bucket name** or **Bucket tag** in the drop-down list on the right for filtering.

Bucket Tagging
Bucket Tag Overview

Last updated：2024-01-31 16:44:15

Overview

A bucket tag is a key-value pair (key = value), where the tag key and tag value are connected by an equal sign (=), for example: group = IT. It can be used to manage buckets in groups. You can set, query, and delete the tag for a specified bucket.

Specifications and Restrictions

Tag key restrictions

A tag key starting with "qcs:" or "project" is a default tag key and cannot be created.
A tag value can only contain characters encoded in UTF-8, spaces, numbers, or special characters including `+ - =` `. _ : / @` .
A tag key should be a combination of 0-127 characters encoded in UTF-8.
Tag keys are case sensitive.

Tag value restrictions

A tag value can only contain characters encoded in UTF-8, spaces, numbers, or special characters including `+ - =` `. _ : / @` .
A tag value should be a combination of 0-255 characters encoded in UTF-8.
Tag values are case sensitive.

Tag quantity restrictions

Bucket dimension: A resource has at most 50 different bucket tags.
Tag dimension:
A user has at most 1,000 different keys.
A key has at most 1,000 values.
Multiple same keys are not allowed in the same bucket.

How to Use

You can set bucket tags in the console as instructed in Setting Bucket Tag.
If you have set a bucket tag in the COS console, the tag will be automatically obtained when you bind the bucket in the CI console.
If you adjust or delete the bucket tag in the COS console after binding a bucket in the CI console, the bucket tag displayed in the CI console won't change.

Setting Bucket Tags

Last updated：2024-01-31 16:44:15

Overview

A bucket tag is a key-value pair (key = value), where the tag key and tag value are connected by an equal sign (=), for example, group = IT. It can be used to manage buckets in groups. You can set, query, and delete the tags for a specified bucket via the console.

Notes

Each bucket can have up to 50 different bucket tags.
`qcs:` and `project` are reserved fields. Therefore, do not use them in tag keys or tag values. For more limits, see Bucket Tag Overview.

Directions

Adding a tag when binding a bucket

You can add a bucket tag when binding a bucket.

Adding a tag when creating a bucket

You can add a bucket tag when creating a bucket.

Adding a tag to a bound bucket

If you didn't add a tag when binding a bucket, you can perform the following steps to add a tag for your bucket:
1. On the Bucket List page, click the name of the desired bucket to enter the bucket configuration page.
2. Click **Bucket Configuration** on the left, find the **Tagging** configuration item, and click **Add Tags**.
3. Enter the tag key and tag value. Then, click **Save**.

File Management

Last updated：2024-01-31 16:44:15

Overview

CI's storage feature is based on COS, which uses buckets to store objects.
On the file management page, you can view the list of files in the bucket and upload, download, delete, and search for files.

Prerequisites

1. Log in to the CI Console and click **Bucket Management** on the left sidebar to enter the bucket management page.
2. Click the name of the target bucket or **Manage** in the "Operation" column on the right to enter the bucket page.

Uploading File

1. On the file management page, click **Upload Files**. In the pop-up dialog box, click **Select Files** and select a local file for upload.
If workflow is enabled, the uploaded video file will automatically trigger the workflow, and applicable feature fees will be incurred. You can click the drop-down list to view all the workflows enabled under this path. For more information, see Workflow.
2. Click **OK**. If the information of the uploaded video is displayed in the resource list, the upload is successful.

Note:

A single file of up to 512 GB in size can be uploaded in the console. If you need to upload bigger files, please use the multipart upload feature of COS.
If you upload a file that has the same name as an existing file in the bucket, the existing file will be overwritten.

Downloading and Deleting File

After a file is uploaded, you can download or delete it in the "Operation" column on the right. In addition, you can view its information, such as attributes, URL, and size.

Searching for File

You can enter a **filename prefix** in the search box in the top-right corner on the page to search for files.

Bucket Configuration

Last updated：2024-01-31 16:44:15

Overview

The bucket configuration page of CI contains **Basic Info**, **Bucket Tag**, **4xx Image Setting**, and **Original Image Protection**.

Note:

CI is a COS-based data processing service. You can modify bucket configurations, such as the following, in the COS console as instructed in the corresponding documents:

Setting Access Permission

Setting Origin-Pull

Setting Cross-Origin Access

Setting Up a Static Website

Basic Information

Basic Info displays information about the bucket, including the bucket name, bucket ID, region, and its creation time.

Directions

1. Log in to the CI console, click **Bucket Management** on the left sidebar, and click the desired bucket to go to the bucket management page.
2. Click the **Bucket Configuration** tab on the left. In this way, you can find the **Basic Info** of the selected bucket on the right.

Bucket Tag

The tagging feature allows you to manage buckets in categories. In **Bucket Tag**, you can add tags for your buckets and view the configured tags.

Directions

1. Log in to the CI console, click **Bucket Management** on the left sidebar, and click the desired bucket to go to the bucket management page.
2. Click the **Bucket Configuration** tab on the left and find **Bucket Tag** on the right. The configuration items are described as follows:

Tag Key: It is case-sensitive, supporting Chinese characters, uppercase/lowercase letters, digits, and special characters (+, -, _, =, /, ., :, @).
Tag Value: It is case-sensitive, supporting Chinese characters, uppercase/lowercase letters, digits, and special characters (+, -, _, =, /, ., :, @).
3. Click **Save**.

4xx Image Setting

4xx Image Setting is used to configure the content returned for HTTP status codes 4xx. The returned content types include **system image**, **return code**, and **custom image**.

Display Type	Returned Content
System image	200 status code + corresponding image
Return code	HTTP status code
Custom image	200 status code + corresponding image

Directions

1. Log in to the CI console, click **Bucket Management** on the left sidebar, and click the desired bucket to go to the bucket management page.
2. Click **Bucket Configuration** on the left and find **4xx Image Setting** on the right.
3. Click **Edit** and select a **display type** as needed.
System Image: Returns an image with the text "Not available now" or "Accessing failed: The image may be illegal" for 403, 404, and 451 error codes accordingly.
Return Code: Returns the HTTP status code.
Custom Image: If selected, you need to upload three JPG images smaller than 20 KB as the returned images for 403, 404, and 451 status codes, respectively.
4. Click **Save**.

Original Image Protection

CI provides the original image protection service to protect source files from being requested by malicious users. Original image protection needs to be used together with CI's style feature. For more information about the style feature, please see Style Setting. After original image protection is enabled, image files in the bucket can only be accessed at style URLs.

Suppose the original image URL is `http://examplebucket-1250000000.picsh.myqcloud.com/picture.jpg` and the `style1` style has been set for the `examplebucket-1250000000` bucket. Once the original image protection feature is enabled, the image can be accessed only at `http://examplebucket-1250000000.picsh.myqcloud.com/picture.jpg?style1` but not the original image URL.

Note:

The original image protection feature supports only CI domain names, such as `examplebucket-1250000000.picsh.myqcloud.com` .

This feature is usually suitable for scenarios such as **original image resource hotlink protection** and **business anti-cheating**. For example, you can save the watermark parameters as a style and enable original image protection, then the image files in the corresponding bucket can be accessed only at the URLs with the watermark style.

You can also call the Enabling Origin Protection API to enable original image protection.

Directions

1. Log in to the CI console, click **Bucket Management** on the left sidebar, and click the desired bucket to go to the bucket management page.
2. Click **Bucket Configuration** on the left and find **Original Image Protection** on the right.
3. Click **Edit**, change **Status** to **Enabled**, and select **Image Type**. `*` indicates enabling original image protection for all image types.
4. Click **Save**.

Managing Domain Names

Last updated：2024-01-31 16:44:15

Basic Concepts

Images stored in a bucket can be processed and recognized by CI and downloaded through the CI domain name. You can access the images stored in a bucket at the following addresses:

System-assigned domain name

CDN acceleration domain name

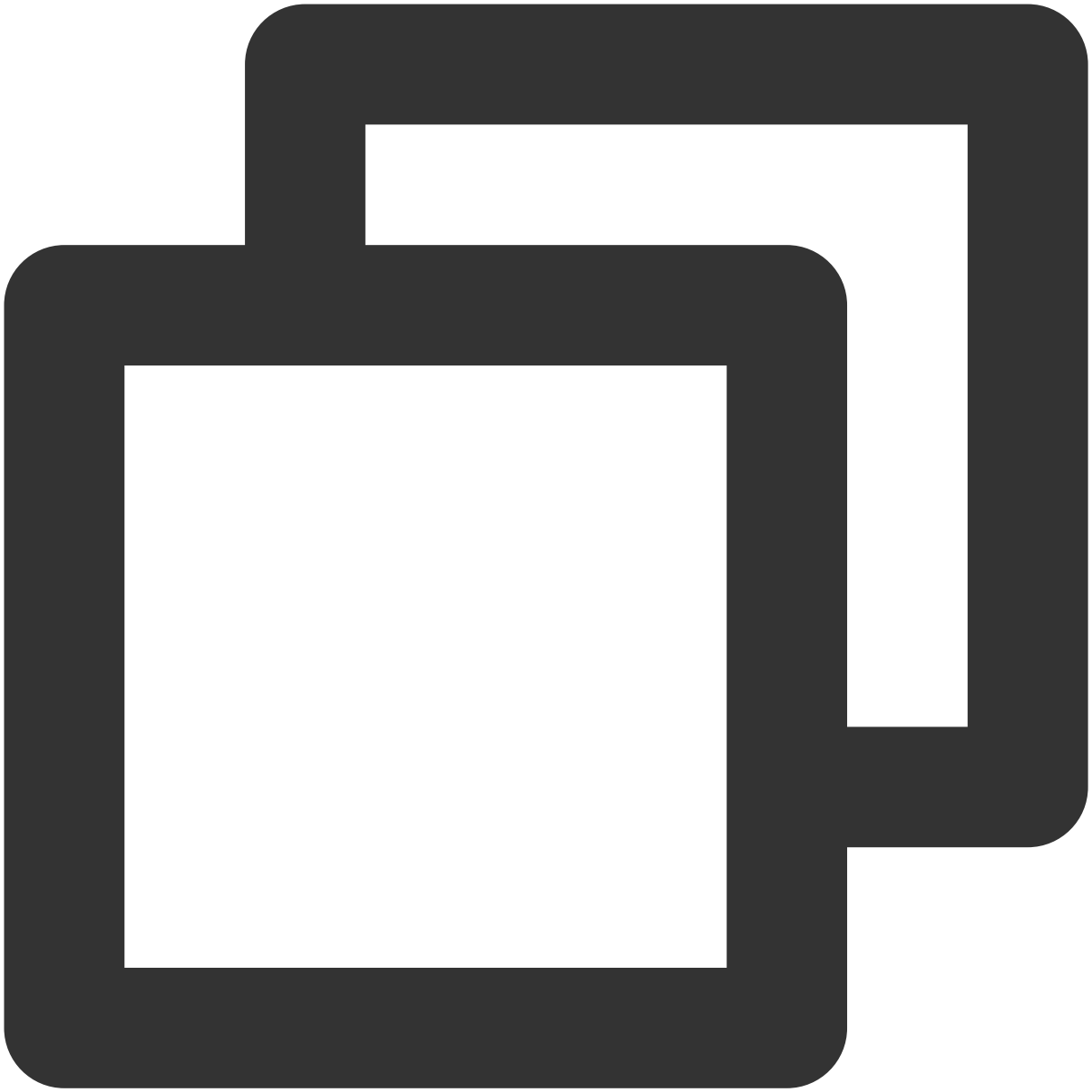
Custom domain name

Note:

Some users' CI domain names have been merged with COS domain names. If this is the case for your account, you can directly use the COS domain name to process images, and the **Domain Management** configuration page will not be present in the CI Console. In this case, you can log in to the COS Console, find the target bucket, and configure the domain name for it. For more information, please see Overview.

System-Assigned Domain Name

This domain name is defined by Tencent Cloud and cannot be changed. If you use it in a Tencent Cloud service to access an image resource, the request will be sent and received over the private network; if you use it for access over the public network, the request will be sent to CI for the file over the public network. After a bucket is created, Tencent Cloud will automatically generate a system-assigned domain name in the following format:

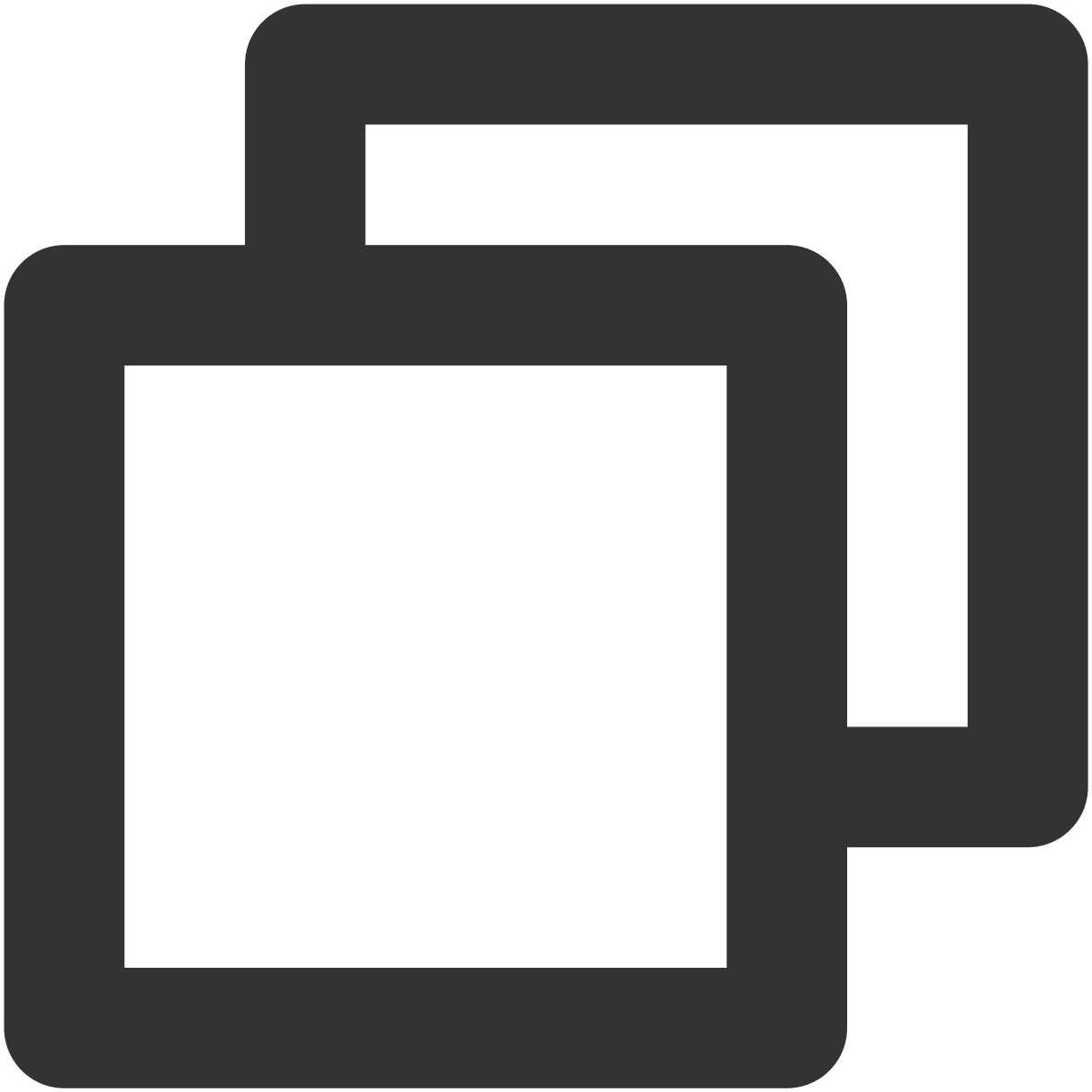


```
[BucketName-APPID].pic[area].myqcloud.com
Example: test-1250000000.picgz.myqcloud.com
```

Note:

This domain name cannot be changed.

To get the URL of a resource in a bucket, add the relative path after the domain name of the bucket as follows:



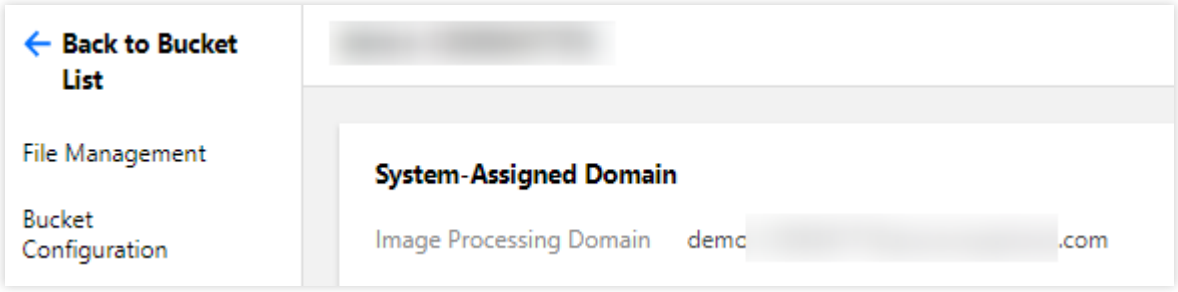
```
http://testbucket-1250000000.picgz.myqcloud.com/test.txt
```

Note:

If the resource is private, you need to add the signature suffix after the above URL.

Viewing system-assigned domain name

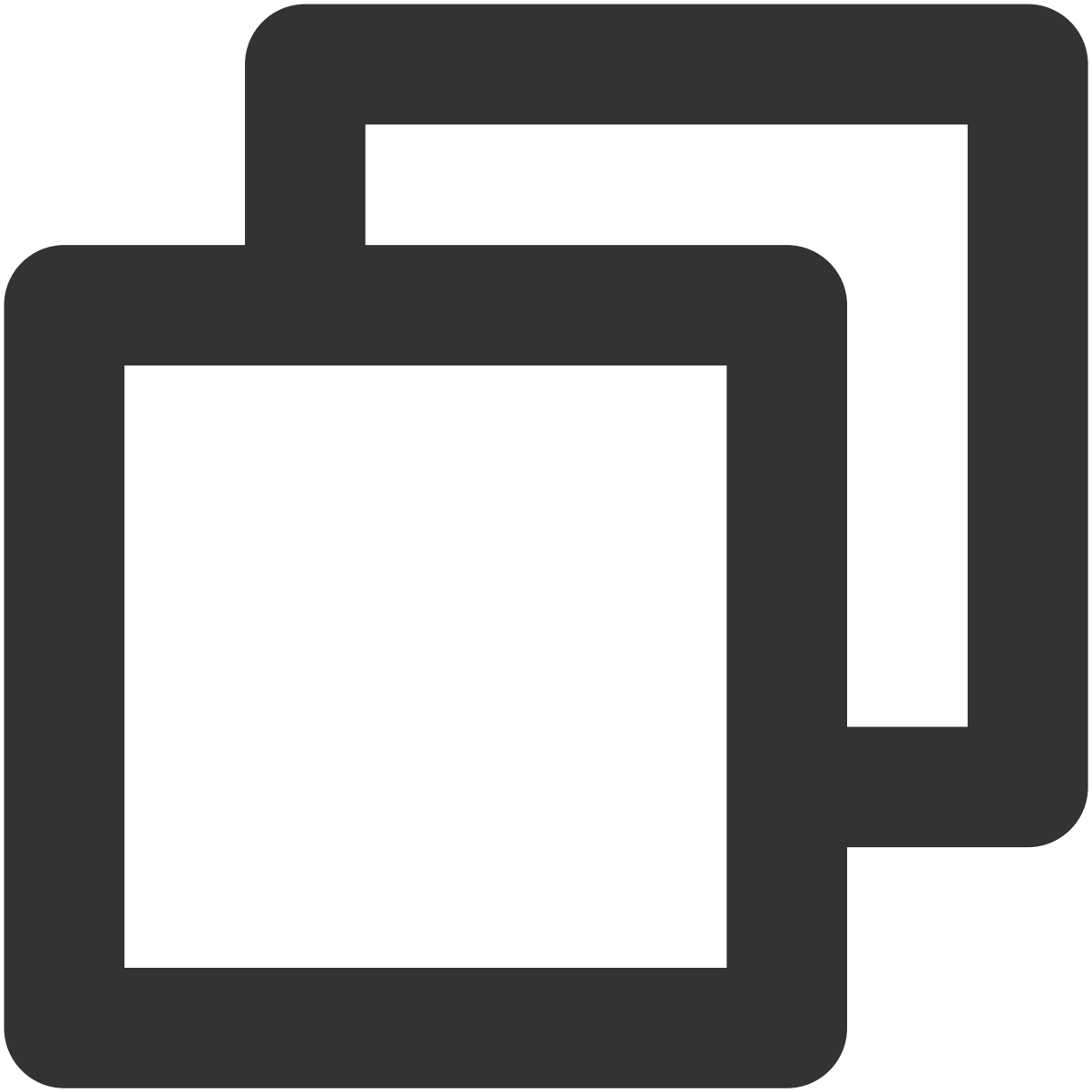
1. Log in to the CI Console and click **Bucket Management** to enter the bucket page.
2. Select the target bucket to enter the bucket management page.
3. Click **Domain Management** to view the system-assigned domain name.



System-assigned domain name - cross-region access over private network: a system-assigned domain name can be used for access between different Tencent Cloud services in the same region. If you want to implement cross-region access over the private network, for example, a CVM instance in the Guangzhou region needs to use data in a CI bucket in the Singapore region, then you need to use a VPC to deploy a dedicated network tunnel for fast access. For more information, please see Virtual Private Cloud.

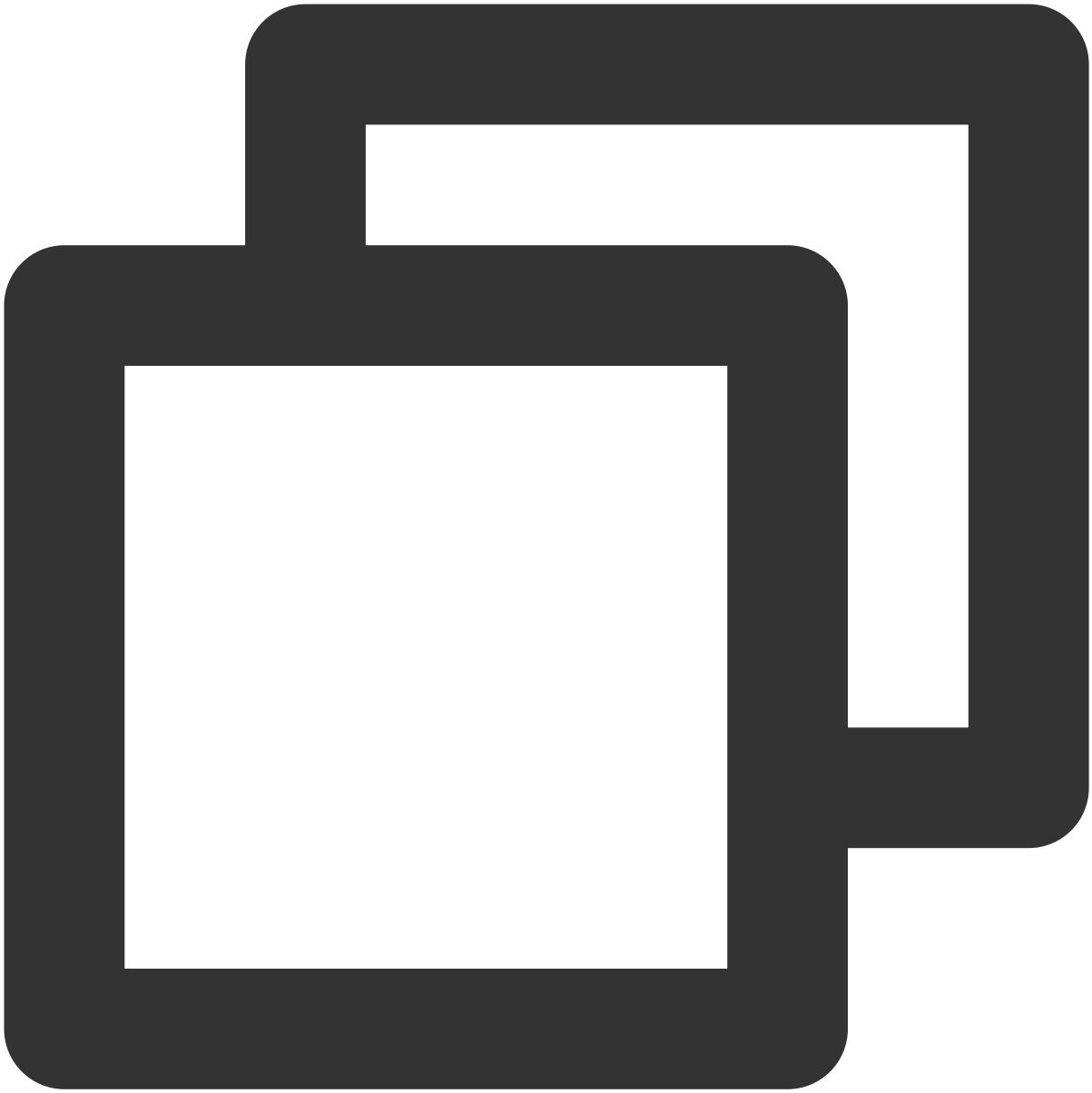
CDN Acceleration Domain Name

A CDN acceleration domain name is initialized by Tencent Cloud and can be changed (with a CNAME record required). It can be used to get higher bandwidth and lower wait latency. After a bucket is created, Tencent Cloud will generate a CDN acceleration domain name in the following format by default:



```
[BucketName-APPID].image.myqcloud.com
```

You can enable CDN acceleration when creating a bucket or in **Domain Management** after creating it. For more information, please see Configuring CDN acceleration domain name. Once enabled, the CDN acceleration domain name can be directly accessed over the public network as follows:



```
http:// testbucket-1250000000.image.myqcloud.com/testdir/test.jpg
```

In this way, the CDN acceleration domain name will be also added in the CDN Console.

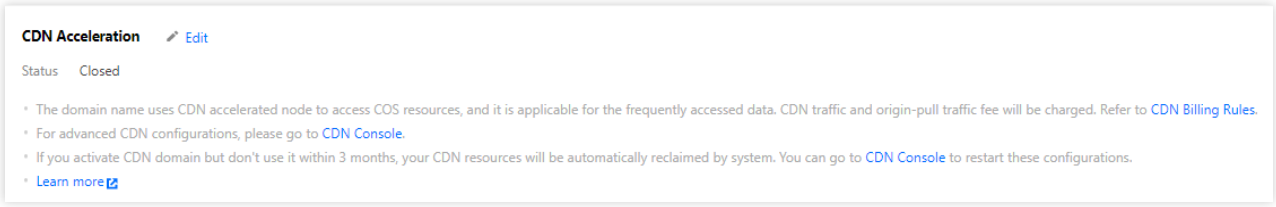
Note:

Up to 100 CDN acceleration domain names can be created under one `APPID` .

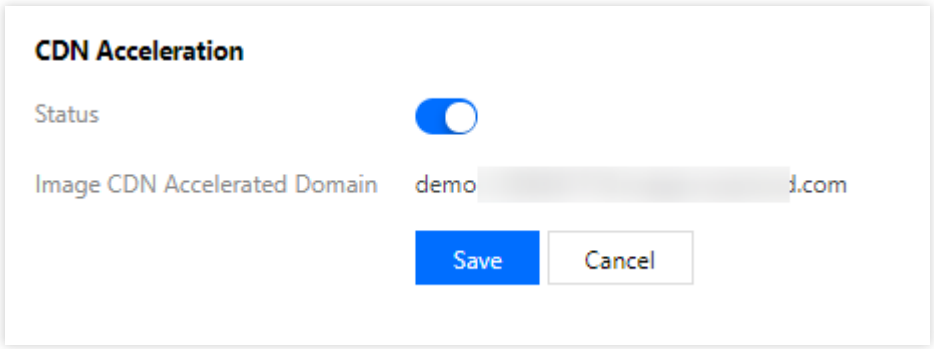
Configuring CDN acceleration domain name

1. Log in to the CI Console, click **Bucket Management** on the left sidebar, and click the target bucket (such as `imagetest`) to enter the bucket.

2. Click **Domain Management** to enter the domain name management page and click **Edit** next to "CDN Acceleration" to enter the configurable page.



3. Modify the current status and click **Save**.



Custom Domain Name

You may not want to display the domain name such as `qcloud.com` for your website or business based on your actual needs. For example, if your website is hosted in Tencent Cloud, you may choose `http://myblog.net/` preferably instead of `http://myblog-1250000000.image.myqcloud.com` . To satisfy this need, you can use a custom domain name by creating a CNAME record in the CDN Console to map `http://myblog.net/` to `http://myblog-1250000000.image.myqcloud.com` .

You can add a custom domain name to directly point to the bucket. After being bound, the custom domain name can be used to directly access the contents in the bucket. After adding a custom domain name, you can enable CDN acceleration for faster access. To avoid security problems involved in the business, we recommend you use a custom domain name to access image files in CI.

Note:

After adding a custom domain name, to ensure that CI can be accessed normally through it, you need to modify the CNAME record of the DNS first for it to take effect.

The bound custom domain name needs to have an ICP filing from MIIT; otherwise, it cannot be accessed.

Custom domain names do not support configuration of HTTPS certificates. If you need to use such a certificate, please enable CDN acceleration and bind a CDN domain name.

Configuring custom domain name

Binding

1. Log in to the CI Console, click **Bucket Management** on the left sidebar, and click the target bucket (such as `imagetest`) to enter the bucket.
2. Click **Domain Management** to enter the domain name management page. In the **Custom Domain** configuration item, click **Add Custom Domain** to add your existing domain name.
3. Copy the CNAME address.
4. Enter the DNSPod Console and click the bound custom domain name.

Note:

Please configure at your corresponding DNS service provider. Here, Tencent Cloud DNS is used as an example.

5. Click **Add Record** to add a CNAME record.

Note:

The record value is the copied CNAME address. Once added, it will take effect in about 15 minutes. Please wait patiently.

Verifying result

After the custom domain name is bound, you can use its addresses to download files in the bucket. Suppose an `index.htm` file is in your `testnew` bucket, and the bound custom domain name is `www.srcostest.com`:

Before binding:

You can use the public network access address of the system-assigned domain name plus the file path for access, such as `testnew-1250000000.image.myqcloud.com/index.htm`.

*After binding:**

You can use the custom domain name address plus the file path for access, such as `www.srcostest.com/index.htm`

Note:

You can enable the static website feature to directly open files in the browser through the custom domain name. For more information on how to enable it, please see Setting Static Website.

Hotlink Protection Setting

Malicious websites may use your image links without authorization and misappropriate the image traffic, causing you economic losses. To prevent this, CI provides a hotlink protection feature, which can recognize and manage sources with the referer mechanism supported by the HTTP protocol.

1. Log in to the CI Console, click **Bucket Management** on the left sidebar, and click the target bucket (such as `imagetest`) to enter the bucket.
2. Click **Domain Management**, scroll down and find **Hotlink Protection Setting** to configure hotlink protection.

Note:

For some users, the **Hotlink Protection Setting** configuration page will no longer be displayed in the CI Console. If this is the case for your account, you can go to the COS Console for configuration. For more information, please see Setting Hotlink Protection.

You can add websites to the referer blocklist/allowlist. You can add multiple domain names separated by line breaks (one entry per line) and use wildcards.

After hotlink protection is enabled, service source can be limited according to policy.

Image Processing
Basic Processing

Last updated：2024-01-31 16:44:15

Style Separators

Overview

A style separator is a character that separates the filename and the processing style. The separator can be a hyphen (-), underscore (_), slash (/), or exclamation mark (!).

Directions

1. Log in to the CI console and click **Bucket Management** in the left sidebar.
2. Click the name of the desired bucket (e.g., `buckettest`) to go to the bucket management page.
3. Select the **Image Processing** tag. Then, click **Basic Processing**, find the **Style Separator** area, and click **Edit** to select one or more style separators.
4. Click **Save**.

Instructions

URL format: http:// Bound domain/Filename + Separator + Style name

Assume that you have selected the exclamation (!) as the separator, the style name is `yunstyle`, and the input image's `fileid` is `sample.jpg`. The URL of the stylized image will be `http://space.image.com/sample.jpg!yunstyle`. If a signature needs to be carried, the URL will be `http://space.image.com/sample.jpg!yunstyle?q-sign-algorithm=<signature>`, where `/sample.jpg!yunstyle` will be used to calculate the signature `<signature>`.

Note:

You can set up to 100 styles for each bucket.

To avoid ambiguity, do not use separators in style names.

The settings take effect in about 30 minutes on average.

Changing separators requires purging the cache. It takes at least 24 hours for separator changes to take effect for both public and private networks.

Canceling a separator used may cause product feature malfunctions.

Style Management

Style management allows you to **preview**, **edit**, **delete**, or **export** a style. You can also import a style or use the visualization method to **add a style**.

Style overview

You can set styles for images in the bucket to manage images as needed. A style is an alias of a set of parameters that process images in real time upon download.

Adding styles

You can import styles in batches using an import rule. Alternatively, you can add styles using the visualization method. The following describes how to add styles using the visualization method:

1. Log in to the CI console and click **Bucket Management** in the left sidebar.
2. Click the name of the desired bucket (e.g., `buckettest`) to go to the bucket management page.
3. Select the **Image Processing** tab. Then, click **Basic Processing** and find the **Style Management** area.
4. Click **Add Styles** to edit the style as instructed below.

Style Name

Style names are case-sensitive.

To avoid ambiguity, do not use separators in style names.

Once saved, a style name cannot be modified.

Editing Mode

Basic: You can set the style using the visualization method.

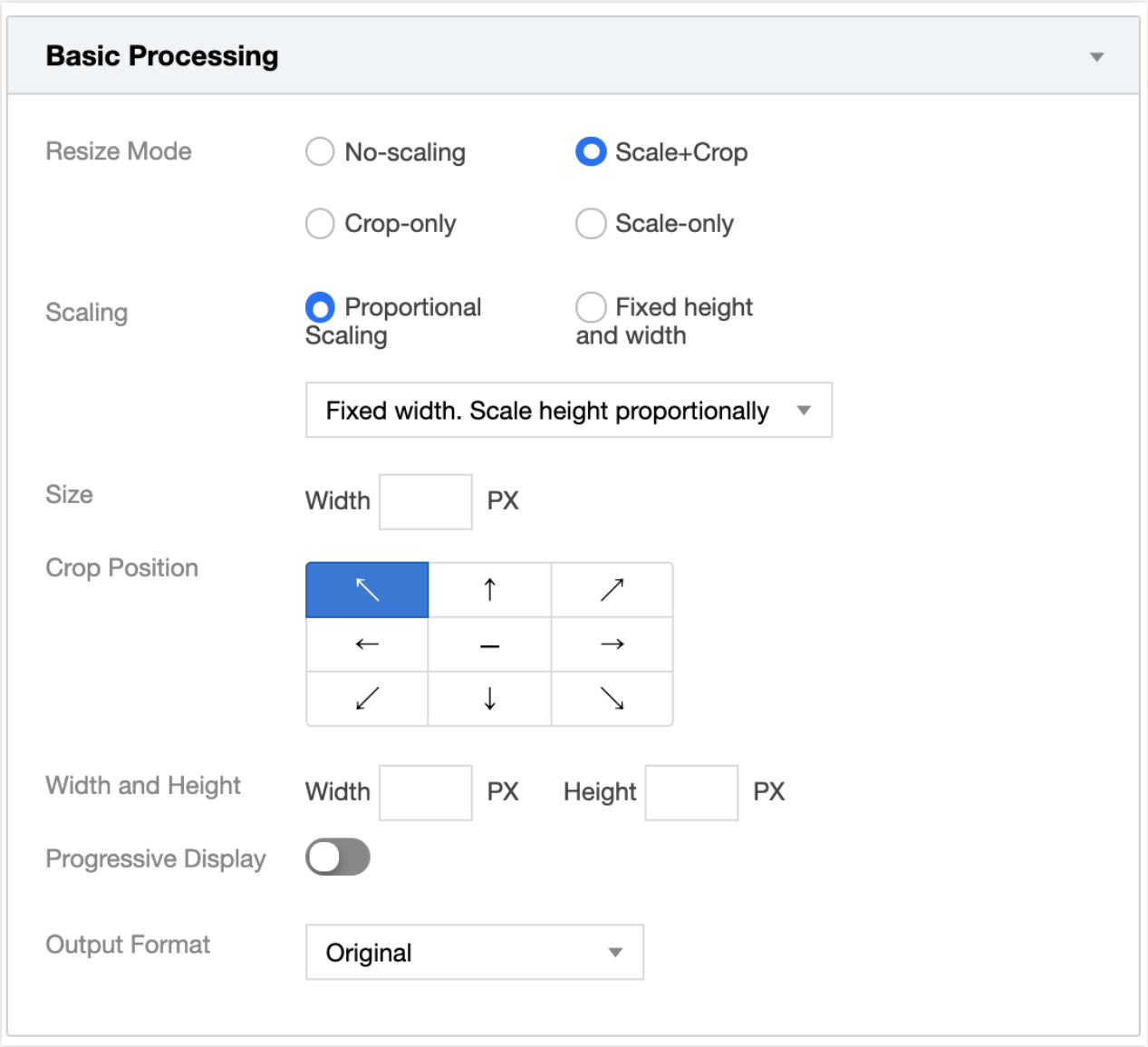
Advanced: You can set styles using parameters. For more information, please see the API documentation of Basic Image Processing.

Basic editing mode

You can use the basic editing mode to set the resizing mode, progressive display effect, output format, output effect, text watermark, image watermark, and more.

Basic processing

CI supports the scale+crop, crop-only, and scale-only resizing modes. Resizing is optional. Therefore, you can set it to **No-scaling** as needed.



Note:

CI's scaling operation enlarges or shrinks images without stretching them.

Scale+crop

When the output image needs to be smaller than the input image and have a different aspect ratio, you can use the **scale+crop** mode to scale the image to the thumbnail size, and then crop it according to the specified crop position as well as the width and height. A 3x3 grid is used to decide the crop position.

Proportional scaling: scales an image according to the specified width without changing the original aspect ratio.

Fixed height and width: scales an image according to the specified width and height. For example, if the input image resolution is 1200×900 and the thumbnail resolution is 600×600, the input image is first cropped according to the thumbnail aspect ratio (that is, 600:600 or 1:1) to 900×900, and then scaled down to the target resolution of 600×600.

Crop-only

The **crop-only** mode crops the input image according to the specified crop position and thumbnail size. A 3x3 grid is used to decide the crop position.

Assume that you set the crop position to **center** and the thumbnail resolution to 600×600. Then, the image is cropped starting from the center of the input image, and 300 pixels at each direction along the horizontal axis and vertical axis will be retained to form a 600×600 thumbnail.

Scale-only

The **scale-only** mode scales the image according to the specified resolution.

Scale proportionally: scales the image according to specified width without changing the original aspect ratio.

Fixed height and width: scales the image according to the specified width and height, with the original aspect ratio ignored.

Text watermark

You can add a text watermark with the text, font, font size, color, and opacity specified. A 3x3 grid is used to decide the watermark position.

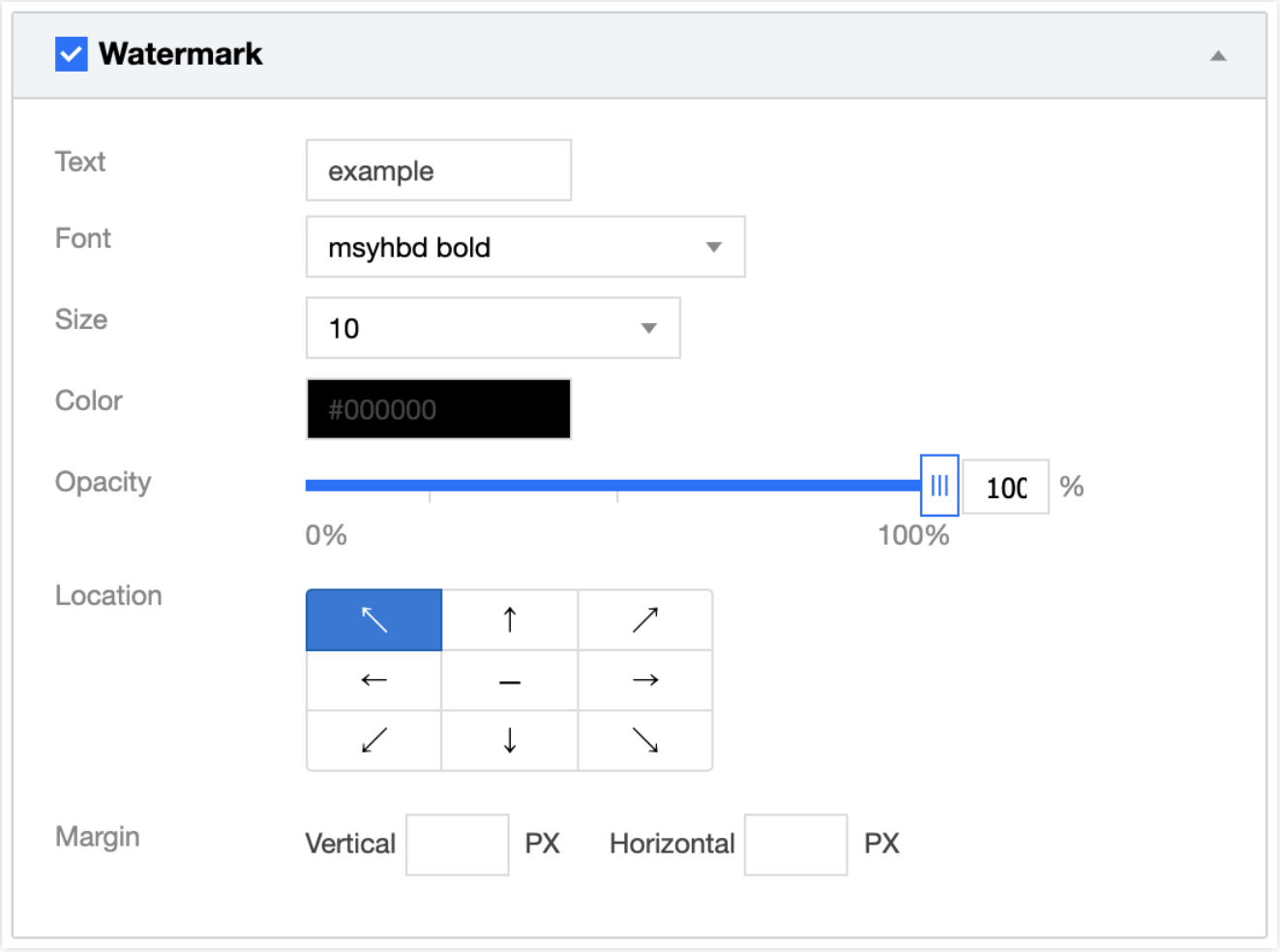
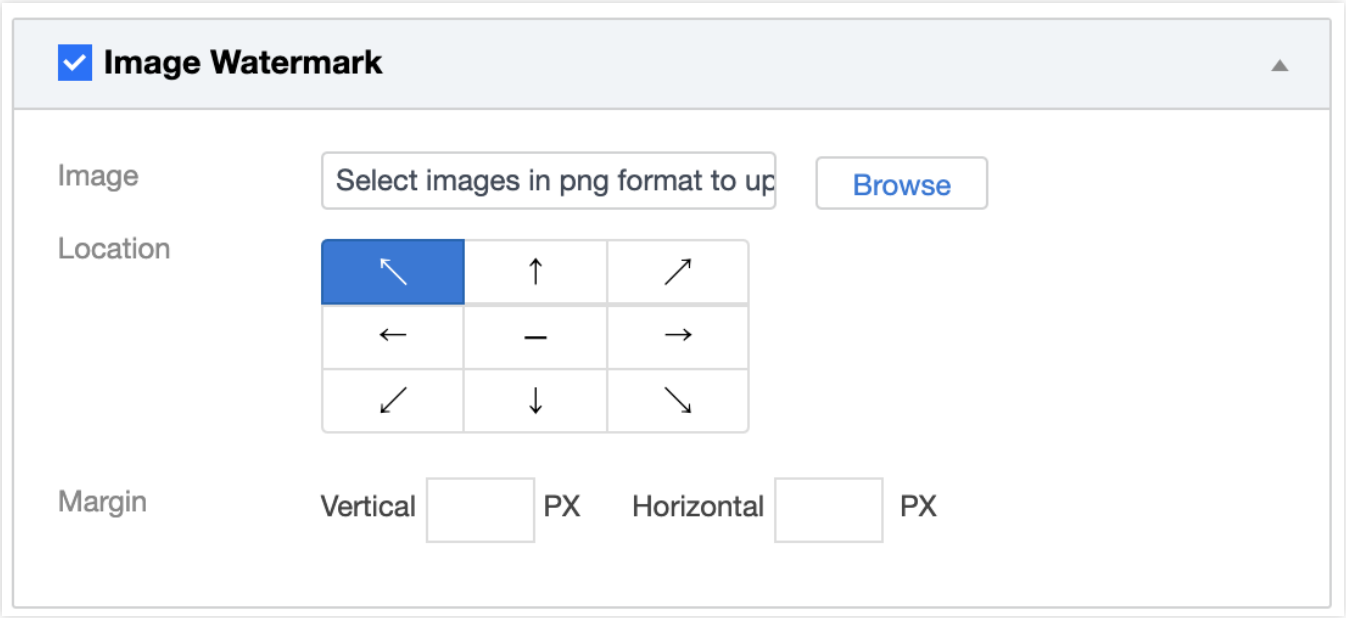


Image watermark

You can overlay an image watermark over the input image. A 3x3 grid is used to decide the watermark position.



Blind Watermark

Last updated：2024-01-31 16:44:15

Overview

This document provides an overview of APIs and SDK code samples for blind watermarking.

SDK API References

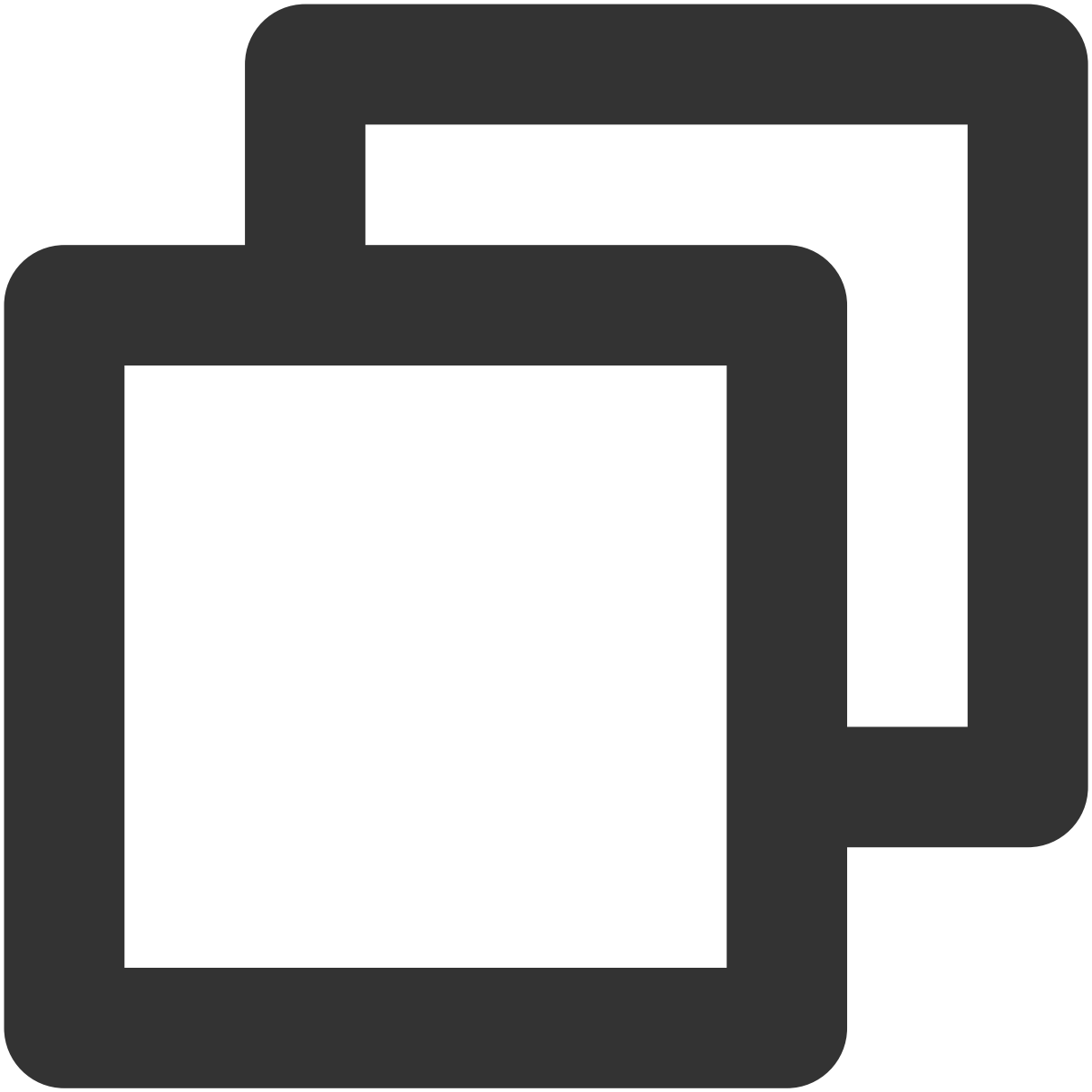
For the parameters and method description of all the APIs in the SDK, see the API documentation.

Adding Blind Watermark

Feature description

You can add a blind watermark when uploading or downloading an object.

Sample 1: Adding a blind watermark during upload



```
PutObjectRequest request = new PutObjectRequest(bucket, key, srcPath);

JObject o = new JObject();
// Do not return the input image
o["is_pic_info"] = 0;
JArray rules = new JArray();
JObject rule = new JObject();
rule["bucket"] = bucket;
rule["fileid"] = key;
// Processing parameters. For rules, visit https://cloud.tencent.com/document/produ
rule["rule"] = "watermark/3/type/<type>/image/<imageUrl>/text/<text>/level/<level>"
```

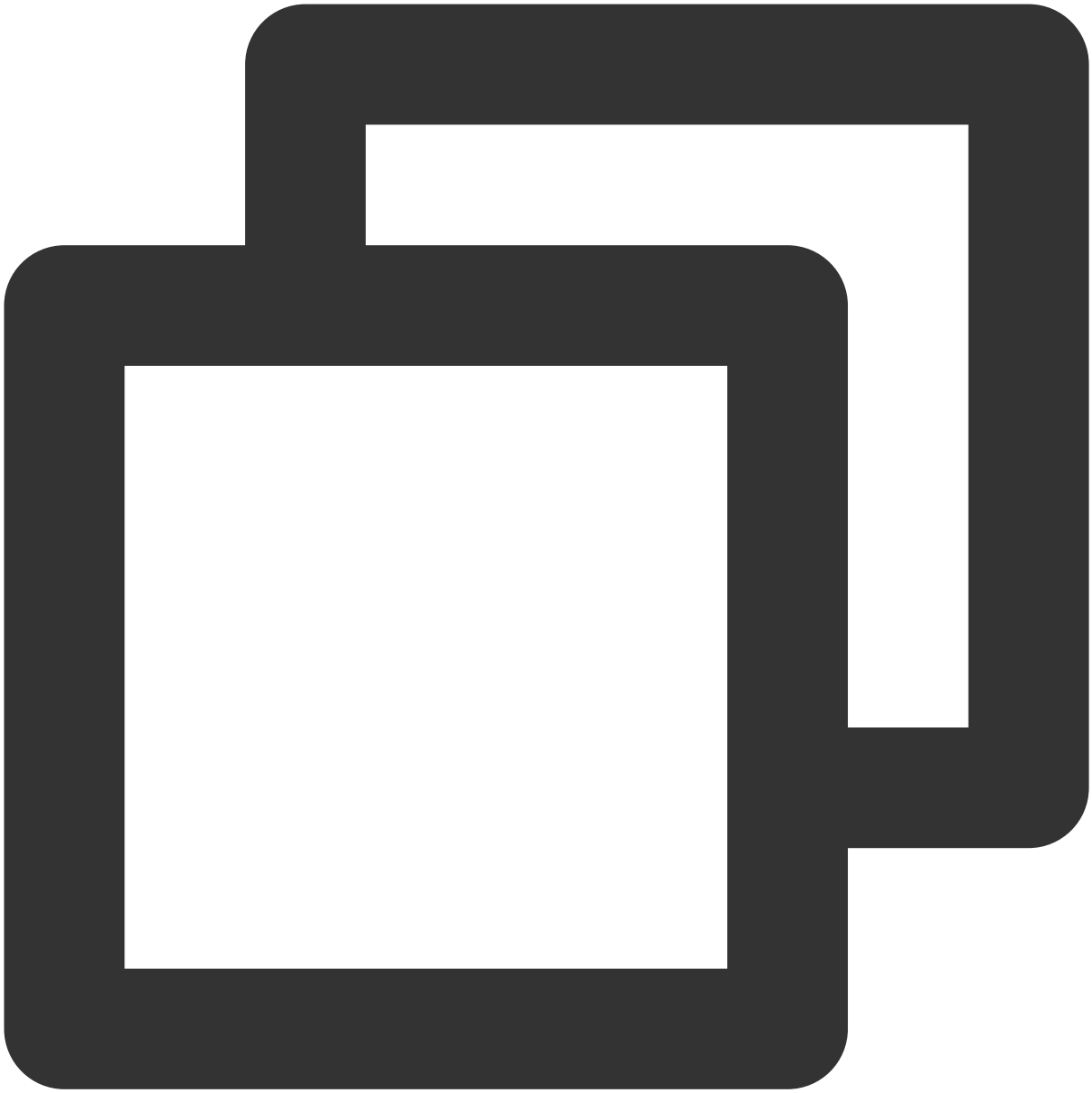
```
rules.Add(rule);
o["rules"] = rules;

string ruleString = o.ToString(Formatting.None);
request.SetRequestHeader("Pic-Operations", ruleString);
// Execute the request
PutObjectResult result = cosXml.PutObject(request);
```

Note:

For more complete samples, visit GitHub.

Sample 2: Adding a blind watermark during download



```
GetObjectRequest getObjectRequest = new GetObjectRequest(bucket, key, localDir, loc
// Processing parameters. For rules, visit https://cloud.tencent.com/document/produ
getObjectRequest.SetQueryParameter("watermark/3/type/<type>/image/<imageUrl>/text/<

GetObjectResult result = cosXml.GetObject(getObjectRequest);
```

Note:

For more complete samples, visit GitHub.

Image Compression Service
Guetzli Image Compression

Last updated：2024-01-31 16:44:15

Overview

CI's Guetzli image compression feature is a **visually lossless** compression service. It compresses **JPG images** at a high ratio to reduce the downstream traffic usage and accelerate downloads. By leveraging human eyes' insensitivity to specific color gamuts and details, Guetzli discards specific details to reduce the image size by 35% to 50% without changing the quality.

Directions

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket management page.
3. Click the name of the target bucket.
4. On the left sidebar, click **Image Processing**.
5. Find the **Guetzli Image Compression** configuration item and click **Edit** to change its status to **Enabled**.
6. Click **Save**.

Note:
After you enable Guetzli, **the original JPG image will be returned if you access the image for the first time**, and Guetzli will compress the image asynchronously. If you request the image again after the compression is completed, the compressed image will be returned.
Currently, Guetzli can process JPG images with the quality being greater than 70 and the number of pixels being smaller than 16 million.
Guetzli is a paid feature. For billing details, see Billing Overview.

Guetzli Status Codes

After Guetzli image compression is enabled, `x-GuetzliState` will be added to the HTTP request headers for images in the bucket to indicate the Guetzli compression status as described below:

x-GuetzliState Status Code	Description
< 0	The image cannot be processed as the compression requirements are not met.

0	Guetzli compression is not performed.
1	The Guetzli compression request has been initiated.
2	Guetzli compressing is in progress.
3	The image is not processed as the input image cache has not expired.
100	Compressed successfully.

Image Advanced Compression

Last updated：2024-01-31 16:44:15

Overview

CI's Image Advanced Compression allows you to easily convert images into formats that provide a high compression ratio, such as TPG and HEIF. This effectively reduces the transmission time, loading time, and the use of bandwidth and traffic.

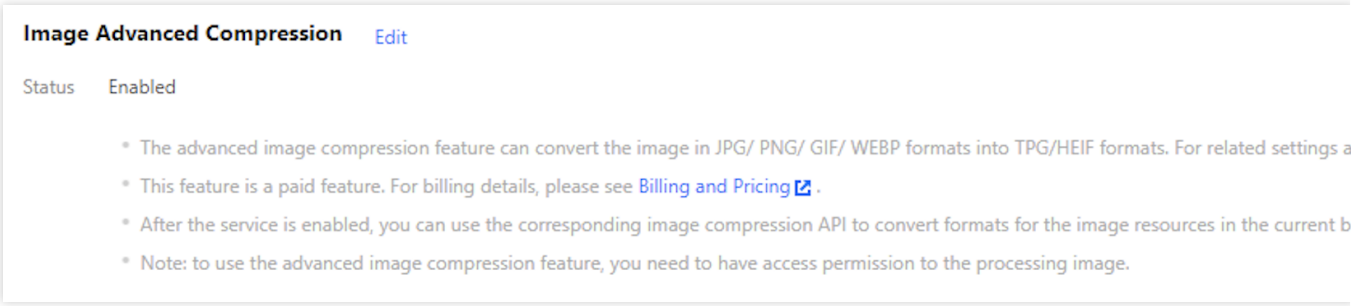
Feature	Description
TPG compression	TPG is a Tencent-designed image format. Converting JPG, PNG, or WebP images into TPG greatly reduces the image sizes.
HEIF compression	If your images are used in iOS environments, you can convert them from JPG, PNG, GIF, WebP, or other formats into HEIF, which offers an ultra-high compression ratio.

Note:
To use the TPG format, ensure that **the environment where images are loaded supports TPG decoding**.
Tencent Cloud's multimedia laboratory provides TPG decoder-integrated SDKs for iOS, Android, and Windows clients to facilitate quick integration with TPG.
Currently, iOS 11 or later and Android P have native support for the HEIF format.
For the pricing of Image Advanced Compression, please see Billing and Pricing.

Directions

To use Image Advanced Compression, you need to enable it on the bucket configuration page first. Once it is enabled, you can call the Image Advanced Compression APIs to compress images in the bucket into TPG/HEIF upon the download.

1. Log in to the CI console.
2. Click **Bucket Management** in the left sidebar.
3. Click the name of the desired bucket.
4. Click **Image Processing** and then select the **Basic Processing** tab at the top.
5. Find the **Image Advanced Compression** area, click **Edit**, enable the status, and click **Save**.



Content Moderation
Moderation Details

Last updated：2024-01-31 16:44:15

Overview

After enabling sensitive content moderation, you can view the moderation results by condition and manually process them on the **Moderation Details** page.

Directions

Filtering results

1. Log in to the CI console.
2. On the left sidebar, select **Bucket Management** to enter the **Bucket Management** page.
3. Click the name of the target bucket to go to the configuration page.
4. On the left sidebar, select **Sensitive Content Moderation** > **Moderation Details** to enter the **Moderation Details** page.
5. Select the conditions as needed.

Scope: You can view the results of moderation through API calls, automatic moderation, and historical data moderation.
File type: You can view the moderation results of images, videos, audios, and text.
Detection Scenario: You can view the moderation results for pornographic, illegal or non-compliant, or advertising content detection or all scenarios of the selected file type.
Moderation Result: Moderated files are categorized into three types: sensitive, suspected, and normal files. You can view a type of file or all files.
Sensitive: Images whose score falls within the range of [91,100].
Suspected: Images that are suspected to be sensitive and whose score falls within the range of [61,90]. For such images, the system cannot determine whether they are sensitive, so we recommend you determine it through human moderation.
Normal: Images whose score falls within the range of [0,60].
Block Status: You can view the moderation results of blocked, normal, or all files.
Moderation time: You can view the moderation results in the specified time period.

Note:

If you rename a file or modify its metadata, the file will be considered a newly uploaded file and have a new moderation result.

Image Score: If you select **All** for **Moderation Result**, you can filter files by customizing the file moderation score interval.

Object Name: You can enter a filename to view the moderation result of the specified file.

6. Click **Query** to view the moderation results.

Note:

The **Moderation Details** page only displays the details of moderations called in the console but not those called through an API or SDK.

Exporting results

After filtering results, click **Export** to export the results as a .csv or .xlsx file.

The fields in the moderation result file are as detailed below:

Field	Name	Description
recordID	Record ID	Unique record ID of the moderation result.
fileName	Filename	Name of the moderated file.
size	Size	Size of the moderated file.
scene	Moderation type	You can select **Porn**, **Ad**, **Illegal**, or **Abuse**.
state	Moderation result	`Normal` : Normal file. `Possible` : Suspiciously sensitive file. `Convince` : Sensitive file.
freeze	Whether the file is blocked	`Yes` : Blocked. `No` : Not blocked.
score	Moderation score	The confidence the moderation result hits the moderation scene. Value range: 0–100. The higher the value, the more likely the content hits the currently returned moderation scene. For example, `Porn 99` means that the content is very likely to be pornographic.
createTime	Creation time	Creation time of the moderated file.
resourcePath	Resource path	Storage path of the moderated file.
sourceUrl	Source URL	URL of the moderated file.

Manually moderating results

After you filter results, the **Moderation Details** page will show filtered results, and you can perform the following operations on the filtered results:

Block an image or set its status to **Normal**.

Click a moderated image to view its details.

Setting Moderation Policy

Last updated：2024-01-31 16:44:15

Overview

When you use the content moderation service, you can specify a moderation category through a moderation policy to moderate content in custom scenes. For different file types, CI provides different scenes for your choice, making it easier for you to customize moderation policies that suit your business.

Currently, the file types and corresponding moderation scenes supported by CI are as follows:

Supported File Types	Moderation Scenes	Specific Moderation Categories
Image moderation policy, video moderation policy, audio moderation policy, text moderation policy, file moderation policy	Pornographic content	Sexually suggestive/vulgar behaviors
		Genital nudity/Sexual behaviors
		Sex toys
		Sexy content
		Pornographic text moderation
	Advertising content	QR code and barcode recognition
		Logo detection and recognition
		Advertising text moderation
	Other non-compliant content	Fire, explosion, bloody scene, etc.

Note:

WEBP images involving advertising QR codes cannot be moderated currently.

Directions

Default policy

Each moderation type has a default moderation policy, which is configured by Tencent Cloud based on your historical moderation conditions. If you have never used the moderation service, the policy developed by algorithm experts based on models for multiple industries will be used by default, which will be suitable for most content security requirements.

Note:

The default policy can be viewed and edited but not deleted.

Custom policy

If the default policy cannot meet your business needs, or you have multiple scenes that require different moderation policies, you can create custom policies as needed.

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar.
3. Click the name of the target bucket to enter the configuration page.
4. Select **Content Moderation** > **Moderation Policy** on the left sidebar.
5. Create a moderation policy based on your business needs. Currently, you can create policies for **image moderation**, **video moderation**, **audio moderation**, **text moderation**, and **file moderation**.

Take the image moderation policy as an example:

i. Click **Create Image Moderation Policy** and enter the policy name.

ii. Select the category you need to moderate under the moderation type, where OCR pornographic text moderation indicates to moderate image content based on OCR.

iii. Click **Save** to create the policy.

6. After the moderation policy is created, the backend will automatically generate a unique `Biztype` value.
7. You can view or edit the created moderation policy; however, you cannot change its name and `Biztype` value.

Using moderation policy

After the moderation policy is created, during the configuration of automatic auditing, creation of historical data audit tasks, and invocation of the content audit API interface, you are required to select the corresponding strategy. This allows for auditing to be conducted in accordance with your custom classifications.

Automatic moderation

Create an automatic moderation configuration in the console, and you can manually select a moderation policy.

Historical data moderation

Create a historical data moderation job in the console, and you can manually select a moderation policy.

Moderation APIs

When calling an API for content moderation, you can manually pass in the `Biztype` value to the API, which you can view in the list of moderation policies in the console. If you don't pass it in, the default policy will be used.

Configuring Custom Graphic Risk Library

Last updated：2024-01-31 16:44:15

Feature Overview

The custom image risk library is designed to help you manage images or keywords that need to be moderated. With risk library customization, you can configure the images or keywords to allow or block them. This can be applied to all moderation scenes.

Image Risk Library

You can use an image risk library to manage images that need to be blocked or allowed, to address unexpected control requirements.
Six preset image risk libraries are available in the system:
Normal image library: The returned moderation result will be normal for images that match those in this library.
Pornographic and illegal image library: The returned moderation result will be the corresponding violation tag for images that match those in the library.
Creating new image risk library is not supported. You can add sample images to the existing default libraries.
Note:
The image risk library is effective by account. After you add sample images to the gallery in any bucket under the same account, these images will automatically take effect in all your buckets and all your moderation policies.
A single image library can contain a maximum of 10,000 sample images.
Some specific images may fail to be added to the image library. In this case, please contact us for assistance.

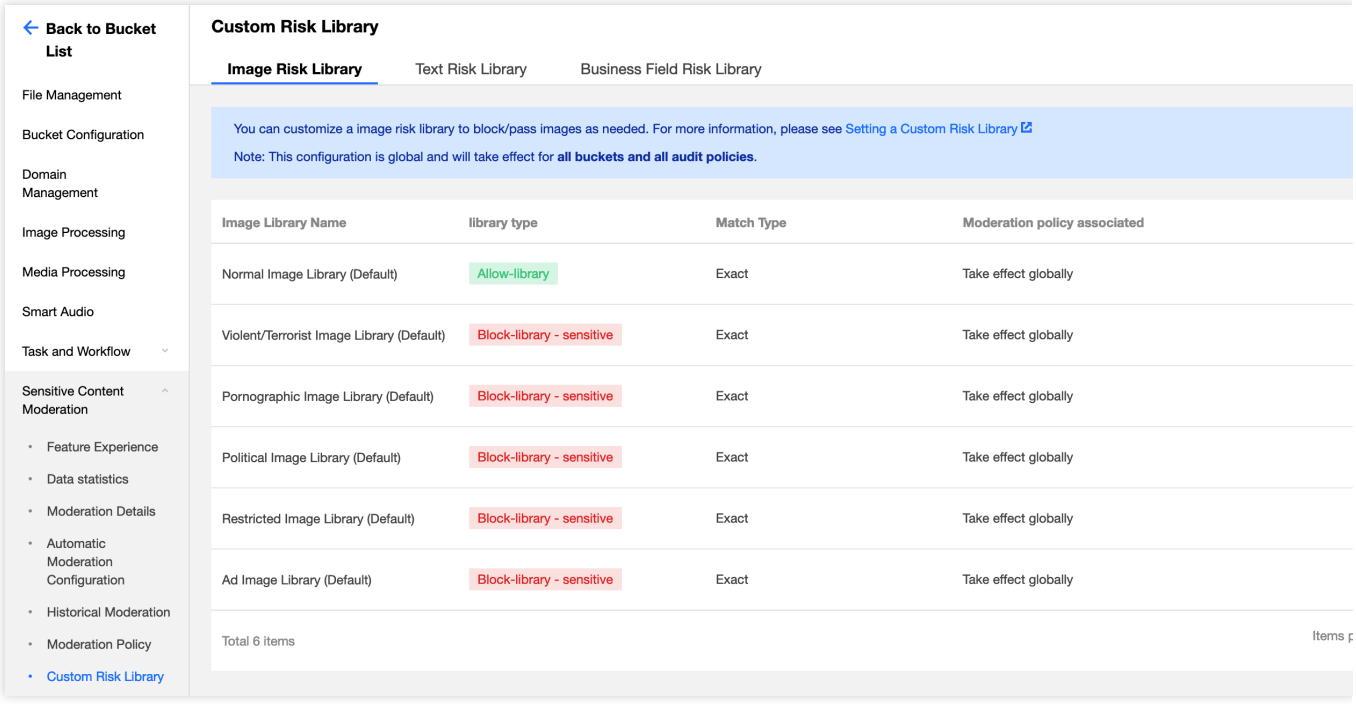
Text Risk Library

You can use the text risk library to manage text to be blocked or allowed, in order to address sudden control requirements.
The text risk library contains the following types:
Pre-defined text library: It is a text library with pre-defined policies for you, which includes:
Normal text library: If a keyword in the library is matched, the moderation result will be returned as normal.
Pornographic text library, illegal text library, and other text libraries: If a keyword in the library is matched, the moderation result will be returned as the corresponding violation tag.
Note

The pre-defined text library takes effect by account. After you add sample keywords to any pre-defined text library for the same account, these keywords will automatically take effect in all your storage buckets and all moderation policies. Up to 10,000 sample keywords can be added to a pre-defined text library.
Custom text library: It is the text library you create, where you can add samples of various types of violations. If the text under moderation matches a keyword in the library, it will be marked with the corresponding tag based on the defined library policy.
Note
The custom text library needs to be associated with a moderation policy and only takes effect within the associated moderation policy.
Up to 2,000 sample keywords can be added to a single custom text library.

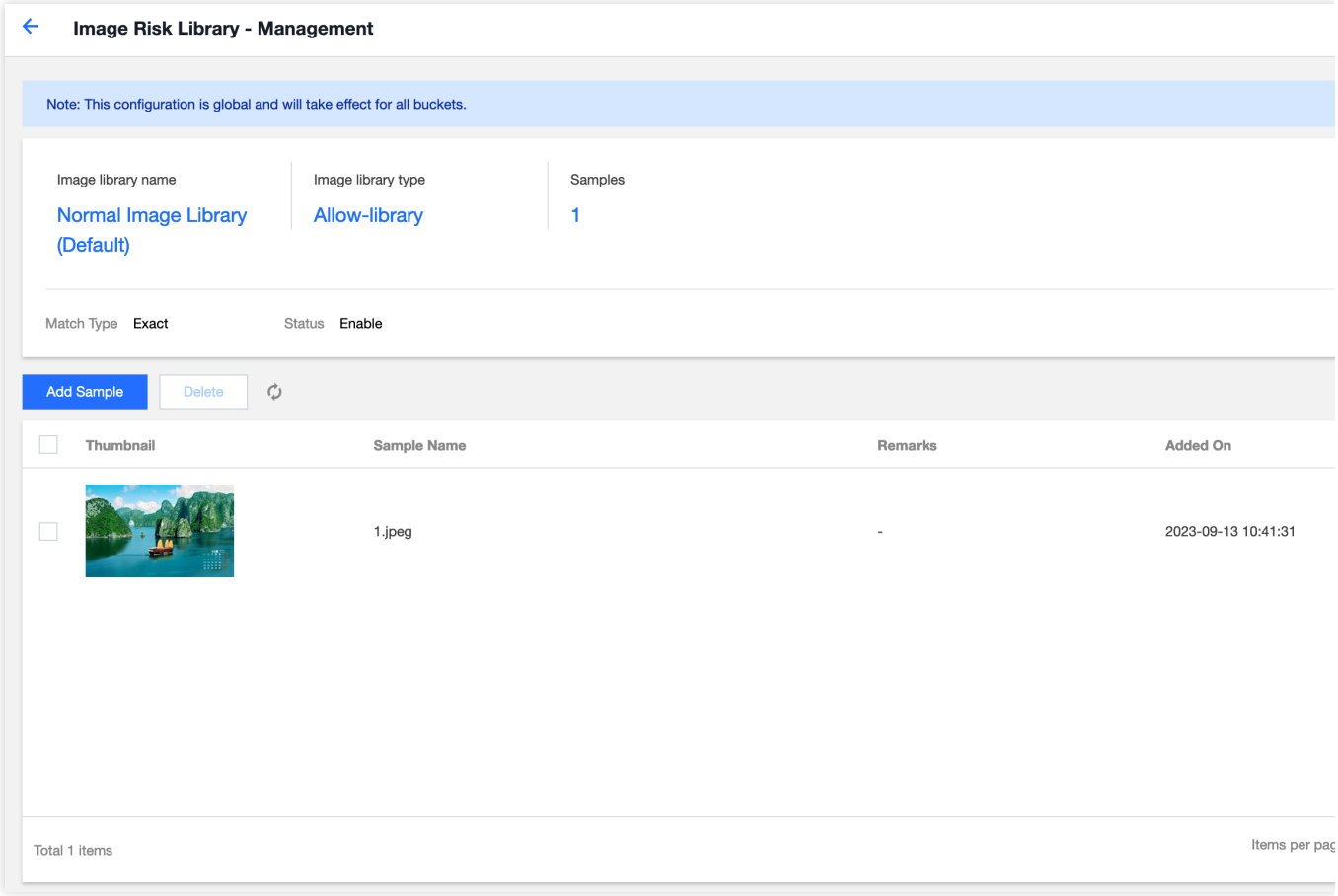
Directions

1. Log in to the Cloud Infinite console. On the **Bucket List** page, select the required bucket to open the bucket management page.
2. On the left navigation bar, choose **Sensitive Content Moderation > Custom Risk Library**.
3. On the Custom Risk Library page, three tabs are displayed: Image Risk Library, Text Risk Library, and Business Field Risk Library. For instructions on operating the Business Field Risk Library, see Setting the Business Field Risk Library.

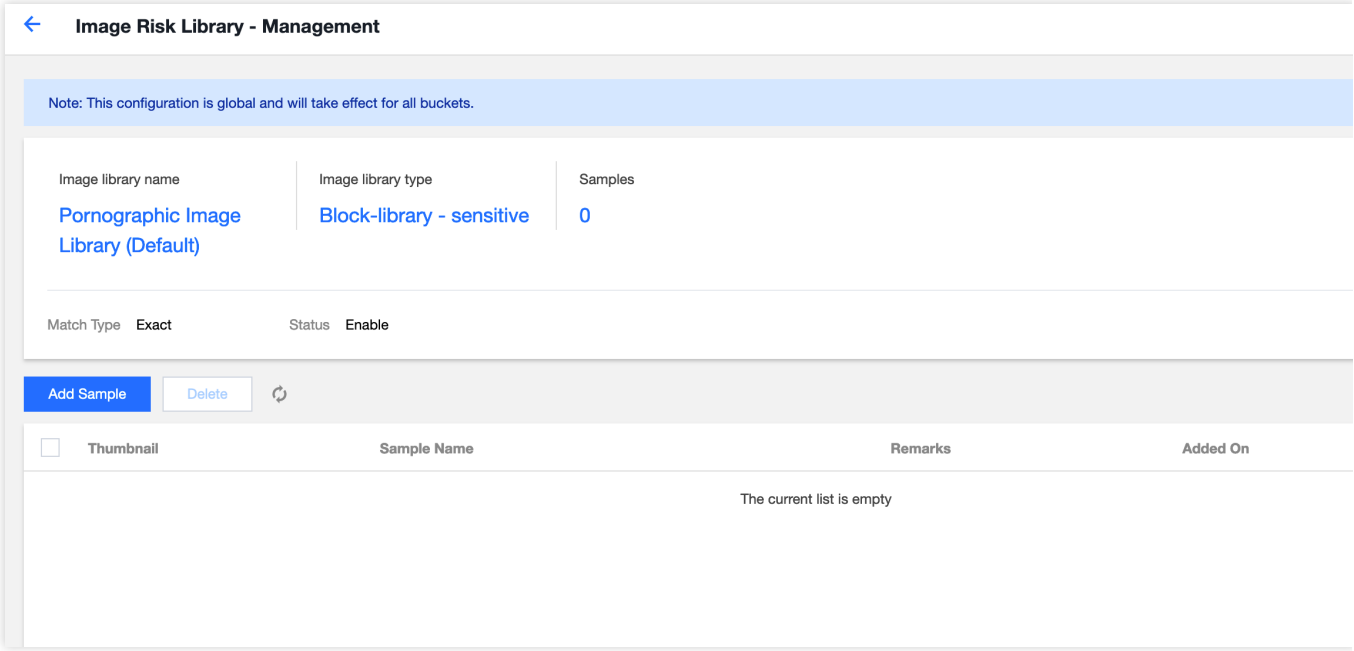


4. The operations on Image Risk Library and Text Risk Library are as follows:

Image Risk Library
Text Risk Library
To handle incorrect moderation, you can add image clean samples, to ensure the image moderation results return as normal:
1.Find the normal image library (pre-defined) from the list and click **Manage** on the right side of the library to access the Image Risk Library page.
2.On the Image Risk Library page, you can perform the following operations:



Viewing the image library policy: The policy for the normal image library is normal.
Viewing samples: Check the number of samples added to the image library.
Adding samples: You can add selected images to the library as samples.
Deleting samples: You can delete sample images from your image library.
For scenarios of missed moderation, add image block samples so that the image moderation results return as sensitive:
1.In the list, find the image library for with the returned sensitive type is desired. If you add an image to the pornographic image library (pre-defined), the moderation result will be tagged as pornography. Click **Manage** on the right of the library to open the Image Risk Library page.
2.On the Image Risk Library page, you can perform the following operations:



Viewing the image library policy: The policy for the pornography library is sensitive.

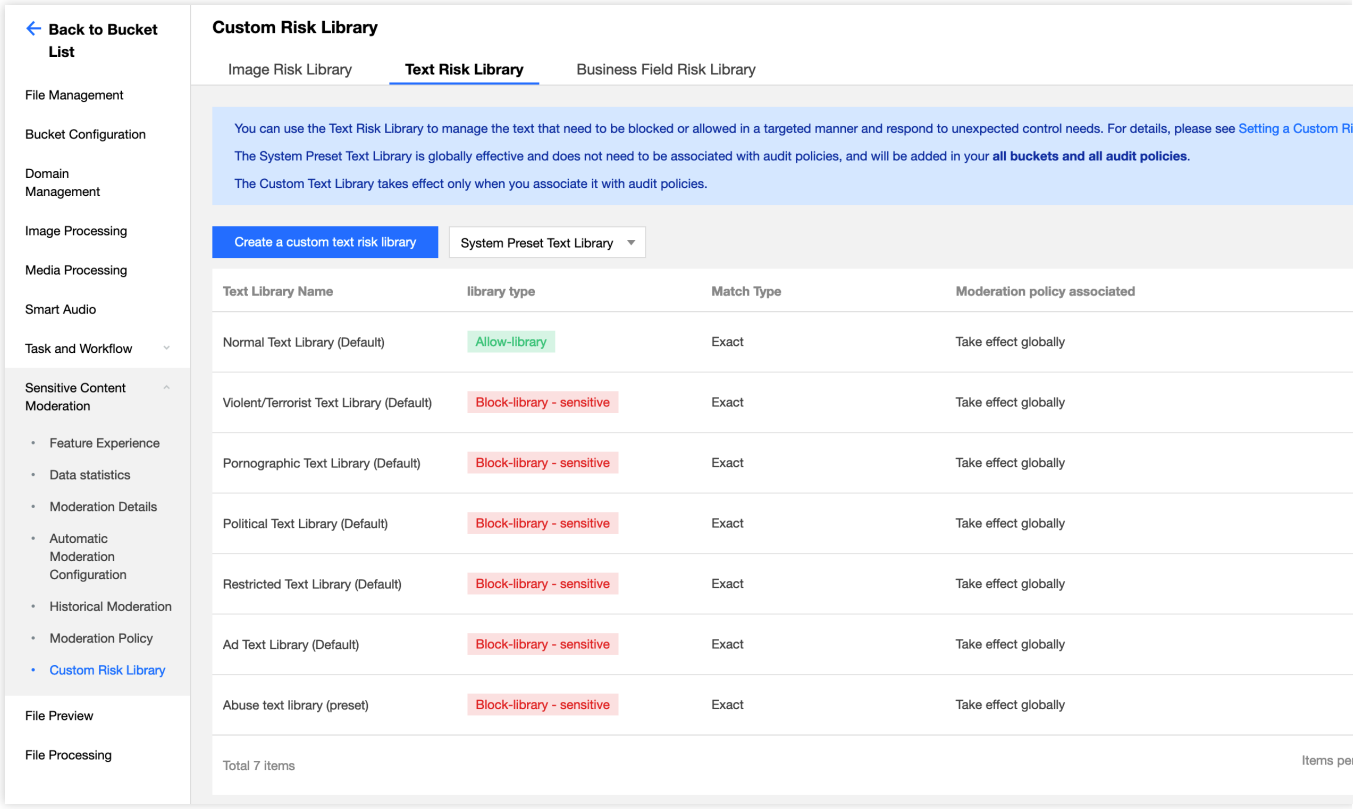
Viewing samples: Check the number of samples added to the image library.

Adding samples: You can add specific images to the library as samples.

Deleting samples: You can delete sample images from your image library.

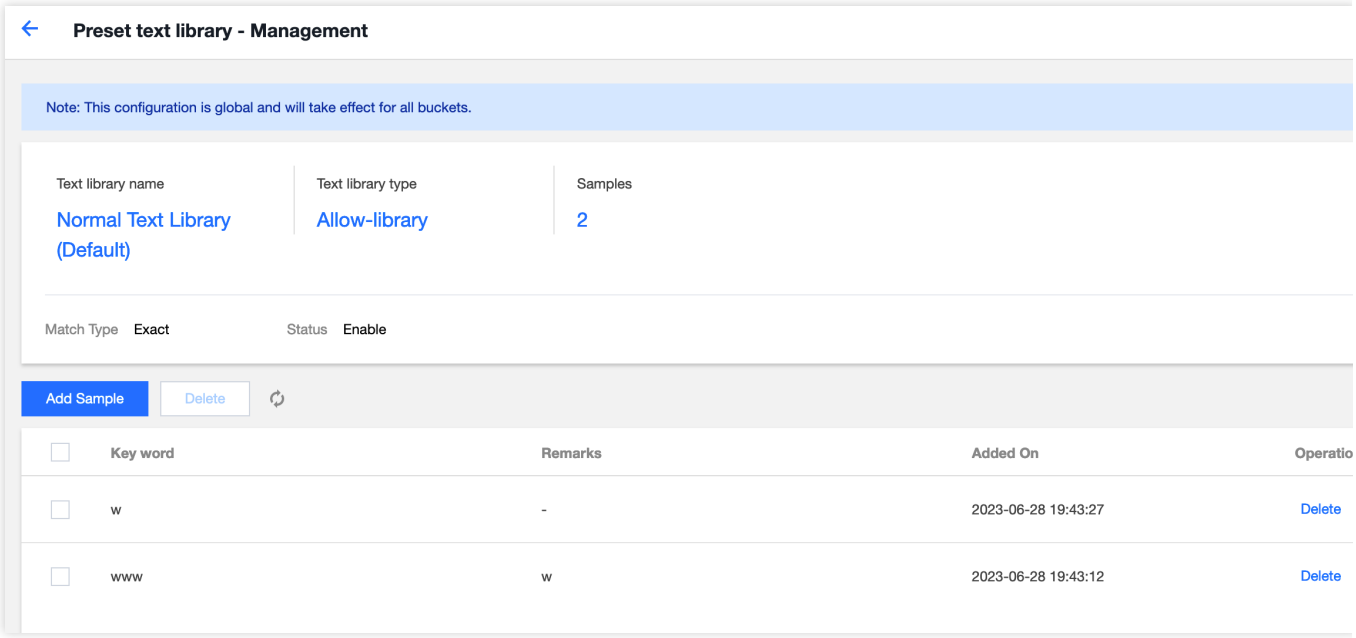
You can directly add keywords into the pre-defined text library or create a custom text library to add keywords:

Keywords added to the pre-defined text library will take effect for all moderation policies:



1.If you want to add clean sample keywords, find the normal text library (pre-defined) in the list, and then click **Manage** on the right side of the text library to open the Text Risk Library page.

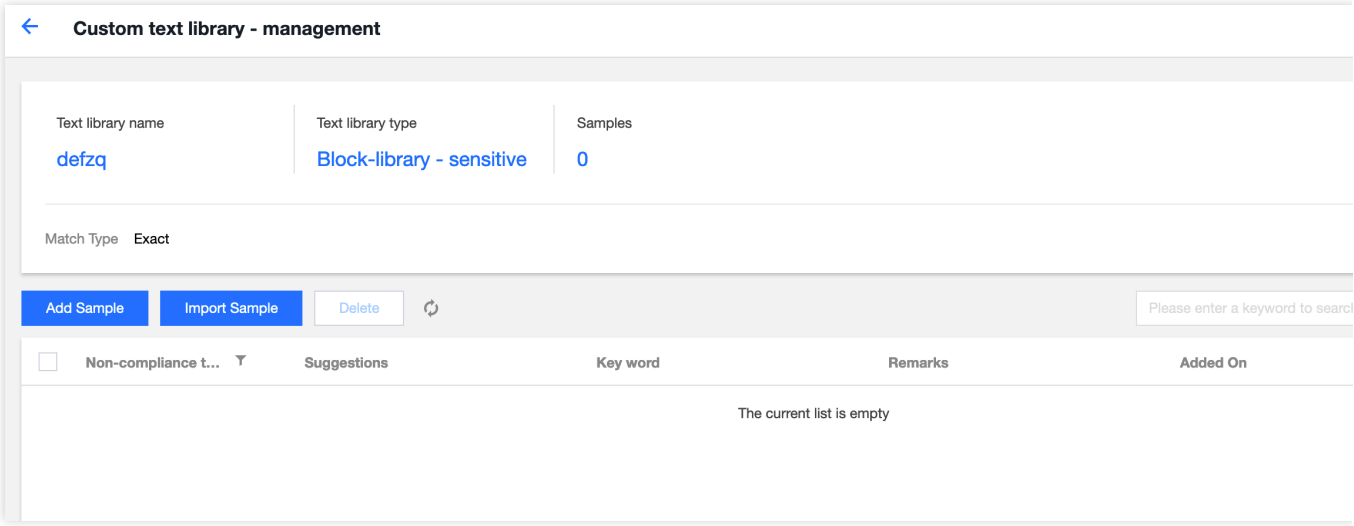
2.On the Text Risk Library page, you can perform the following operations:



Viewing the text library policy: The policy of the normal text library is normal.

Viewing samples: Check the number of samples added to the text library.

Adding samples: You can add specific keywords into the text library as samples.
Deleting samples: You can delete keywords from the text library.
Creating a custom text library: The custom text library needs to be associated with a moderation policy. In moderation operations, only the text library associated with moderation policies takes effect:
1.Click **Create Custom Text Library**, and in the window, specify the Text Library Name, and select the Text Library Policy and Match Type:
Text Library Policy: When a keyword sample in the text library is matched, you can choose sensitive or suspected as the returned moderation result.
Match Type: You can choose an exact match or a fuzzy match. For a fuzzy match, variants of the entered keyword can be detected to match similar words. Split words, homographs, homophones, simplified or traditional forms, case differences, and numeral words are supported.
2.After the Custom Text Library has been created, find the newly created library in the list, and click **Manage** on the right side of the selected library to open the Text Risk Library page.
3.On the Text Risk Library page, you can perform the following operations:



Viewing the text library policy: The custom text library policy can be sensitive or suspected.
Viewing samples: Check the number of samples added to the text library.
Adding samples: You can add specific keywords into the text library as samples.
Deleting samples: You can delete keywords from the text library.
5. After the risk library is configured, if samples from the risk library are encountered while you use the content moderation feature, they will be automatically allowed or blocked according to the risk policy.

Setting the Historical Data Moderation Task

Last updated：2024-01-31 16:44:15

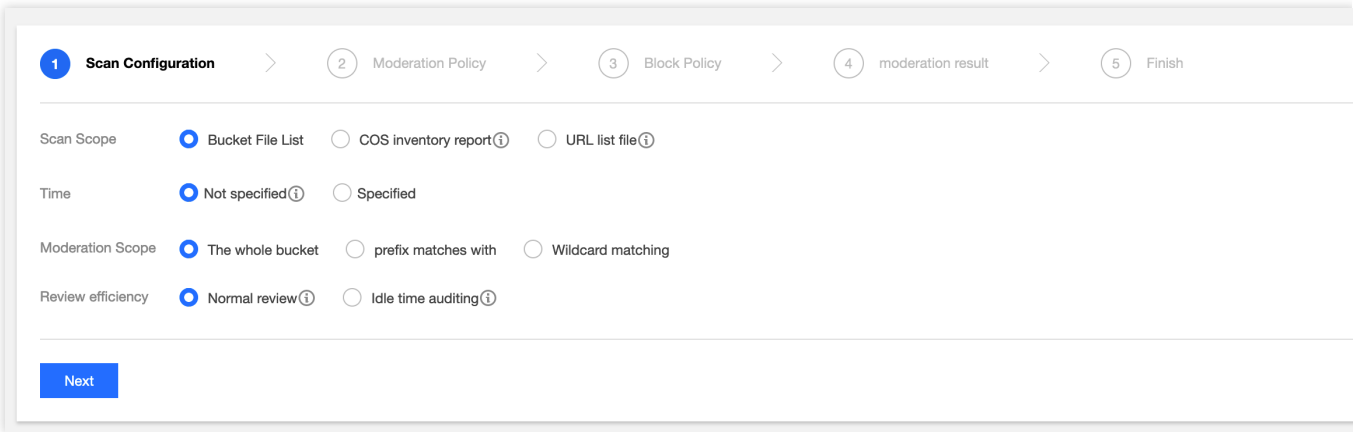
Feature Overview

This document describes how to use the historical data moderation feature of the content moderation feature on the console. You can create a historical data moderation task to perform a one-time batch moderation on your images, videos, audios, text, and files.

Creating Moderation Tasks

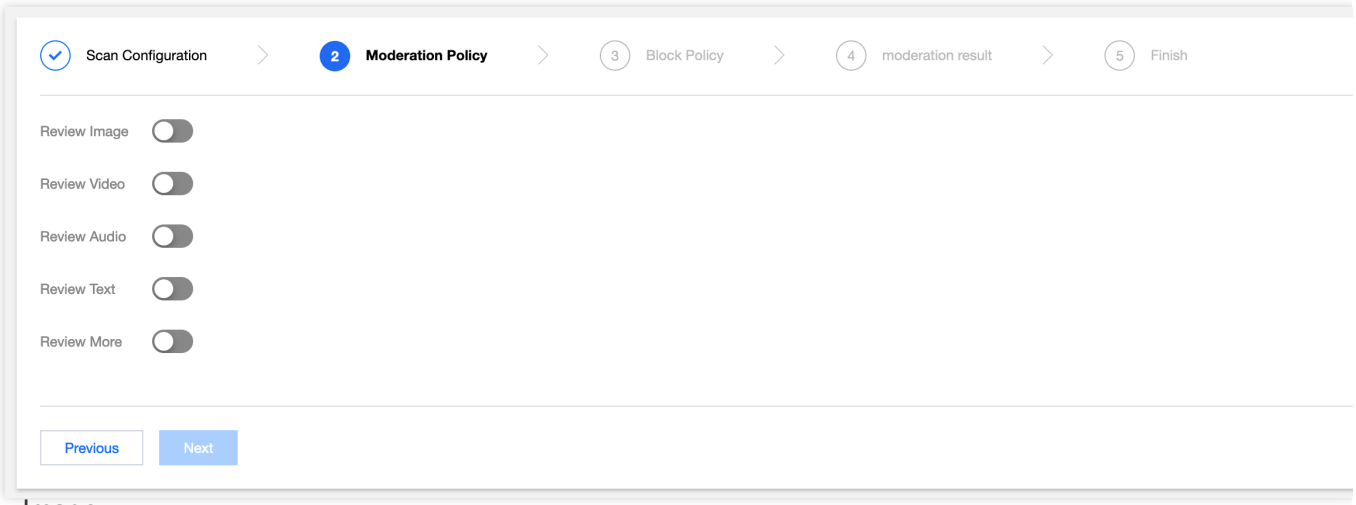
Directions

1. Log in to the Cloud Infinite console.
2. Choose **Bucket Management** from the left-side navigation bar to open the bucket management page.
3. Navigate to the required bucket and click on its name to open the bucket configuration page.
4. In the left navigation bar, choose **Sensitive Content Moderation > Existing File Moderation** to open the historical data moderation page.
5. Click **Create Moderation Task**.
6. In the Scan Configuration page, you can moderate your files as needed through different scan scopes:



Scan Scope: Three options are included: Bucket File List, COS Inventory report, and URL list file:
Bucket File List: You can select files in the bucket for moderation. The scan scope supports scanning based on file upload time and prefix scan.
COS Inventory report: You can scan the inventory lists generated by the COS Inventory Feature and store the list files in the current bucket.
URL list file: You can scan a specified URL list file. Currently, TXT files with one URL per line are supported.
7. Click **Next**.

8. On the Moderation Policy page, configure your moderation policy, corresponding moderation file types, and moderation scenes. Click **Next**.



Review Image:

Moderation suffix: The image moderation supports image files with the suffixes of JPG, JPEG, PNG, BMP, WEBP, and GIF.

Note

Intelligent suffix recognition can recognize the preceding six common image suffixes as well as some special suffixes.

Selecting moderation policies: Select the moderation policy you have configured (if you have not configured any policies, you can select the system default policy). Different moderation policies correspond to different policy categories, and you can customize moderation scenes through these policies. This includes moderation for pornographic, illegal, and advertising content, and you can select one or multiple detection scenarios. For more information on how to configure moderation policies, see Setting Moderation Policy.

Moderation scene: Your default moderation scene or the scene you have configured within your moderation policy are displayed here. You can select the moderation scene categories that you want to moderate.

Review Video:

Moderation suffix: Video moderation supports video files with suffixes of MP4, AVI, MKV, WMV, RMVB, FLV, and M3U8.

Moderating content: Both video footage and audio content can be moderated.

Selecting moderation policies: Select the moderation policy you have configured (if you have not configured any policies, you can select the system default policy). Different moderation policies correspond to different policy categories, and you can customize moderation scenes through these policies. This includes moderation for pornographic, illegal and advertising content, and you can select one or multiple detection scenarios. For more information on how to configure moderation policies, see Setting Moderation Policy.

Moderation scene: Moderation scene options include moderation for pornographic, illegal, and advertising content, and you can select one or more detection scenes as required.

Frame capturing rule: Video moderation is performed based on video frame capturing, through the moderation of captured images. Captured frame moderation can be performed by fixed time, fixed frame rate, and fixed quantity.

Fixed Time: Frames are captured at fixed intervals for moderation. You can set the time interval and the maximum number of frames per video.
Fixed Frame Rate: A fixed number of frames are captured per second for moderation. You can set the per-second frame capture rate and the maximum number of frames per video.
Fixed Quantity: A pre-defined quantity of images are moderated, procured from full-length videos and based on an average percentage. You can set the maximum number of captured frames per video.

Note

The settings of frame capture rules will influence the moderation process result.

Review Audio:

Moderation suffixes: Audio files wilt the following suffixes are supported: MP3, WAV, AAC, FLAC, AMR, 3GP, M4A, WMA, OGG, and APE.
Selecting moderation policies: Select the moderation policy you have configured (if you have not configured any policies, you can select the system default policy). Different moderation policies correspond to different policy categories, and you can customize moderation scenes through these policies. Moderation for pornographic, illegal and advertising content is included, and you can select one or multiple detection scenes. For more information on how to configure moderation policies, see Setting Moderation Policy.
Moderation scene: The moderation category displays the scenes you have configured in your moderation policy. You can select the moderation categories you want to moderate.

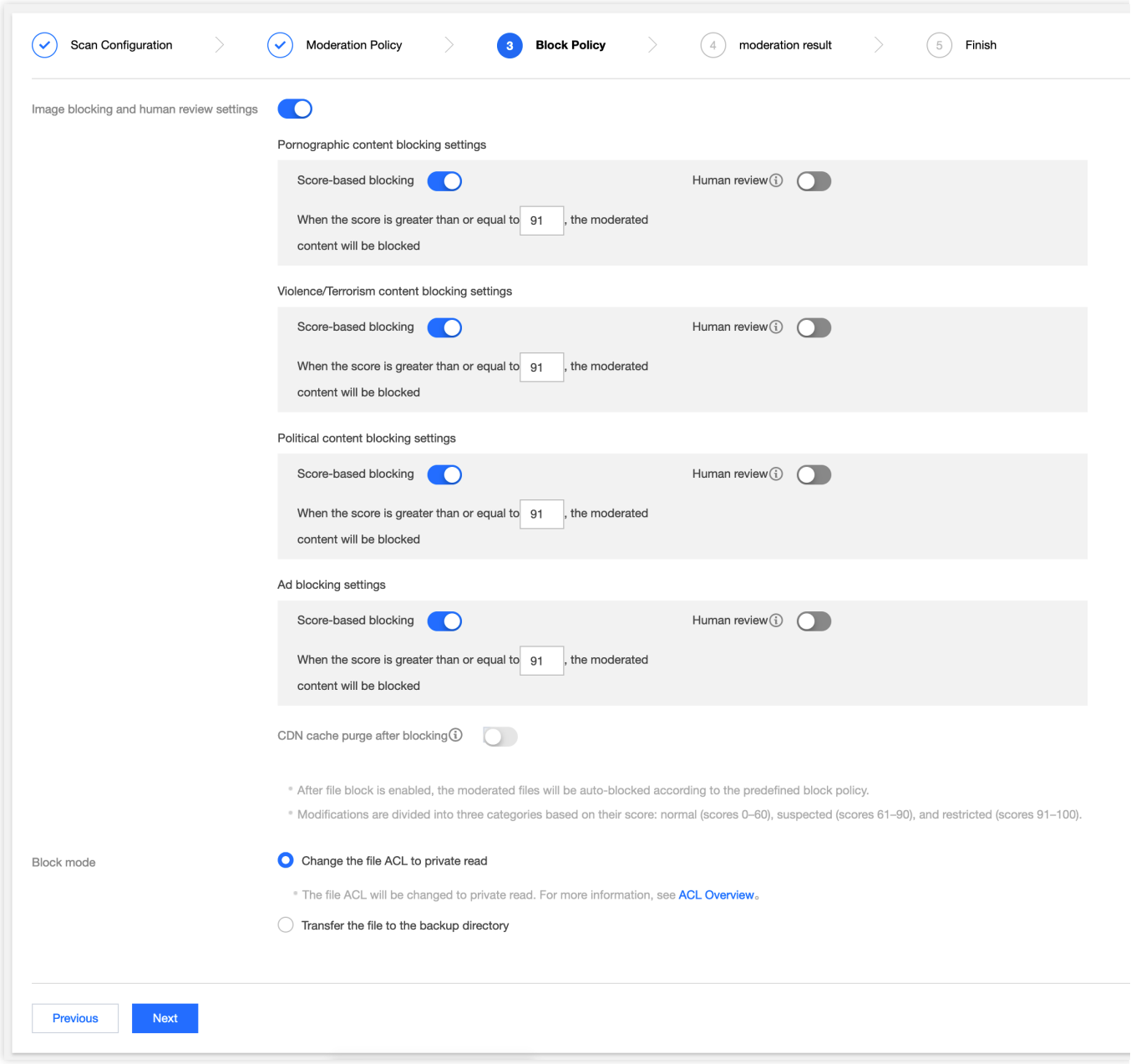
Review Text:

Moderation suffixes: TXT files and files with no defined suffix are supported.
Selecting moderation policies: Select the moderation policy you have configured (if you have not configured any policies, you can select the system default policy). Different moderation policies correspond to different policy categories, and you can customize moderation scenes through these policies. Moderation for pornographic, illegal and advertising content is included, and you can select one or multiple detection scenes. For more information on how to configure moderation policies, see Setting Moderation Policy.
Moderation scene: The moderation category represents the scenes you have configured in your moderation policy. You can select the moderation categories you want to moderate.

Review More:

Moderation suffixes: Presentation files, text files, spreadsheet files, and PDFs are supported. You can also select multiple types of files.
Selecting moderation policies: Select the moderation policy you have configured (if you have not configured any policies, you can select the system default policy). Different moderation policies correspond to different policy categories, and you can customize moderation scenes through these policies. Moderation for pornographic, illegal and advertising content is included, and you can select one or multiple detection scenes. For more information on how to configure moderation policies, see Setting Moderation Policy.
Moderation scene: Scenes that you have configured in the selected moderation policy are displayed here. You can select the target scene as required.

9. In the Block Policy page, set the blocking policy and click **Next**. After the blocking policy is enabled, you're granting the CI cloud service the permission to automatically moderate and block the file of the corresponding type or perform manual re-moderation, effectively denying public read access to identified non-compliant content.



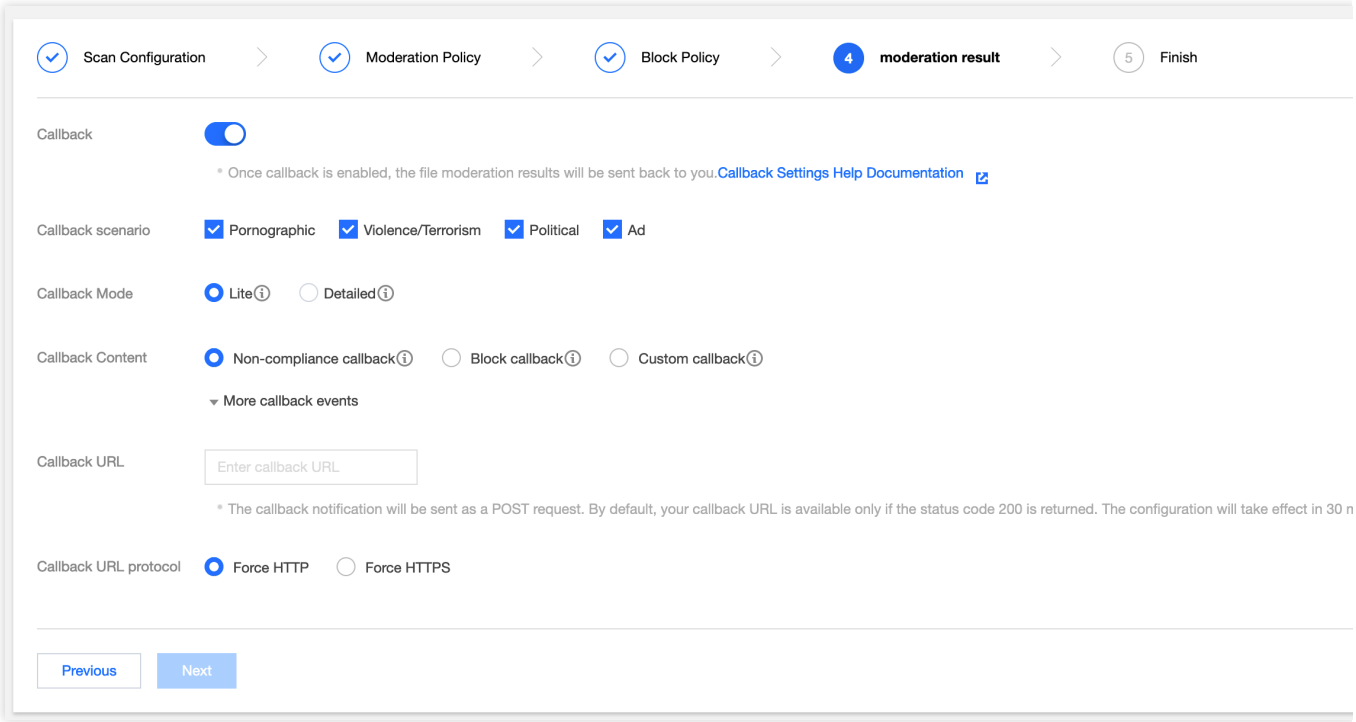
Blocking settings: By default, direct blocking is selected. You can set a score (an integer from 60 to 100) based on different moderation types. When the set score range is reached, the image will be directly blocked. If you choose manual re-moderation, a professional security team will conduct a secondary moderation of the data with the specified moderation score.

Note

The moderation results are classified into confirmed sensitive, likely sensitive, and normal categories based on the moderation score.

The score range for confirmed sensitive images is 91 or higher.

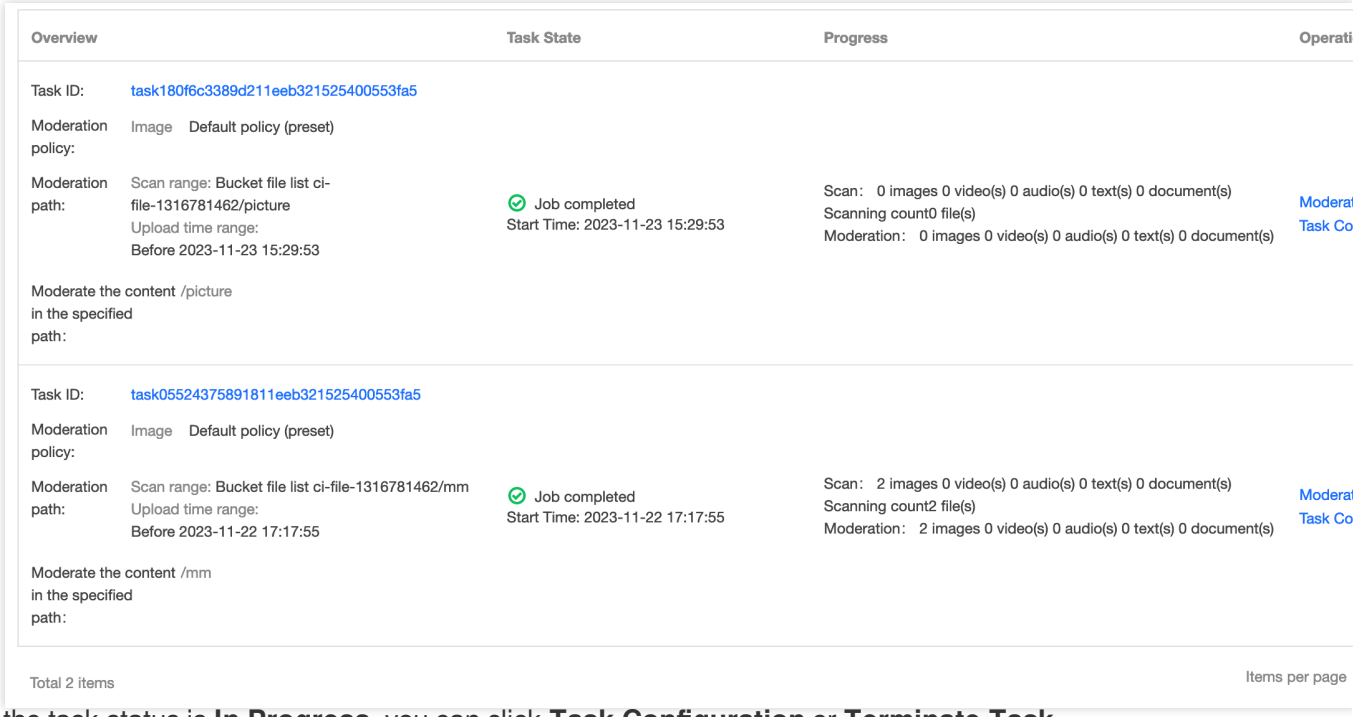
The score range for images to be likely sensitive is from 61 to 90. In this range, the system cannot precisely categorize these images as sensitive. It is recommended that users conduct a secondary manual re-moderation to ensure the image security.
The score range for normal images is 60 or lower. The system considers these images as normal.
10. On the Moderation Result page, set the moderation result callback and click **Next**. After callback settings are enabled, we will send the moderation results to your designated callback address. You need to choose the callback type, content, and set the callback URL.



Callback scenario: According to the moderation policy you set, pornographic and advertising content can be selected.
Callback Mode: Supports **Lite** or **Detailed.**
Callback Content:
Non-compliance callback: The moderation result should be called back only when it is deemed sensitive.
Block callback: The review result should be called back only when it is blocked.
Custom callback: The review result should be called back when the users specify that the review result is within a certain score range.
Callback URL: The callback URL must return a default status code of 200 so that callback can take effect.
Callback URL Protocol: You can choose enforced HTTP or HTTPS.
11. After ensuring that all task configurations are correct, click **Create** to complete task creation.

Viewing Task Result

On the Historical Data Moderation page, you can perform various actions depending on the task status.



When the task status is **In Progress**, you can click **Task Configuration** or **Terminate Task**.

When the task status is **Execution Successful**, you can view **Moderation Details** or **Result Statistics**.

Viewing the moderation details: This feature only supports viewing moderation details from the past one month. After clicking it, you will be redirected to the moderation page where you can export moderation results, conduct manual moderation, among others. For specific operation instructions, see Moderation Details.

Viewing result statistics: This page displays the statistical results of the moderation task. If you have any doubts about the moderation results, you can go to the Moderation Details page on the console to view the specific moderation content.

File Processing

Last updated：2024-01-31 16:44:15

Overview

CI provides **privacy protection** and **file preview** features for document files.

File Preview

The file preview feature allows generating **images** from multiple types of files for preview. It addresses the display problems of file content on webpages and enables easy **online file preview** on PC, app, and other terminals. It is widely suitable for diverse business scenarios, such as online education, enterprise OA, and website transcoding. Currently, this feature supports **real-time preview during download** and **async file preview job creation**.

Note:

Currently supported input file types include:

Presentation files: PPTX, PPT, POT, POTX, PPS, PPSX, DPS, DPT, PPTM, POTM, PPSM.

Text files: DOC, DOT, WPS, WPT, DOCX, DOTX, DOCM, DOTM.

Spreadsheet files: XLS, XLT, ET, ETT, XLSX, XLTX, CSV, XLSB, XLSM, XLTM, ETS.

Other files: PDF, LRC, C, CPP, H, ASM, S, JAVA, ASP, BAT, BAS, PRG, CMD, RTF, TXT, LOG, XML, HTM, HTML.

The input file size cannot exceed 200 MB.

The number of pages in the input file cannot exceed 5,000.

Directions

The **File Preview** page in the console provides file preview operations, such as enabling/disabling the file preview feature, creating file preview jobs, enabling/disabling file preview queues, and setting the callback.

Activating service

1. Log in to the CI console and click **Bucket Management** to enter the bucket management page.
2. On the **Bucket Management** page, click the target bucket to enter the bucket details page.
3. Click **File Processing** on the left and select the **File Preview** configuration item.
4. Click **Edit** to enable file preview and click **Save**.
5. After the feature is enabled, you can use the corresponding file preview API to preview files during downloading as instructed in Sync Request API. You can also create file preview jobs asynchronously as instructed in Submitting File Transcoding Job.

Creating job

1. Click **Create Job** in the job management module and enter job parameters as follows:
File Path: The file path must start with "/" and use "/" to separate folders, such as `/doc/example.dox`.
Preview Setting: Select to preview whole document or specified page. A job supports up to 5,000 pages. If more pages are input, only the first 5,000 pages can be converted.
Queue: After you activate the file preview service, the system will enable the `queue-doc-process-1` queue for you by default. You can manually disable it in the queue module. If you need more queues, submit a ticket for assistance.
Output Bucket: Select a bucket for which the file preview feature has been enabled in the current region.
Output Image Format: Currently, JPG and PNG formats are supported for output images.
Output Path: It is optional. If it is not set, it will be the same as the input file path.
Output File Name: The file preview feature converts each page of the original file into an image. Therefore, you need to add a placeholder (`${Number}` or `${Page}`) to the output filename to number the output images. The output numbers are the same as the file page numbers. For example, if you want to preview a file with three pages and set the output filename to `output${Number}.jpg`, then three images `output1.jpg`, `output2.jpg`, `output3.jpg` will be output.
2. Click **Confirm**.

Managing job

You can filter and view file preview jobs in the job management module by time, job ID, and job status. You can also click **View** in the **Operation** column to view more job information in addition to that displayed on the page.

Setting queue

After you activate the file preview service, the system will enable the `queue-doc-process-1` queue for you by default. You can pause it in the **Operation** column in the queue module.

Setting callback

1. Click **Queue** to enter the **Queue** page.
2. Click **Configure Callback Rule** in the **Operation** column to enter the callback settings page.
3. Click **Edit** to enable callback, enter a callback URL, and click **Confirm**. Then, after a file preview job is completed, its execution result will be sent to the callback URL for you to perform subsequent operations.

Note:

The callback URL can be used only if the HTTP 200 status code is returned by default. It will take effect in five minutes after configuration.

Note:

File preview is a paid feature. For billing details, see Billing Overview.

Privacy Protection

CI's privacy protection feature can filter various types of private data in files to effectively prevent information leakage, such as ID number, taxpayer identification number, business registration number, military ID number, email address, license plate number, and mobile number. Currently, it can only scan data automatically during upload.

Note:

Currently, the privacy protection feature is supported for the following types of files:

Microsoft Office files: DOC, DOCX, PPT, PPTX, XLS, XLSX, RTF

WPS files: WPS, DPS, ET

PDF files: PDF

Plain text files: TXT, XML, SLK

Web files: HTML, MSG

Email files: EML, PST

Directions

1. Log in to the CI console and click **Bucket Management** to enter the bucket management page.
2. On the **Bucket Management** page, click the target bucket to enter the bucket details page.
3. Click **File Processing** on the left and select the **Privacy Protection** configuration item.
4. Click **Edit** to enable this feature and configure it as follows:

File Type: You can select multiple file types for which privacy protection will be automatically triggered.

Moderation Type: You can select multiple types of sensitive data to be filtered.

Callback: After callback is enabled, you can enter a callback URL to receive the filtering results of privacy protection. Note that the callback URL can be used only if the HTTP 200 status code is returned by default. It will take effect in five minutes after configuration.

5. After enabling privacy protection, you can view the **private data details** below by time, violation type, sensitivity level, or moderation type.

Note:

Violation types include violation of GDPR, cybersecurity classified protection compliance, and the Cybersecurity Law of China. Files will be classified into high, medium, and low sensitivity levels based on the moderation results.

Usage Statistics

Last updated：2024-01-31 16:44:15

Overview

The usage statistics service displays usage data in various dimensions and ways. Currently, the usage statistics of **image processing**, **media processing**, **content moderation**, **content recognition**, **file processing**, and **traffic** services are available. In addition, you can view the usage of a specified service by bucket or period on the statistics page and download the usage statistics by time or bucket.

Directions

Viewing Usage Statistics

1. Log in to the CI console, click **Usage Statistics** on the left sidebar, and select and click the usage statistics tab of the target service.
2. On the usage statistics page, click the drop-down list in the top-left corner, and select the target bucket. All buckets are selected by default.
3. Click **Time Selection**, and select a time period (for example, today, yesterday, last 7 days, last 15 days, last 30 days, or custom time period) to view the corresponding usage statistics.
4. You can hover over a date on the visualized data display to view the corresponding usage.

Downloading Usage Statistics

1. Log in to the CI console, click **Usage Statistics** on the left sidebar, and select and click the usage statistics tab of the target service.
2. On the usage statistics page, click the drop-down list in the top-left corner, and select the target bucket. All buckets are selected by default. Then, download the corresponding statistics by time or bucket.

Download statistics by time: click the download icon on the right of the time box to download the usage statistics file.
Download statistics by bucket: scroll down to find the **Bucket Statistics** section and click the download icon in the top-right corner of the section to download the usage statistics file.

Note:

The downloaded file is in CSV format.

Data Monitoring
Setting Alarm Policies

Last updated：2024-01-31 16:44:15

Overview

You can leverage the alarm policy feature of Cloud Monitor to set threshold-reaching alarms for CI monitoring metrics. An alarm policy must include the policy name, policy type, trigger condition, alarm object, and alarm notification template. You can create an alarm policy for CI as instructed below.

Note:

Tencent Cloud's Cloud Monitor enables users to monitor cloud resources in real time and provides alarm services. Users can set alarm policies for CI monitoring metrics to query the alarm history and receive alarm notifications. For more information, see Creating Alarm Policy.

Directions

1. Log in to the CI console. On the **Overview** page, click **Configure Alarm Policy** in the **Alarm Configuration** section.
2. Click **Create**.
3. On the **Create alarm policy** page, configure a new alarm policy.

Notes:

Configuration Type	Configuration Item	Description
Basic info	Policy name	A custom policy name
	Remarks	Remarks for the policy
	Monitor Type	Choose Cloud Product Monitoring.
	Policy type	Select CI.
	Project	Setting the policy project allows you to: Manage alarm policies. Alarm policies of a project can be quickly located in the alarm policy list.

		Manage instances. You can select the project as needed. Instances of the project can be quickly located in **Alarm Object**. You can distribute Tencent Cloud services to the desired project according to your business types. After the project is created, you can distribute resources to projects in the console of each Tencent Cloud service. Some Tencent Cloud services cannot be distributed to a project. If you do not have project permission, see Cloud Access Management (CAM) for authorization.
Configure alarm rule	Alarm object	If you choose Instance ID in the drop-down list, select the bucket you want to add an alarm to. If you choose Instance Group in the drop-down list, the alarm policy is bound to the selected instance group. If there is no instance group, you can click Create Instance Group on the right to create a group for the bucket first. If you choose All Objects in the drop-down list, the alarm policy is bound to all buckets the current account has permission on.
	Select template	Select a configured template from the drop-down list. For more information on the configuration, see Configuring Trigger Condition Template. If the newly created template is not displayed, click Refresh on the right.
	Manual configuration(Metric alarm)	Trigger condition: Consists of metric, comparison, threshold, statistical period, and the number of consecutive periods.For example, if the metric is set to `Total usage of basic image processing`, comparison to `>`, threshold to 100 MB, statistical period to 1 minute, and number of consecutive data points to 2, the total usage of basic image processing will be collected once every minute, and an alarm will be triggered if a bucket's usage of basic image processing is greater than 100 MB for two consecutive times. Alarm frequency: You can set a repeated notification policy for each alarm rule. In this way, an alarm notification will be sent repeatedly at a specified frequency when an alarm is triggered.

		Frequency options: do not repeat, once every 5 minutes, once every 10 minutes, at an exponentially increasing interval, and other frequency options. An exponentially increasing interval means that a notification is sent when an alarm is triggered the 1st time, 2nd time, 4th time, 8th time, and so on. In other words, the alarm notification will be sent less and less frequently as time goes on to reduce the disturbance caused by repeated notifications. Default logic for repeated alarm notifications: The alarm notification will be sent to you at the configured frequency within 24 hours after the alarm is triggered. After 24 hours, the alarm notification will be sent once a day by default.
Configure alarm notification	Alarm notification	Select a preset or custom notification template. Each alarm policy can be bound to three notification templates at most. For more information, see Alarm Notification.
Advanced configuration	Auto scaling	If enabled, the auto scaling policy can be triggered when the alarm condition is met.

4. After configuring the above items, click **Save**.

Querying Monitoring Data

Last updated：2024-01-31 16:44:15

Overview

CI can monitor various service capabilities. The monitoring data window of CI's statistics displays the monitoring metrics of image processing, media processing, content recognition, and document processing.
You can query the details of data processing in different storage classes for different time periods. The following describes how to view the monitoring data of a single bucket with a root account or sub-account.

Querying with a Root Account

1. Log in to the CI console.
2. Click **Bucket Management** on the left sidebar to enter the bucket list.
3. Find the target bucket and click **Data Monitoring** on the right.
4. On the data monitoring page, view the information.

Querying with a Sub-account

To query monitoring data with a sub-account in the console, you need to first grant the sub-account relevant permissions.
You can grant such permission by using a **Policy Template** or **Custom Access Policy**.

Using a policy template

1. Log in to the CAM console as the root account and select **Users** > **User List** to enter the user list page.
2. Find the target sub-account and click **Authorize** in the **Operation** column on the right.
3. Search for and select the `QcloudMonitorFullAccess` policy in the pop-up window and click **OK** to associate it with the sub-account. Then, the sub-account can access monitoring reports.

Note:
This policy template grants the sub-account the **full access** to CM. To protect the security of your account, you can customize an access policy to grant only read permissions to the sub-account.

Using a custom access policy

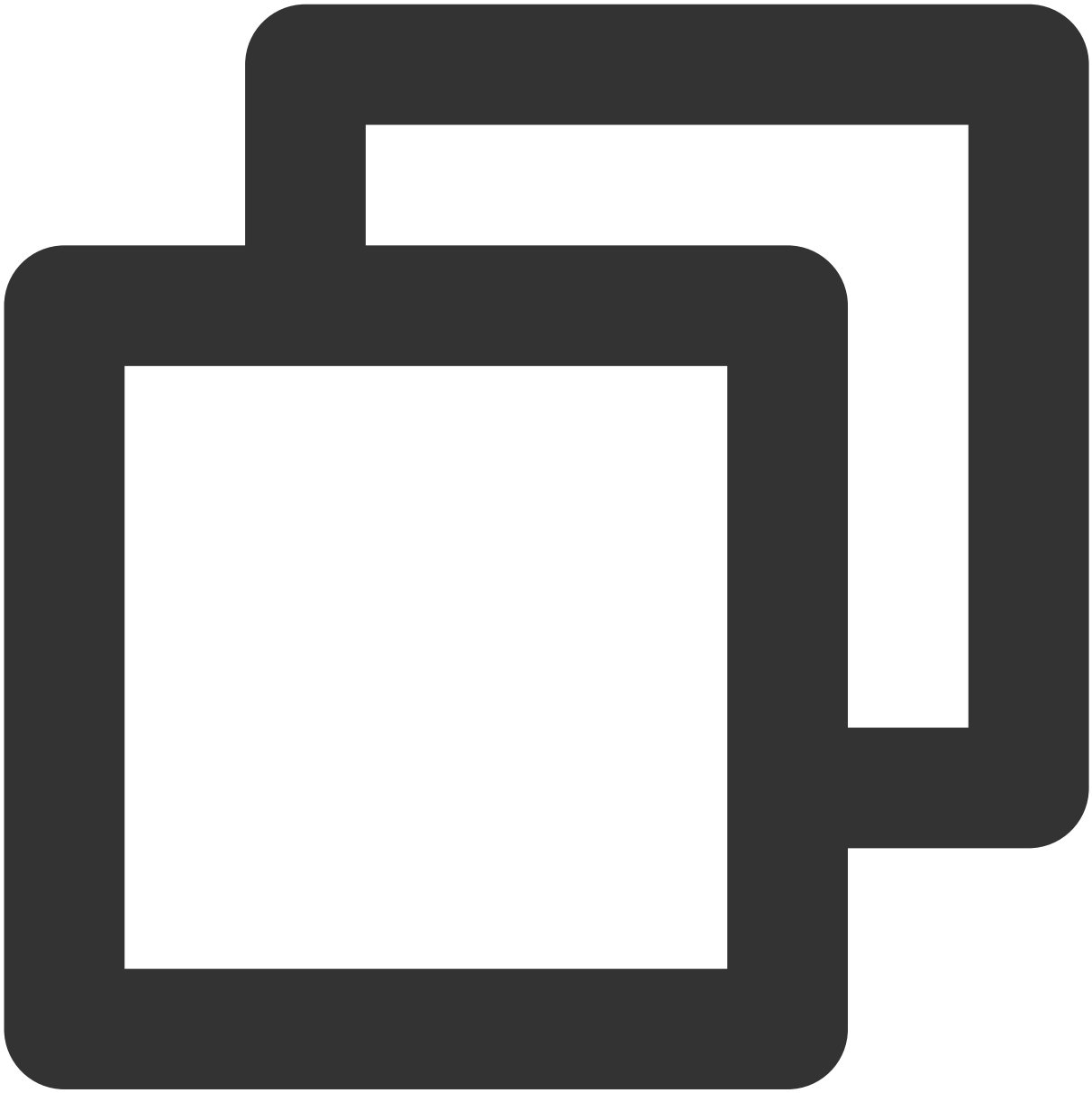
1. Log in to the CAM console as the root account.
2. On the left sidebar, click **Policies** > **Create Custom Policy** > **Create by Policy Syntax**.

3. Select **Blank Template** and click **Next**.

4. Copy and paste the following policy syntax into the **Edit Policy Content** input box.

You can rename the policy as needed.

Policy syntax:



```
{
 "version": "2.0",
 "statement": [
     {
         "effect": "allow",
         "action":[
```

```
                "monitor:GetMonitorData"
            ],
            "resource": "*"
        }
    ]
}
```

5. Click **Create Policy**.

After the policy is created successfully, you can associate it with the sub-account as instructed in Authorizing by policy template.