ApsaraVideo Live

User Guide

User Guide

Product functions list

Console

Function	Description
ApsaraVideo Live CDN domain management	Supports creation and deletion of ApsaraVideo Live CDN domain names.
Live video transcoding setting	Creates different transcoding templates for different AppNames.
Live stream management	Queries real-time live streams and historical live streams.
Live stream blacklist management	Sets and deletes stream blacklists.
Set NotifyUrl	Sets the target URL the live stream information is pushed to.

API

Function	Description
Query online users	- Gets the number of online users of the RTMP live stream, - Supports query by domain name or stream.
Query streaming blacklist	Gets the blacklist of the currently played live stream under the domain name.
Query stream control history	Gets the operation history of a live stream under a domain name or application.
Query the live stream frame rate and bit rate	- Gets the frame rate and bit rate history of a live stream, - Supports query by domain name or stream.
Query streaming list	Views the information of all the streams being pushed under a specific domain name (or an application under a specified domain name).

Query streaming history	Views the streaming history of a domain name (or an app under the domain name) within a period of time.
Disable live streaming	Disables the push of a stream. You can set the time to resume the streaming.
Resume live streaming	Resumes the push of a stream.
Set NotifyUrl	Sets the target URL the live stream information is pushed to.

Resource quota limit

Live video CDN domain

You can create up to 20 live video CDN domains under each account. If you require more than 20 live video CDN domains, open a ticket to contact Alibaba Cloud technical support.

Concurrent live streams

Each live video CDN domain under each account can push up to 20 original (non-transcoded) live streams concurrently. If you enable the transcoding function, each CDN domain can push up to 10 transcoded live streams. If you require more than 20 live video CDN domains, open a ticket to contact Alibaba Cloud technical support.

Streaming

> ApsaraVideo Live does not limit the stream bit rate. It supports common resolutions and corresponding bit rates.
>
> We recommend that you set a bit rate not exceeding 4 Mbps to prevent buffering interference.

Domain name management

Manage a domain name

Add a domain name

Before creating an ApsaraVideo Live activity, you must add an ApsaraVideo Live domain name in the ApsaraVideo Live console.

Prerequisite

If you want to use ApsaraVideo Live service in China, confirm whether your domain name requires ICP record filing. In regions like **China East 2 (Shanghai)** and **China North 2 (Beijing)**, you must complete the ICP record filing. And in the **Singapore** region, you do not require to complete the ICP record filing. If the record-filing is pending, you must first apply for Website record-filing.

Procedure

Log on to the ApsaraVideo Live console.

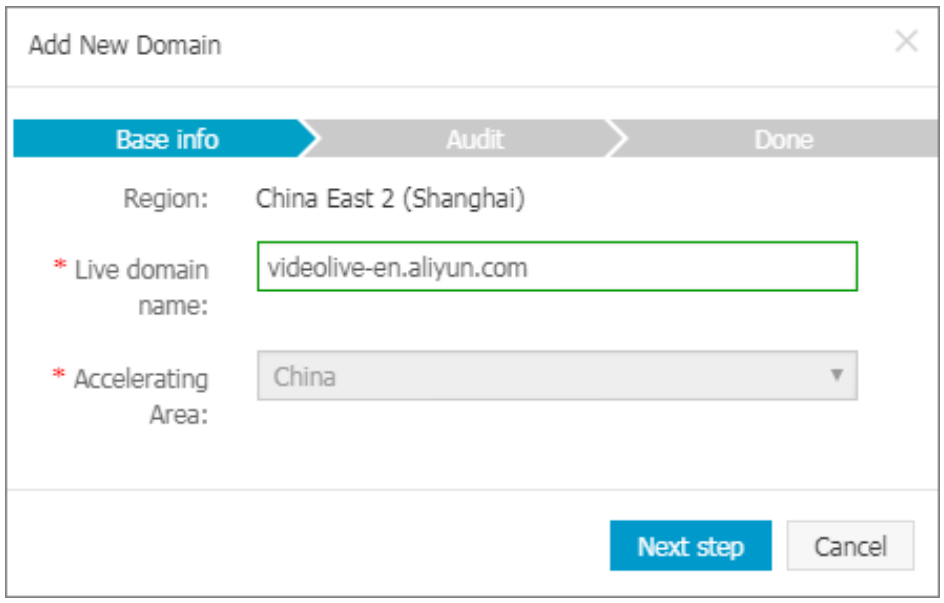
The console checks the activation status of services on which the product depends. Follow the instructions on the status page.

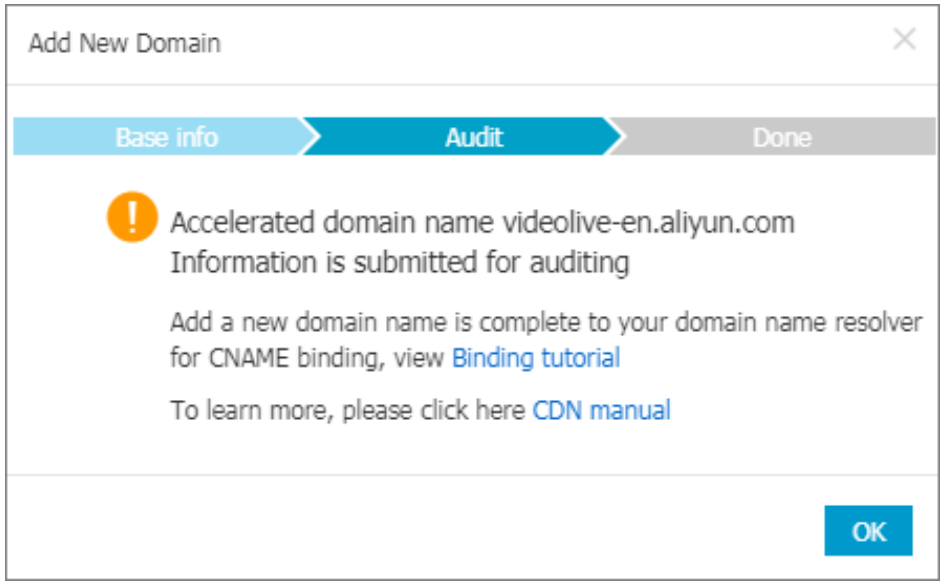
Add a domain name.

Select the expected region.

Click **Add New Domain**.

Enter the new domain name and click **Next step**.





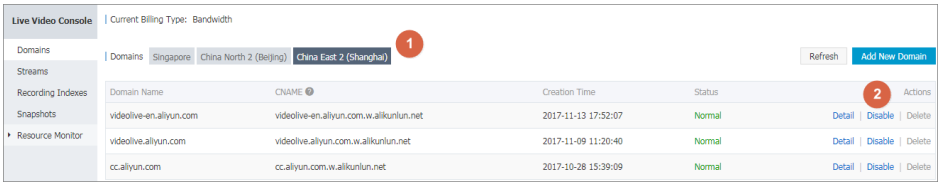
After the domain name is sucessfully configured, the domain name automatically configures the CDN live acceleration function. The live acceleration function is ready to use once the domain name completes CNAME binding.

Disable a domain name

Log on to the ApsaraVideo Live console.

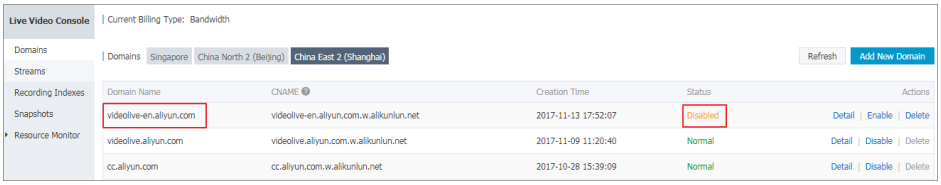
Select the region in **Domains**.

Select the domain name, and click **Disable** at the right side.



Click **OK**.

The current **Status** of the domain name is **Disabled**.

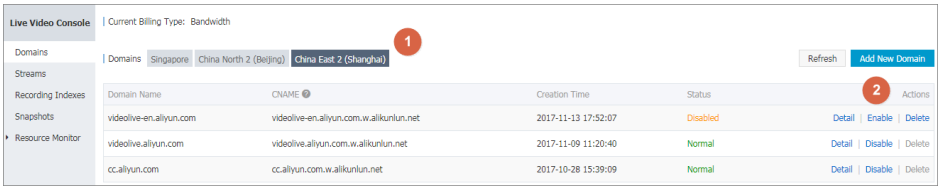


Enable a domain name

Log on to the ApsaraVideo Live console.

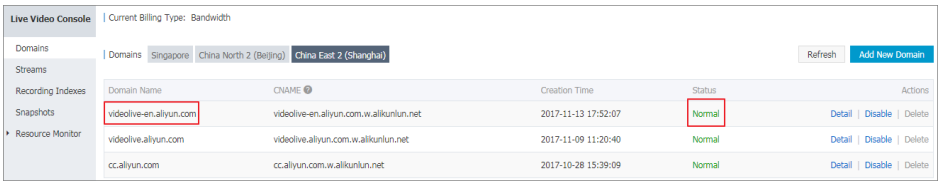
Select the region in **Domains**.

Select the domain name, and click **Enable** at the right side.



Click **OK**.

The current **Status** of the domain name is **Normal**.



Delete a domain name

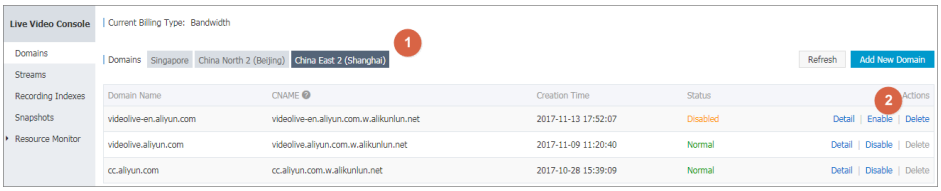
A domain name can only be deleted when its status is **Disabled**.

Procedure

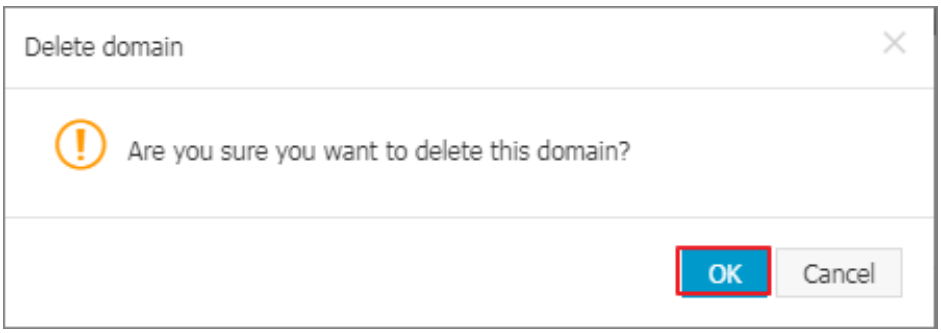
Log on to the ApsaraVideo Live console.

Select the region in **Domains**.

Click **Delete** at the right side of the domain which is disabled.



Click **OK**.



CNAME resolution

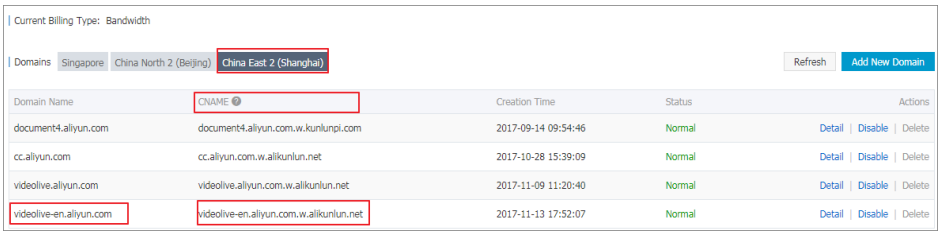
You can bind CNAME at www.net.cn website or other domain name registrars.

Procedure

Log on to the ApsaraVideo Live console.

Select the region.

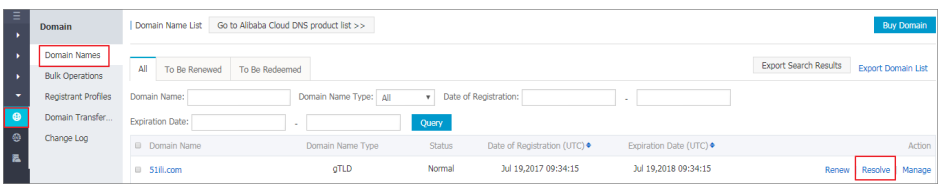
Select the domain name and get the CNAME corresponding to the domain name.



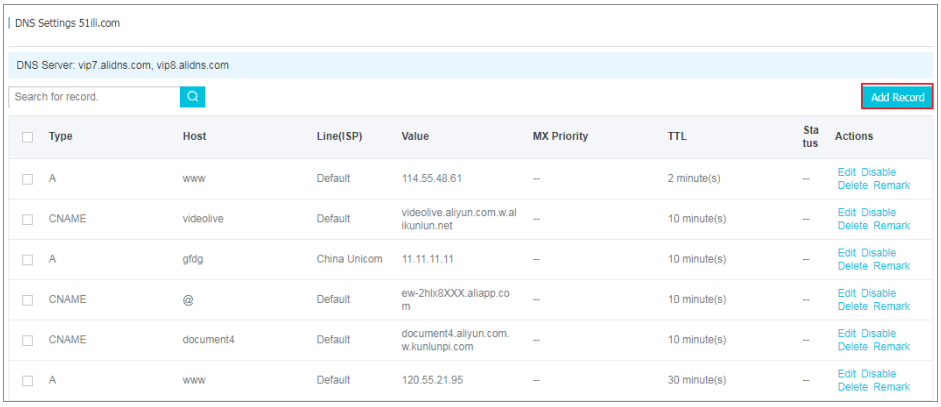
Log on to the Domain console.

Click **Domain Names**.

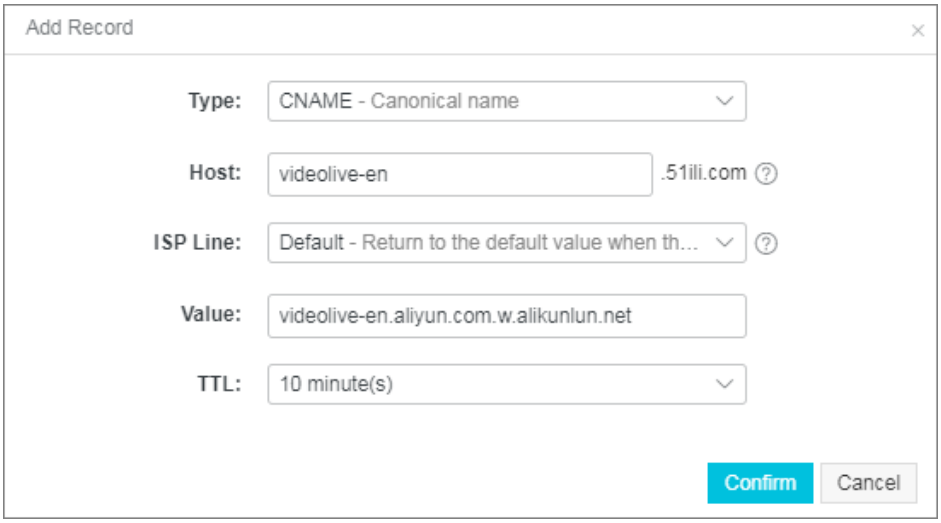
Click **Resolve**.



Click **Add Record**.



Enter the resolution parameters and click **Confirm**.



Select **CNAME-Canonical name** in **Type**.

Enter the secondary domain name of the streaming address in **Host**. For example, if the streaming address is videolive-en.aliyun.com, then the secondary domain name is videolive-en.

Enter the CNAME into **Value** of the domain name list.

- If it is a newly created domain name, the resolution does not require to refresh the DNS.
- Different data is cached on different DNSs. And, if the CNAME changes, it may take up to 48 hours to complete the updates.

Streaming management

Live streaming

A complete live video process includes collection, processing, encoding, packaging, streaming, transmission, transcoding, distribution, decoding, and playing steps. Streaming refers to the process of transmitting live content to the server using streaming tools and other content capturing softwares.

Procedure

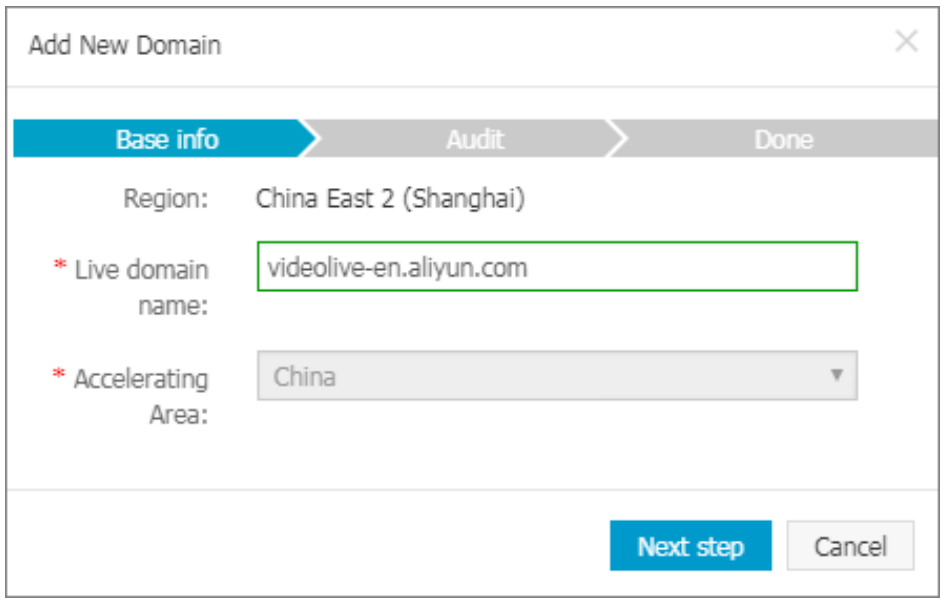
Add a domain name.

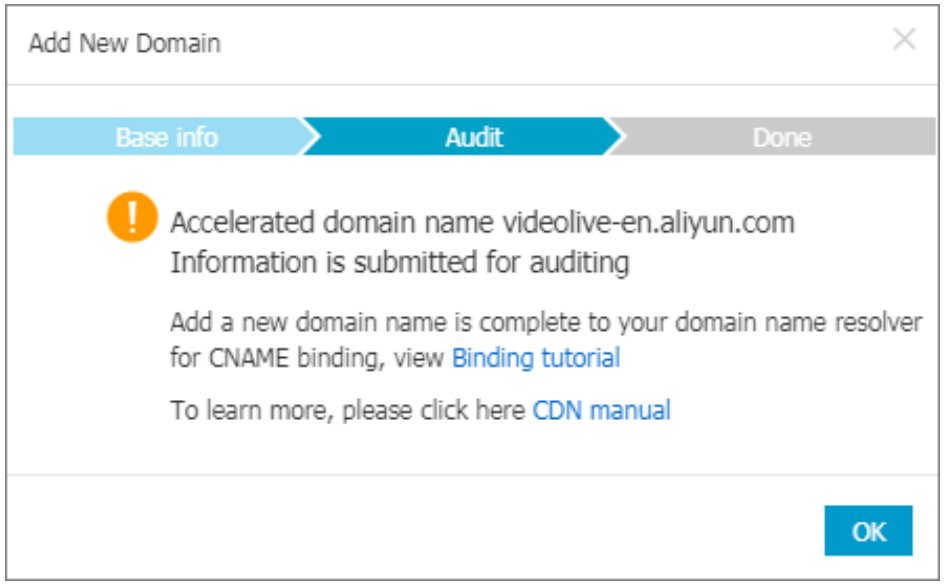
Log on to the ApsaraVideo Live console.

Select the region in **Domains**.

Note: You can select **Singapore**, **China East 2 (Shanghai)** or **China North 2 (Beijing)** in the ApsaraVideo Live console. After selecting a region, the stream is pushed to the corresponding streaming center. If you select **China East 2 (Shanghai)** or **China North 2 (Beijing)**, the stream undergoes domestic video acceleration. If you select **Singapore**, the stream undergoes foreign video acceleration.

Enter the **Live domain name** and click **Next Step**. Your domain name is submitted for auditing.

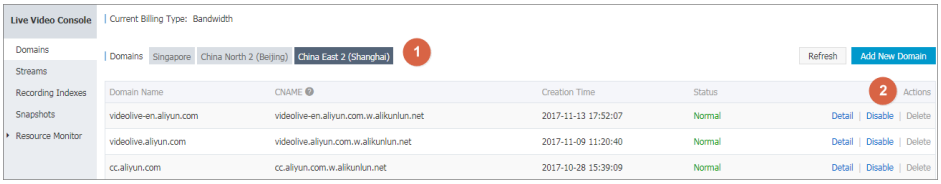




Get the streaming URL.

Select the region in **Domains**.

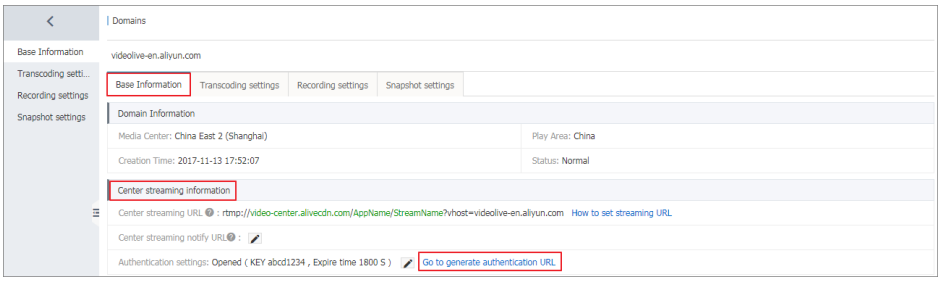
Select the domain name and click **Detail** at the right side.



In **Base Information** > **Center streaming information**, get **authrntication URL**.

Note: The authentication is enabled by default, you must use the **authrntication URL** for streaming. For details, see Live authentication.

Click **Go to generate authentication URL** at the right side of **Authentication settings**.

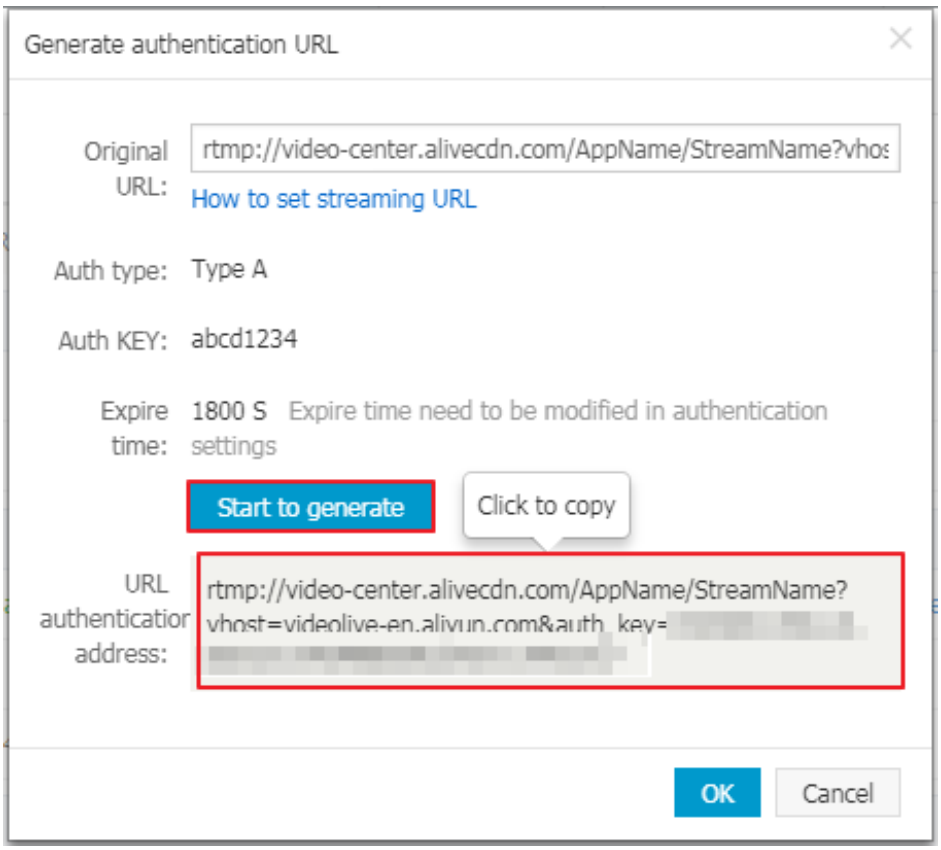


On the **Generate authentication URL** page, click **Start to generate**.

Click to copy the generated **authentication URL**.

Click **OK**.

The generated authentication URLrtmp://video-center.alivecdn.com/AppName/StreamName?vhost=videolive-en.aliyun.com&auth_key=**********can be used for streaming.



Streaming operations.

Copy the streaming address to the streaming tool for the streaming operation.

Common streaming test tools are OBS official download, XSplit official download and FMLE official download.

AppName and StreamName

Live broadcasting address structure

A live video service address consists of three levels of live video management units, that is, the domain name (Domain), an application (AppName) and a live stream (StreamName). You can create multiple apps (AppName) under each domain name (Domain), and multiple live streams (StreamName) under each app.

AppName and StreamName can be edited and customized. Different values generate different streaming and playback addresses.

If an app is named aslive, for example, you can create multiple live streams underlive. The streaming addresses are then as follows:

```
rtmp://video-center.alivecdn.com/{live}/{3}?vhost={live video domain name}
rtmp://video-center.alivecdn.com/{live}/{1}?vhost={live video domain name}
```

```
rtmp://video-center.alivecdn.com/{live}/{2}?vhost={live video domain name}
```

You can also create multiple live streams for the app.

```
rtmp://video-center.alivecdn.com/{live1}/{Stream}?vhost={live video domain name}
rtmp://video-center.alivecdn.com/{live2}/{Stream}?vhost={live video domain name}
rtmp://video-center.alivecdn.com/{live3}/{Stream}?vhost={live video domain name}
```

Live authentication

URL authentication function aims to protect the user’ s website content from the illegal or malicious activity.

It is a safe and reliable anti-theft mechanism that protects site resources by coordinating Alibaba Cloud CDN acceleration node with customer resources site. The customer site provides customer with an encrypted URL (including authentication information), which the user then uses to make a request to the acceleration node. The acceleration node verifies the authentication information in the encrypted URL to determine the validity of the request (that is, whether to respond normally to a valid response or refuse an invalid response), thus effectively protecting customer site resources.

Note: The authentication function is enabled by default for the newly created domain name since Janurary 1, 2018. You can adopt the authentication by default, or custimize it on the Apsaravideo Live console.

Authentication URL composition

Components

Live streaming address/playaddress+verification string, the verification string is caculated according to md5 algorithm by usingauthentication key+expiration time. This address is applicable to PC end, mobile end, third-party streaming and play tools.

> The **Auth KEY** field can be set by the user,
>
> If the **Expire time** in which user visits customer source server exceeds the self-defined time (**timestamp** field designation), the authentication is invalid. For example, if the expire time is 1800s, and the user sets the visit time as 2020-08-15 15:00:00, the link expires at 2020-08-15 15:30:00.

URL authentication concept

Encrypted URL component

```
http://DomainName/Filename?auth_key=timestamp-rand-uid-md5hash
```

Authentication field description

Field	Description
timestamp	expire time, positive integer, fixed length 10, seconds measured from 1970-01-01. Used to control expire time, integer of 10 digit, expire time 1800s.
rand	random number, usually set to 0
uid	not used yet (set to 0)
md5hash	verification string caculated according to md5 algorithm, lowercase letters and digits are supported, fixed length 32

When the server receives the request, it first determines whether the timestamp in the request is shorter than the current time. If it is shorter, then the expire time is thought to be invalid and it returns an HTTP 403 error. If the timestamp is longer than the current time, then a same string is structured (refer to the following composition mode of sstring). The server then calculates the HashValue according to MD5 algorithm, and compares this value with md5hash in the request. If the values are the same, then the authentication is successful; otherwise, it returns an HTTP 403 error.

HashValue is calculated with the following strings,

```
  sstring = "URI-Timestamp-rand-uid-PrivateKey" ( URI is the address corresponding to the user's request object, not including parameters , for example : /Filename )
HashValue = md5sum(sstring)
```

Examples

Pass **req_auth** request object

```
http://cdn.example.com/video/standard/1K.html
```

Set the key to: aliyuncdnexp1234 (set by the user)

The expire time of authentication is 2015-10-10 00:00:00, the seconds calculated is: 1444435200.

The server structures a signature string used to calculate Hashvalue

```
/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234
```

The server calculates HashValue according to the signature string

```
HashValue = md5sum("/video/standard/1K.html-1444435200-0-0-aliyuncdnexp1234") =
80cd3862d699b7118eed99103f2a3a4f
```

The URL, when making a request, is

```
http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-0-
80cd3862d699b7118eed99103f2a3a4f
```

The calculated HashValue is consistent with md5hash = 80cd3862d699b7118eed99103f2a3a4f in the user’ s request, and the authentication succeeds.

Note: We recommend that the streaming address performs encryption and authentication operations for enhanced security.

Procedure

Authentication by default.

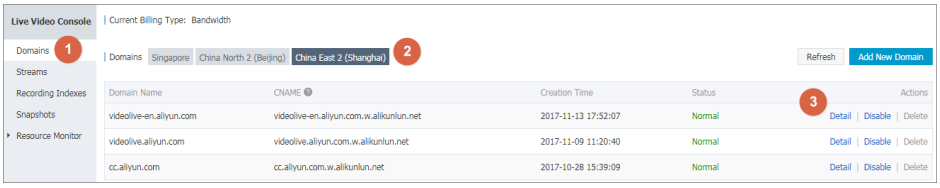
The authentication function is in the **Opened** state by default. The **Main KEY** is abcd1234，and the **Expire time** is 1800s. The authentication expires if the time exceeds 1800s.

Log on to the ApsaraVideo Live console.

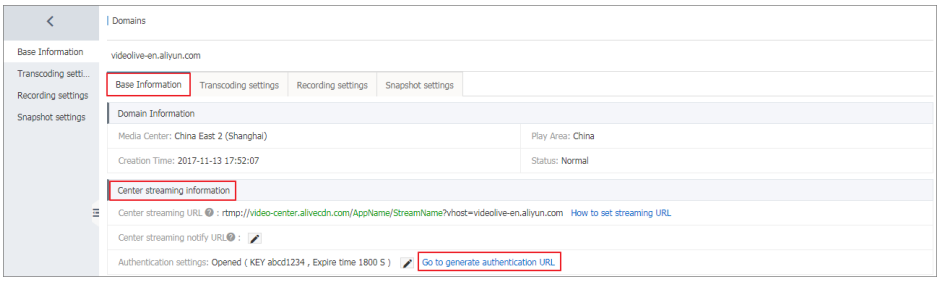
Click **Domains** in the left-side navigation pane.

Select the region.

Select the domain name, and click **Detail** at the right side.



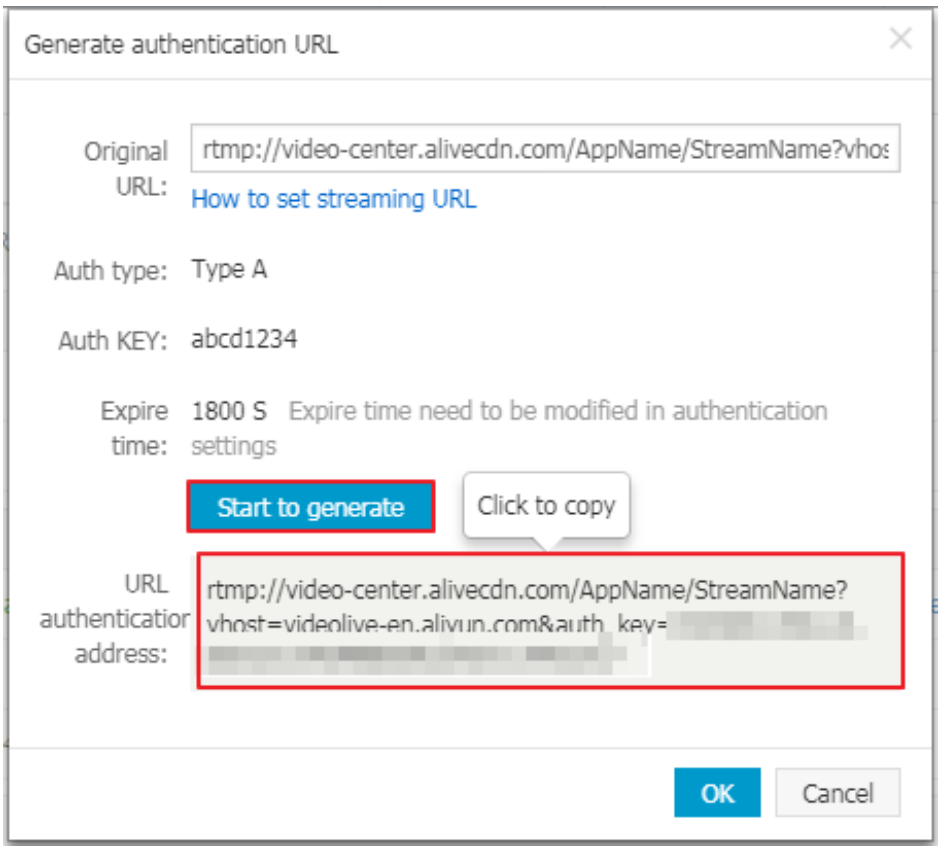
In **Base Information** > **Center streaming information**, click **Go to generate authentication URL** at the right side of **Authentication settings**.



In the **Generate authentication URL** page, click **Start to generate**.

> Note: A demo streaming URL is generated in the **Original URL** field, the playback address is custimized according to your playing requirement. If you want to set a new custom AppName and StreamName, you need to replace the AppName and StreamName in the streaming URL with the AppName and StreamName you customize respectively, and then generate **authentication URL**.

Click to copy the generated **URL authentication address**.



Click **OK**.

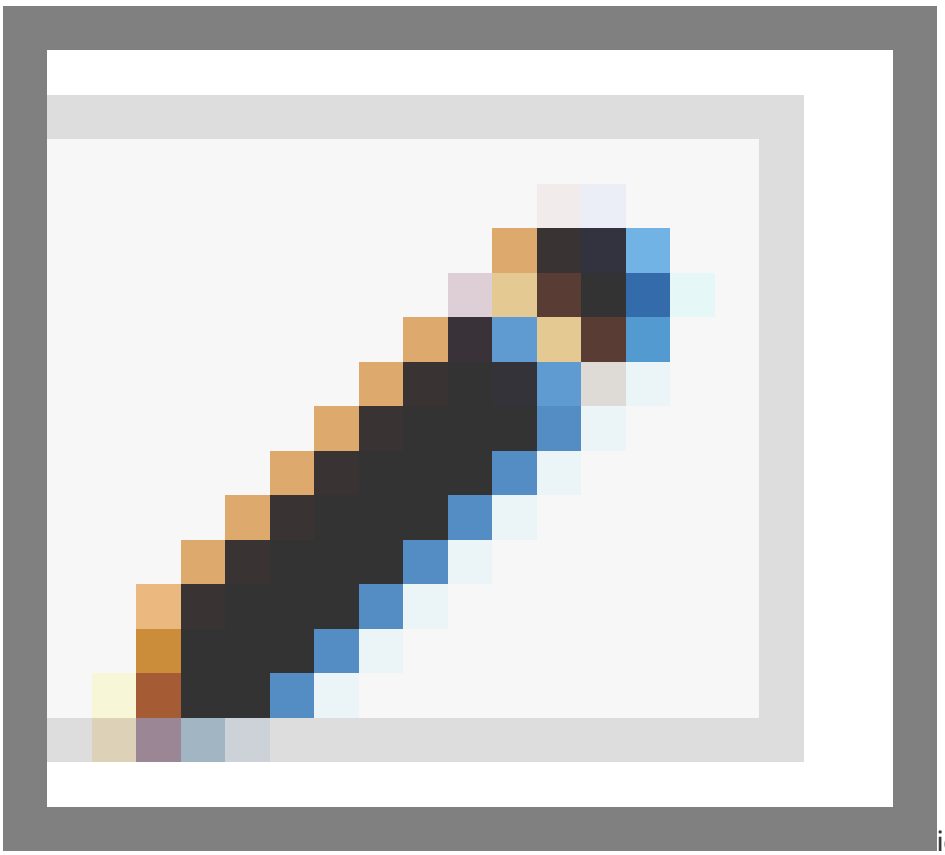
The generated **Authentication URL** rtmp://video-center.alivecdn.com/AppName/StreamName?vhost=videolive-en.aliyun.com&auth_key=********** can be used for streaming and playback.

> Note: The authentication is set at the domain name level. If the authentication function is enabled under the domain name, all the streaming addresses under the domain name must perform authentication operation. Meanwhile, the playback address corresponding to the streaming address must perform authrntication. We recommend that you use the authentication URL for playback operation.

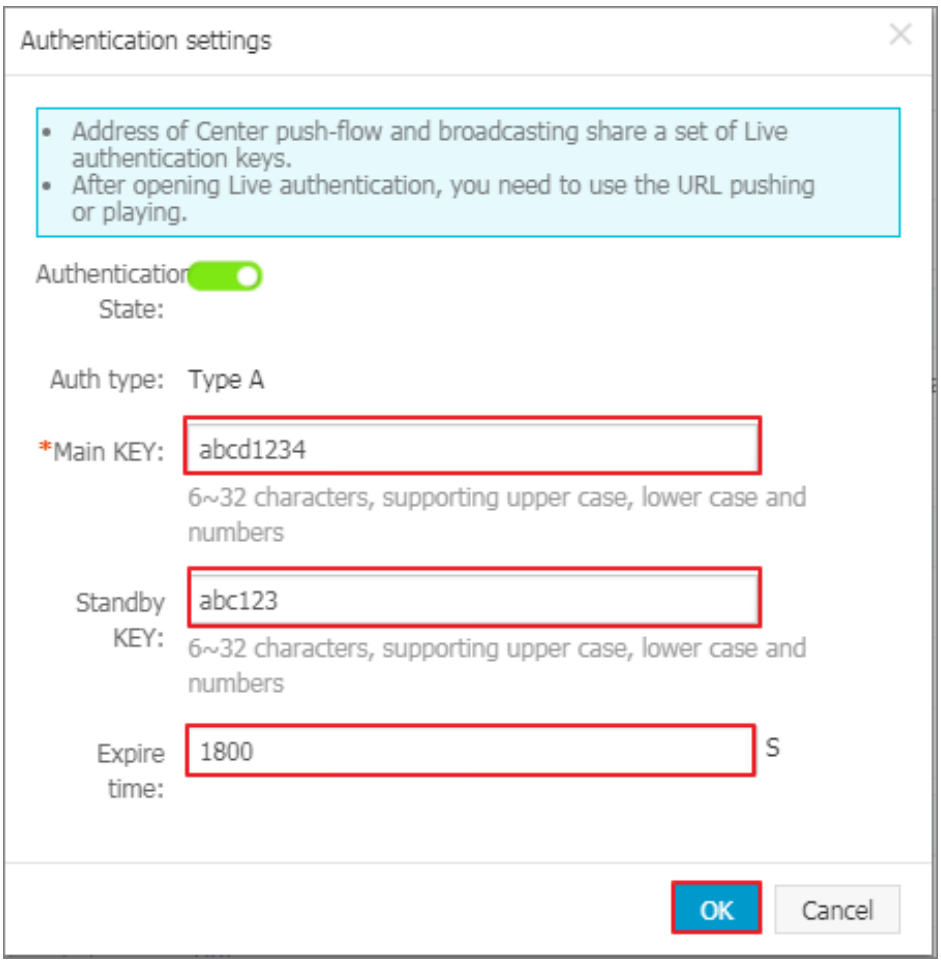
Customize authentication

If you don’ t adopt the configration by default, you can also customize **Main KEY**, **Standby KEY**, **Expire time**, **AppName** and **StreamName**, and then generate **Authentication URL** for streaming and playback.

In **Base Information** > **Center streaming information**, click the


icon at the right side of **Authentication settings**.

In the **Authentication settings** page, customize the **Main KEY**, **Standby KEY**, and **Expire time** and click **OK**.



Note:

- **Main KEY** is a key for calculating encrypted string. If the **Main KEY** is changed, all addresses using the **Main KEY** instantly becomes invalid. If the **Standby KEY** is changed to the **Main KEY**, the streaming or playback address using the **Main KEY** does not become invalid instantly, but uses the **Standby KEY** as a mechanism for performing the switch.

Click **Go to generate authentication URL** at the right side of **Authentication settings** to set the **AppName** and **StreamName** on the **Generate authentication URL** page.

Original URL : rtmp://video-center.alivecdn.com/AppName/StreamName?vhost=videolive-en.aliyun.com, wherein,

Thevideo-center.alivecdn.comis a server of the live video center and can be customized. For example, if your domain name isvideolive-en.aliyun.com(Note: This domain name cannot be the same with your

CDN domain name), you can set the DNS and point your domain name CNAME tovideo-center.alivecdn.com.

AppNameis the app name. This parameter can be customized.

StreamNameis the stream name. This parameter can be customized.

Thevhostparameter specifies a domain name for eventual playback on an edge node, namely your live video CDN domain name.

Streaming notification URL

Function overview

Streaming notification URL or callback URL, is mainly used to call back stream-status real-time information and promptly notify users about the video streaming results.

You can add a callback URL of your background server in the console to Alibaba Cloud, so that when the stream status changes, Alibaba Cloud can send a GET request to your server using the HTTP interface and send the real-time feedback on whether the video streaming suceeds or fails.

Attentions

Principle: The real-time stream status feedback is implemented through GET requests sent to the user’ s server through the HTTP interface . The user server returns 200 responses to the interface. You do not have to identify the URL if normal access is allowed. The following requirements are imposed on the URL responses: In case of access time-out, the URL can be retried. The current time-out duration is 5 seconds, the number of retries is 5, and the interval is 1 second.

It supports the HTTPS address authorized by the certificate authority.

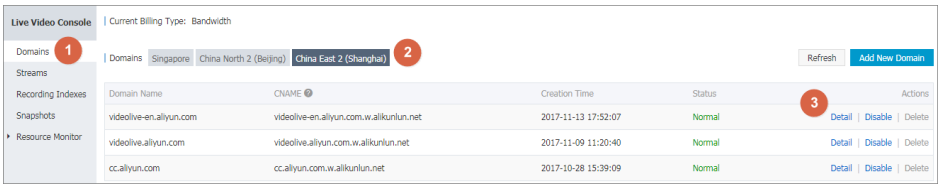
Procedure

Log on to the ApsaraVideo Live console.

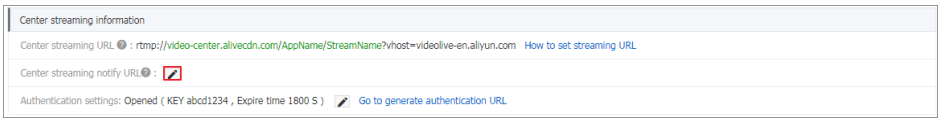
Click **Domains**.

Select the region.

Select the domain name and click **Detail** at the right side.



In **Base Information** > **Center streaming information**, set the **Center streaming notify URL**.



Example:

```
https://live.aliyunlive.com/pub? action=publish & app=xc.cdnpe.com & appname=test01 & id=test01 &
ip=42.120.74.183 & node=cdnvideocenter010207116011.cm3
```

Configuration in the console is supported, and is optional.

Parameters	Value description
time	Unix timestamp.
usrargs	Streaming parameters.
action	**Publish** indicates push streaming, and **publish_done** indicates completion of push streaming.
app	The default value is the custom streaming domain name. If no streaming domain name is bound, it is the playback domain name.
appname	Application name.
id	Stream name. **Note: You must convert Stream name to lowercase**.
node	The name of the node or machine in the CDN that receives the stream.
IP	IP address of the client that pushes the stream.

HTTPS secure acceleration configuration

Function overview

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a secuity suite of the normal HTTP channel focusing on security. It encapsulates HTTP with the SSL/TLS protocol with SSL/TLS protocol as its security base.

Advantages of HTTPS acceleration

Key user data is encrypted during transmission to prevent sensitive information from the leakage, such as session IDs or cookies that can be maliciously used by attackers.

Data integrity verification is performed during transmission to prevent the hidden danger of man in the middle (MITM) such as DNS or content hijacked or tampered by an unverified third party.

Alibaba Cloud ApsaraVideo Live provides HTTPS secure acceleration schemes. You must enable the secure acceleration mode and then upload the certificate/private key of the CDN domain. The ApsaraVideo Live console also supports viewing, disabling, enabling, and editing the certificates.

If the certificate is configured correctly and enabled, both HTTP access and HTTPS access are supported. If the certificate does not match or is disabled, only HTTP access is supported.

Notes

Configuration restrictions

Feature	Description
Disable and **Enable** HTTPS status	**Disable**: No HTTPS requests are supported and no certificate/private key information is retained. **Enable**: You must re-upload the certificate/private key to enable the certificate again.
View certificate	It allows you to view the certificate only. Viewing private key information is not supported.
Modify and edit certificate	Modification and editing of the certificate are supported, but the effective period for performing these operations is 1 hour. Perform the operation with caution.

Certificate restrictions

The certificate and private key of a CDN domain for which **HTTPS secure acceleration** is enabled, must be uploaded. Both the certificate and private key must be in PEM format.

> Note: Tengine used in ApsaraVideo Live is based on Nginx, which means certificates that can be read by Nginx are supported (the certificates must be in PEM format).

Only SSL/TLS handshakes containing SNI information is supported.

The certificate and private key that you upload must have a one-to-one correspondence with each other; otherwise, the verification fails.

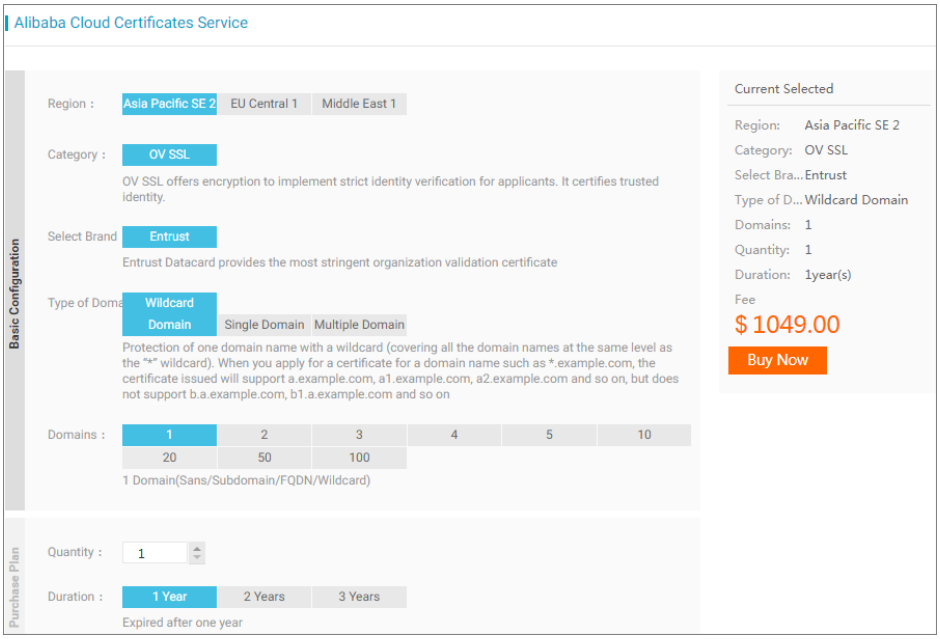
The effective period of the updated certificate is 1 hour.

Private key with a password is not supported.

Configuration guide

Step 1. Buy a certificate.

To enable **HTTPS secure acceleration**, you must have a certificate that matches the CDN domain. Click **Buy Now** at the **Alibaba Cloud Certificates Service** to buy a certificate.



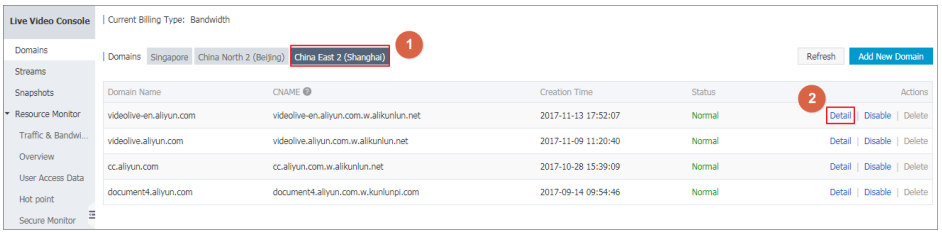
Step 2. Configure the live video domain name.

Enable HTTPS secure acceleration.

Log on to the ApsaraVideo Live console.

Select the region in **Domains**.

Select the domain name and click **Detail** at the right side.



Click **Base Information** > **Settings** to perform HTTPS Settings.

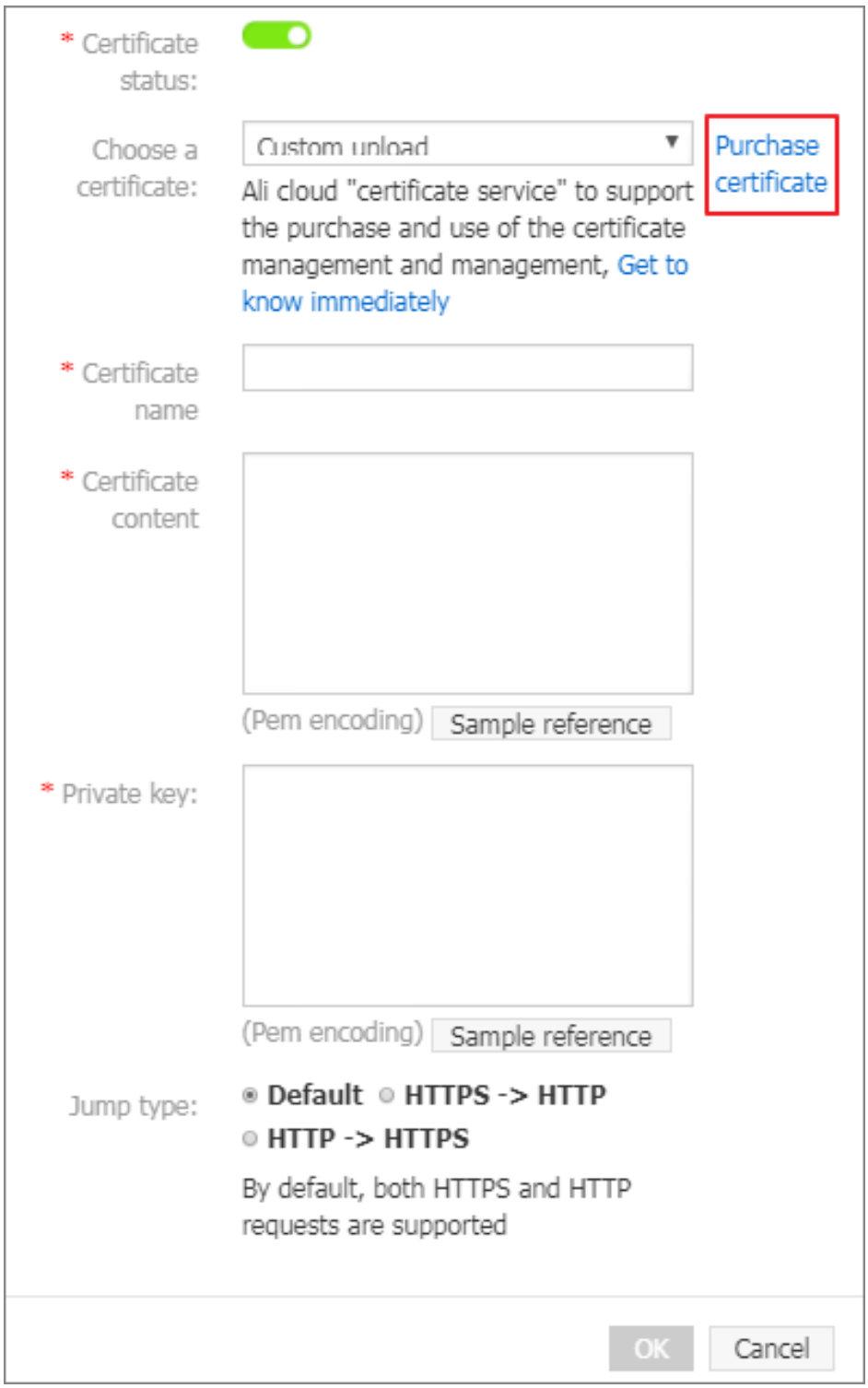
Click **HTTPS secure acceleration** to go to the setting page, and then enable **Certificate Status**.

Select a certificate.

Alibaba Cloud ApsaraVideo Live supports two types of certificates for deployment.

Self-owned certificate: You must set the certificate name and then upload the certificate content and private key. The certificate is then saved in the Alibaba Cloud SSL Certificates console. You can view it under **My Certificates** tab.

Alibaba Cloud certificate: Certificates purchased from the Alibaba Cloud Certificates Service are supported. You can select a certificate name to adapt to the CDN domain.



NOTE: Only certificates in PEM format are supported.

Set the redirection type.

Forced redirection is supported: The system forces redirection of the users' original

request methods by default.

For example, if **HTTP > HTTPS** redirection is enabled and a user initiates an HTTP request, the server returns a 302 redirect response and the original HTTP request is forcibly redirected to the HTTPS request.

Default: HTTP and HTTPS requests are compatible.

HTTP > HTTPS redirect: Users' HTTP requests are forcibly redirected to the HTTPS requests.

HTTPS > HTTP redirect: Users' HTTPS requests are forcibly redirected to the HTTP requests.

Step 3. Verify whether the certificate has taken effect.

You can access resources by HTTPS when the settings are completed and the certificate are active now. If a green HTTPS mark appears in your browser, it indicates that currently a private connection is established with the website and HTTPS secure acceleration is effective.

View the stream information

Procedure

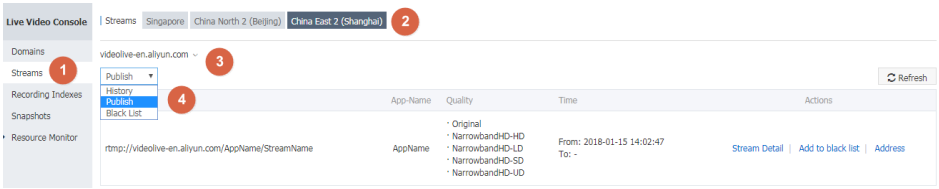
Log on to the ApsaraVideo Live console.

Click **Streams** in the left-side navigation pane.

Select the region.

Select the domain name.

You can then select **History**, **Publish** or **Black List** based on your needs to check the streams information under different status.



Bit rate and frame rate monitoring

In a live video environment, buffering interference often leaves a biggest impact on the live video streaming. The general cause is poor bandwidth stability of the uplink transmission.

The ApsaraVideo Live console monitors the uplink traffic. This can easily view the uplink transmission status of the live stream to check if there is any problem.

View the monitoring data

Log on to the ApsaraVideo Live console.

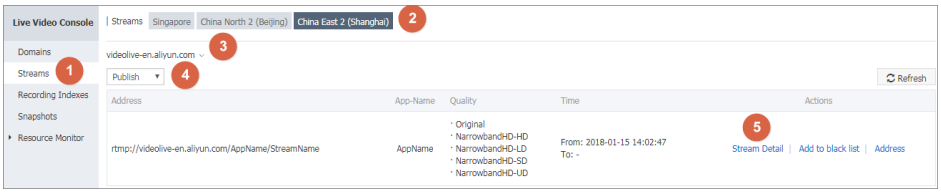
Click **Streams** in the left-side navigation pane.

Select the region.

Select the domain name.

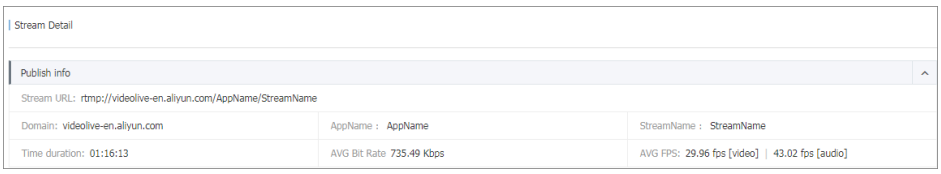
Select the stream status.

Select the streaming address and click **Stream Detail** at the right side.

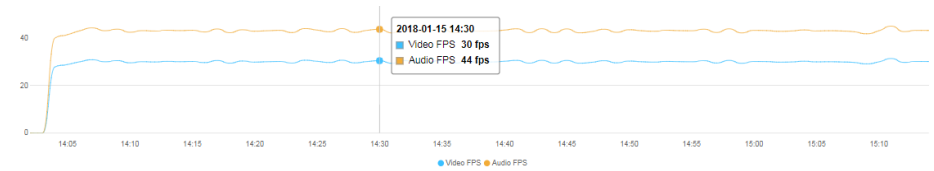


View the stream data such as Publish info, Video FPS, Audio FPS and Bit Rate.

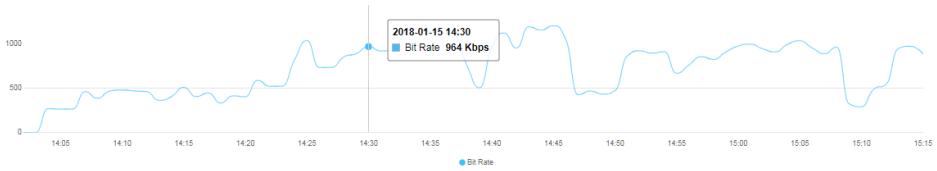
Publish Info



Frame rate



Bit rate



On an average, the stream data is updated every minute. You can view the uplink transmission on the **Stream Detail** page.

When the data status appears to be smooth, the valley and the peak values are comparatively stable. This indicates that the uplink transmission is comparatively stable too. If sharp fluctuations occur, we recommend that you check the stability of the uplink transmission.

Causes of choppy streaming

Several factors can cause video playback to buffer incorrectly. The following recommendations are troubleshooting tips that may help resolve streaming issues:

Mobile phone configuration.

Streaming consumes CPU resources. During the streaming process, low-end mobile phones with poor hardware configuration may encounter poor quality video if the overall CPU usage exceeds 80%. This affects the video collection and viewing experience on the user terminals.

Video collection parameter settings.

A video must have at least 15 frames per second (FPS) or higher to make sure smooth playback. An FPS set lower than this rate may result in unstable video quality. Note that if the frame rate is set for more than 30 FPS, the image content may not be viewed naturally by most of the viewers. Additionally, a higher frame rate also increases the bandwidth cost of the video transmission.

Network bandwidth.

Common network factors include:

Network bandwidth size

Confirm the bandwidth size provided by the network operator and whether the bandwidth is sufficient for this live video transmission.

Downlink bandwidth usage

Check whether any data downloading activity occupies the network bandwidth.

System resource usage

Check whether a large number of programs are running in the background, and terminate any unnecessary programs to save the resources.

Add a streaming address to the blacklist

After the streaming address is added to the blacklist, the streaming operations under this domain name, and any operations thereafter, are suspended. To continue the streaming operations, you must restore the address from the blacklist.

Add the address to the blacklist

Log on to the ApsaraVideo Live console.

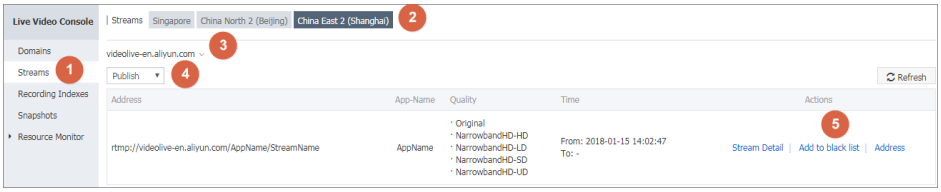
Click **Streams** in the left-side navigation pane.

Select the region.

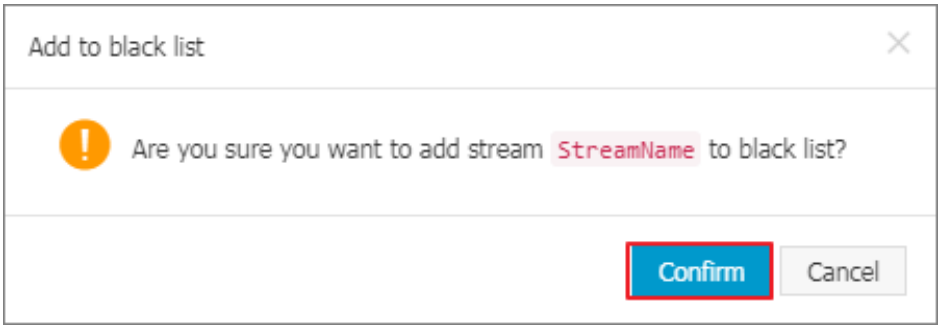
Select the domain name.

Select the status of the stream.

Select the address and click **Add to blacklist** at the right side.



Click **Confirm**.



The address is added to the blacklist successfully.

Restore the address from the blacklist

If you want to restore the address from the blacklist, you must find the adresss in the blacklist first and then restore it.

Log on to the ApsaraVideo Live console.

Click **Streams** in the left-side navigation pane.

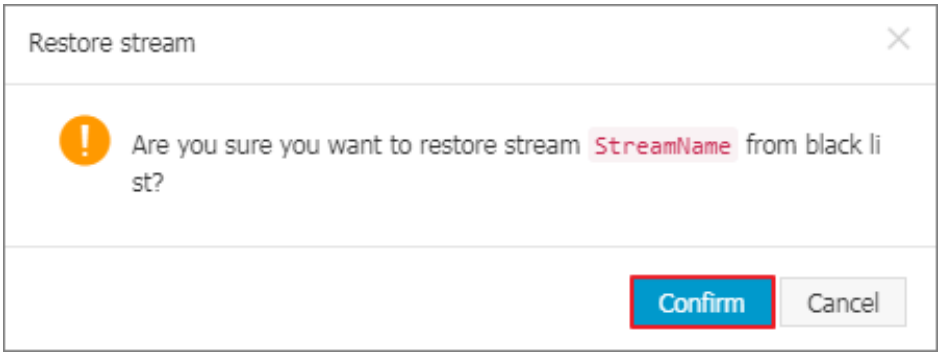
Select the region.

Select the domain name.

Select **BlackList**.

Select the address and click **Restore** from the **Actions** column, from the selected address.

Click **Confirm**.



The address is restored from the blacklist successfully.

Streaming address

The live streaming includes **Center Streaming** and **Edge Streaming**.

Center Streaming: Pushes the video streams to the live center. It is applicable to the scenarios where the live video is played in a single region.

Edge Streaming: Preferentially pushes the video content to the CDN node closest to user, and then to the live center through the intranet. Alibaba Cloud has more than 1,000 CDN nodes, covers the big or small cities, and is appropriate for the scenarios where the host or hostess is located in different regions.

The structure of the streaming address

A streaming address consists of three live management units, that is Domain, AppName and StreamName. More than one AppName can be created under each Domain, and more than one StreamName can be created under each AppName.

Center streaming

Address example:rtmp://video-center.alivecdn.com/AppName/StreamName?vhost= stream playing domain

For example: You have an App. The stream playing domain ispull.aliyunlive.com; the Appnameislive; and more than one live streams can be created underlive.

RTMP format: rtmp: //video-center.alivecdn.com/live/stream01?vhost=pull.aliyunlive.com

Edge streaming

Address example:rtmp://streaming domain/AppName/StreamName

For example: You have an APP. The streaming domain ispush.aliyunlive.com; the stream playing domain ispull.aliyunlive.com; theappnameislive; and more than one streams can be created underlive. The streaming address is:

RTMP format : rtmp:// push.aliyunlive.com/live/stream01

The corresponding relationship between the streaming address and the palying addess

TheAppNameandStreamNamein the live streaming address can be customized. Different name generates different streaming and playing addresses.

The corresponding relationship between center streaming address and the playing address

Note: The rules of playing address for FLV and HLS and those for RTMP are the same.

http:// pull.aliyunlive.com/liveApp/liveStream.flv

http:// pull.aliyunlive.com/liveApp/liveStream.m3u8

The corresponding relationship between edge streaming address and the playing address

Note: The rules of playing address for FLV and HLS and those for RTMP are the same.

http:// play.aliyunlive.com/liveApp/liveStream.flv

http:// play.aliyunlive.com/liveApp/liveStream.m3u8

Playback address

Original image address

Live video addresses can be classified into original image addresses and transcoded addresses.

Original image address

Original images are original video streams that are not transcoded. The original image address is in the format of Playback domain name+AppName+StreamName.

Alibaba Cloud provides three playback protocols that can be applied to the multiple terminals and platforms.

	Advantage	Disadvantage	Latency	Feature	Applicable terminal
RTMP	Low latency	Unstable during high concurrency Players that support related protocols must be developed for iOS. Usage of the non-standard TCP ports	1s to 3s	TCP persistent connection	PC end
HLS	Cross-platform Playing using HTML5 decompressed packet	High latency	>10s	HTTP short connection	PC end and mobile end
HTTP-FLV	Low latency Playing using HTML5 decompress	Playing through the integrated SDKs	1s to 3s	TCP persistent connection	PC end

	ed packet				

Playback addresses of different specifications:

RTMP format: rtmp:// live.aliyun.com/{AppName}/{StreamName}

FLV format: http:// live.aliyun.com/{AppName}/{StreamName}.flv

M3U8 format: http:// live.aliyun.com/{AppName}/{StreamName}.m3u8

Example

The streaming address is:

rtmp://video-center.alivecdn.com/{live}/{3}?vhost={Live video domain name}

The corresponding playback addresses are:

rtmp:// play.aliyunlive.com/{live}/{3}

http:// play.aliyunlive.com/{live}/{3}.flv

http:// play.aliyunlive.com/{live}/{3}.m3u8

Transcoding address

Transcoding template

The ApsaraVideo Live transcoding service provides **NarrowbandHD templates**.

- The **NarrowbandHD template** relies on Alibaba Cloud’ s proprietary narrowband HD image processing technology to achieve a higher compression ratio while maintaining the same image quality and saving more live broadcast traffic.

Playback address

Different transcoding temlates correspond to different playback addresses. The playback address are spliced based on different transcoding rules.

Rule of playback address splicing:Live video domain name+AppName+StreamName+Transcoding template ID

Transcoded template IDs corresponding to different specifications and templates:

Template\Specification	LD	SD	HD	UHD
Original image	None	None	None	None
High-quality transcoding template	ld	sd	hd	ud

Example of playback address splicing:

RTMP format:rtmp://+{Live video domain name}+/{AppName}/+/{StreamName}+{Trancoding template ID}

Example:rtmp://live.aliyunlive.com/AppName/StreamName_sd

FLV format: http://+{Live video domain name}+/{AppName}/+/{StreamName}+{Transcoding template ID}.flv

Example:http://live.aliyunlive.com/AppName/StreamName_sd.flv

M3U8 format:http://+{Live video domain name}+/{AppName}/+/{StreamName}.m3u8

Example:http://livetest01.aliyunlive.com/AppName/StreamName.m3u8

Note: Currently playback in the M3U8 format is not supported.

Template parameters

NarrowbandHD template

Template name	Template ID	Resolution (self-adaptive height and width)	Bit rate (kbps)
LD	ld	360	≤420
SD	sd	432	≤580
HD	hd	648	≤1100
UHD	ud	1080	≤1900

Restrictions

Only one transcoding template type is supported for each AppName.

Each domain name supports a maximum of two channels of transcoding concurrent streams. That is, a maximum of two channels of live broadcast using transcoding templates can be conducted under one domain name.

If the provided ApsaraVideo Live service cannot meet your current business needs, you can open a ticket to describe your needs or contact your customer service manager.

Transcoding rules

ApsaraVideo Live supports latancy-based transcoding. If the system detects that a channel of live stream is not being watched, the system does not perform transcoding. If the system detects watching behavior, transcoding is immediately performed. Transcoding stops if no watching behavior is detected in 10 minutes.

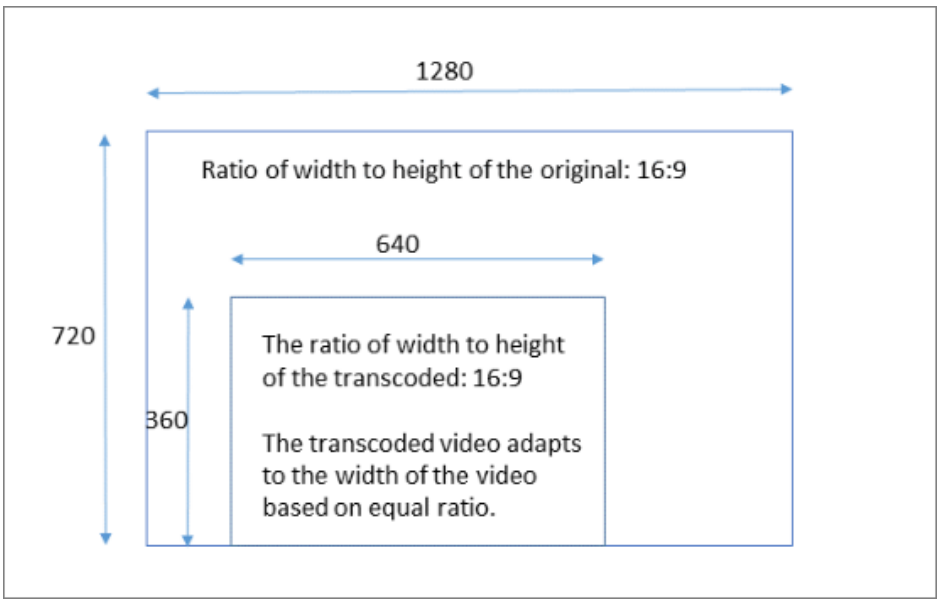
After a channel of video is transcoded, transcoded video is played for viewers.

Transcoding is a not required service. You can configure transcoding as needed.

Currently transcoding supports FLV and RTMP formats.

Width self-adaptation

Transcoding uses self-adaptive width algorithms. Width of transcoded video is self-adaptive according to the height of the original streaming video.



Transcoding

For details about transcoding address splicing rules, see Transcoding address.

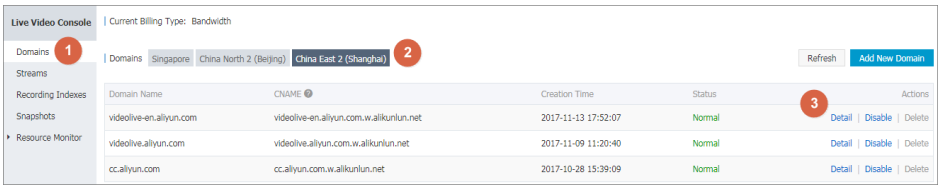
Procedure

Log on to the ApsaraVideo Live console.

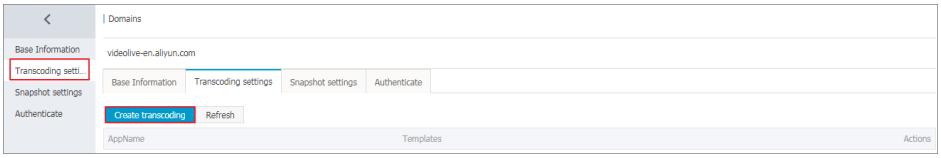
Click **Domains**.

Select the region.

Select the domain name and click **Detail** from the **Actions** column.



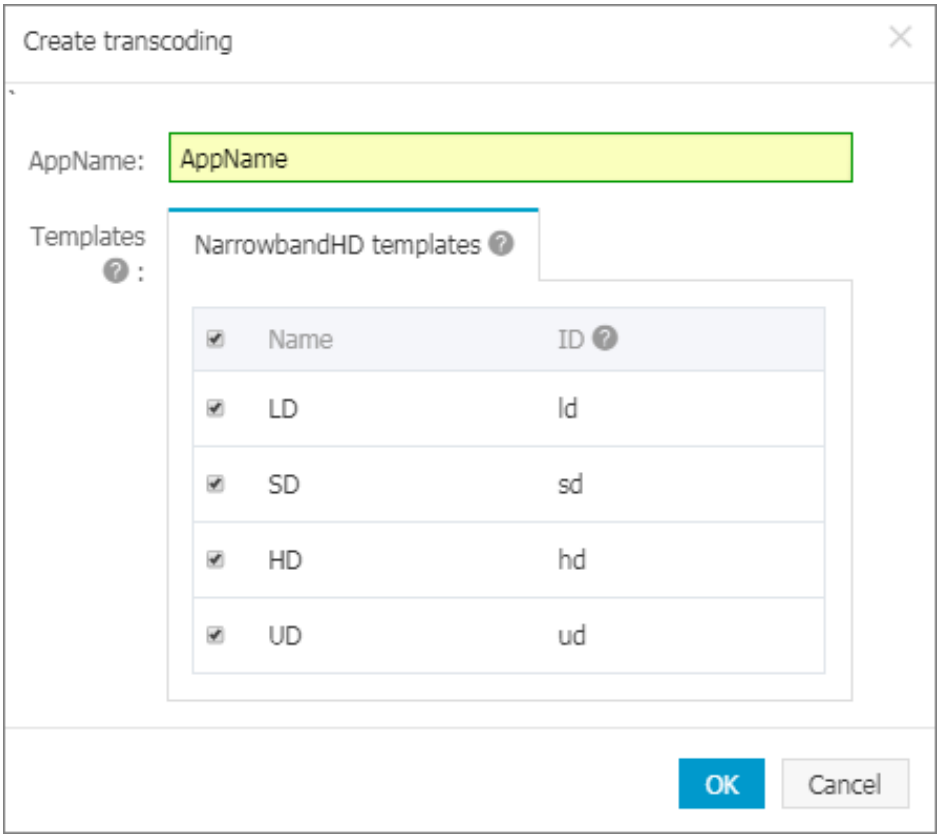
Click **Transcoding settings** and click **Create transcoding**.



Set the transcoding parameters and click **OK**.

Enter the AppName.

The transcoding template becomes effective only when the entered AppName matches that in the streaming address.



Select the transcoding template name.

Note: The high-quality (narrowband HD) transcoding template contains four transcoding templates: LD, SD, HD, and UHD.

Video playback.

After the transcoding template is created, you can perform video streaming. Video transcodes automatically according to the transcoding template. The transcoded video can be previewed on the ApsaraVideo Live console.

For more details about live video streaming, see Live streaming.

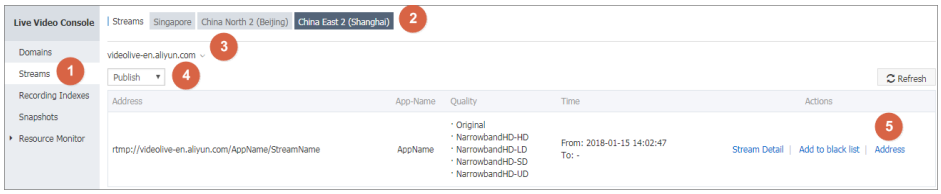
Click **Streams** in the left-side navigation pane.

Select the region.

Select the domain name.

Select the stream status from the drop-down list.

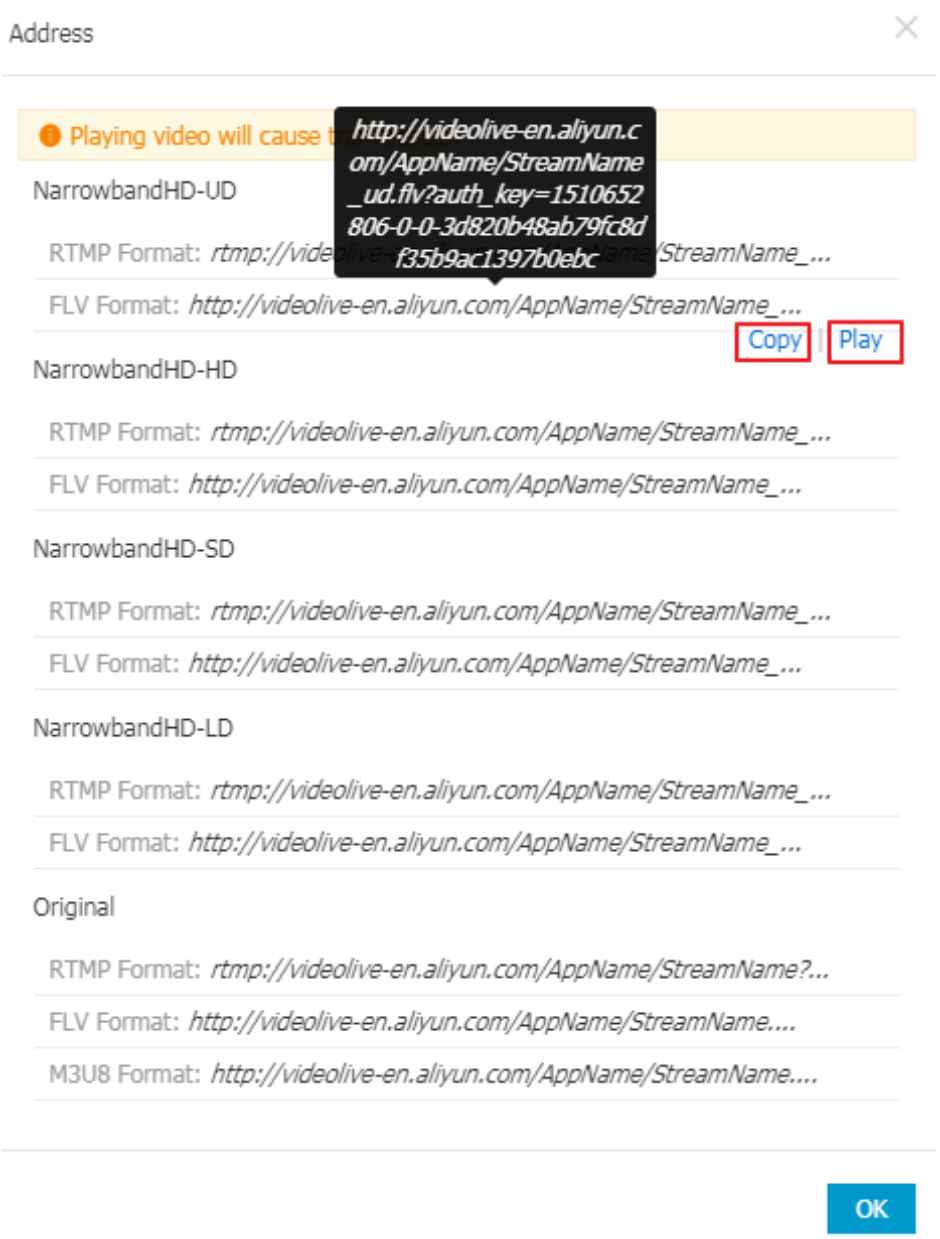
Select the streaming address, and click **Address** from the **Actions** column.



The playback addresses of the transcoded video and original video are displayed in the address list.

Hover the cursor over an address, the **Copy** and **Play** link are displayed.

Click **Copy** > **Confirm**. To play the video, paste the address in the address field. You can also click **Play** to play the video in the dialog box of the web player.



Recording management

Store live recordings in OSS

ApsaraVideo Live allows you to record source video streams. It supports m3u8 (.ts fragment files), mp4, and flv format, along with recording duration settings. Video files are saved in OSS. After a streaming ends, a recording index file for the streaming is generated automatically. The service also supports the generation of custom recording index files (m3u8, mp4, or flv files) based on your specified recording start time and end time.

Under a live video CDN domain name, the livestream recording settings are differentiated by the AppName of the livestream. That is, streams under the same AppName all perform recording operations following the settings for this AppName.

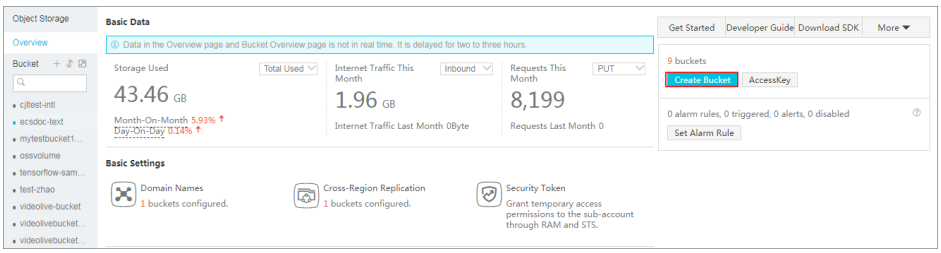
To facilitate the playback of your recorded content, the live recordings must be stored in OSS and your media bucket. If they are stored in the media bucket, you must first activate Media Transcoding (MTS) and then set the input and output media buckets. This document takes the recordings stored in OSS as an example. For recordings stored in media bucket, see Convert live recordings to media files.

Procedure

Step 1. Create an OSS bucket

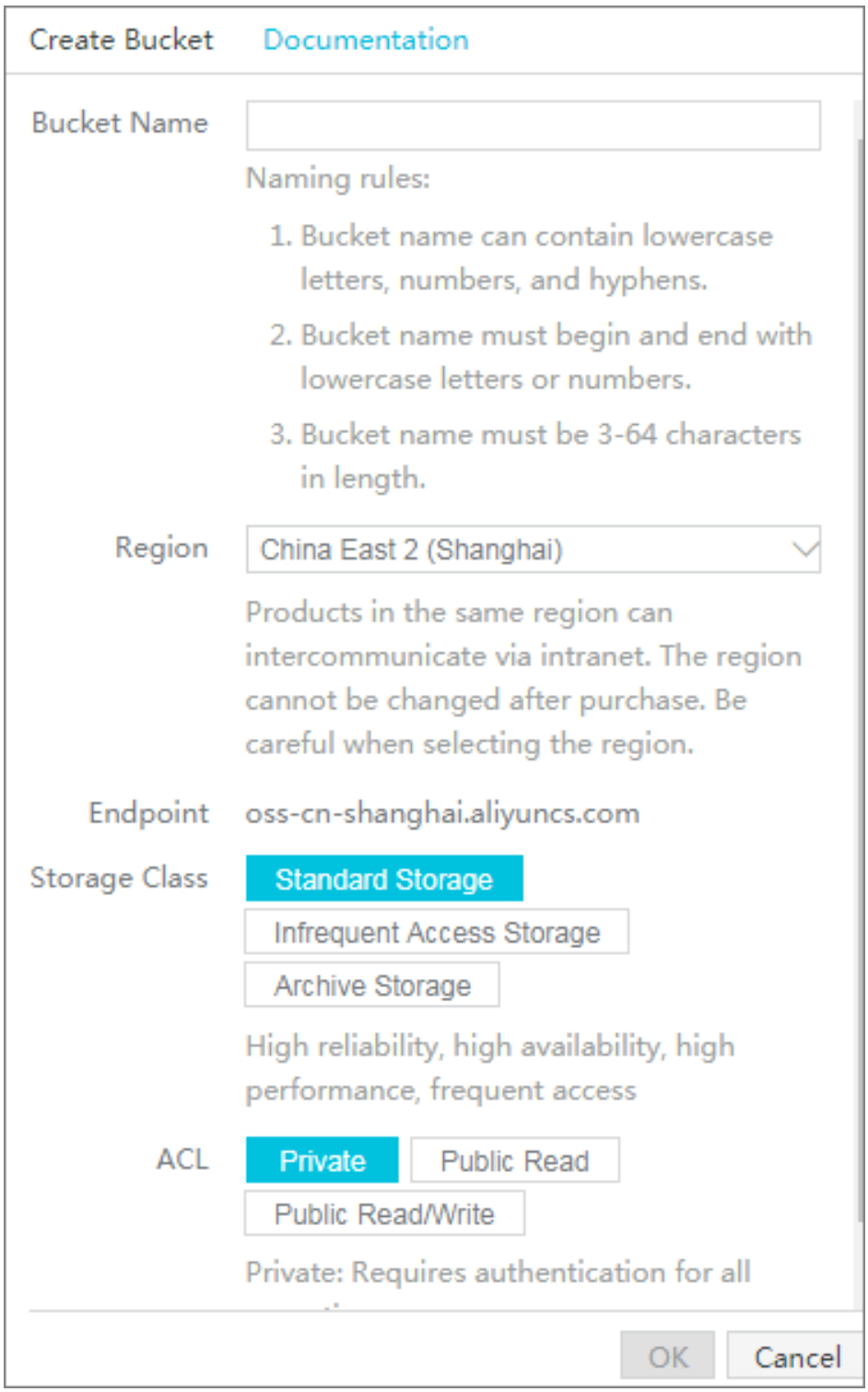
When creating a live recording service, you must store videos in an OSS bucket. Therefore, you must first create an OSS bucket.

Log on to the OSS console and click **Create Bucket**.



Enter the bucket information.

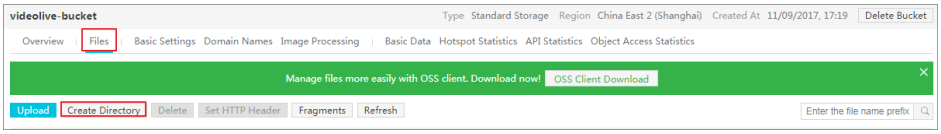
Select the region where the live video domain name is located as the **Region**. The live video domain name is located in **China East 2 (Shanghai)**. Therefore, you must select **China East 2 (Shanghai)**.



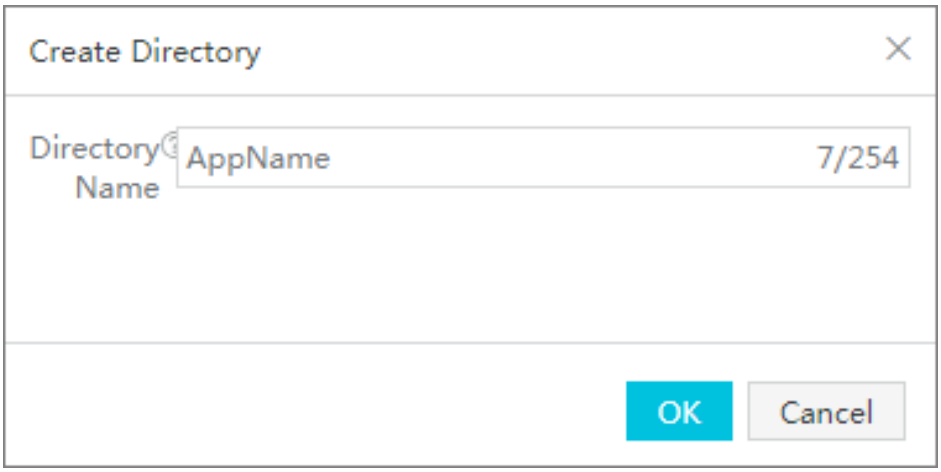
Note: After the bucket is created, check that the region of the bucket is consistent with that of the live video domain name. You can also create bucket folders as needed.

In **Files**, click **Create Directory**.

If you have many recording files, you can create folders to classify them so as to facilitate recording management.



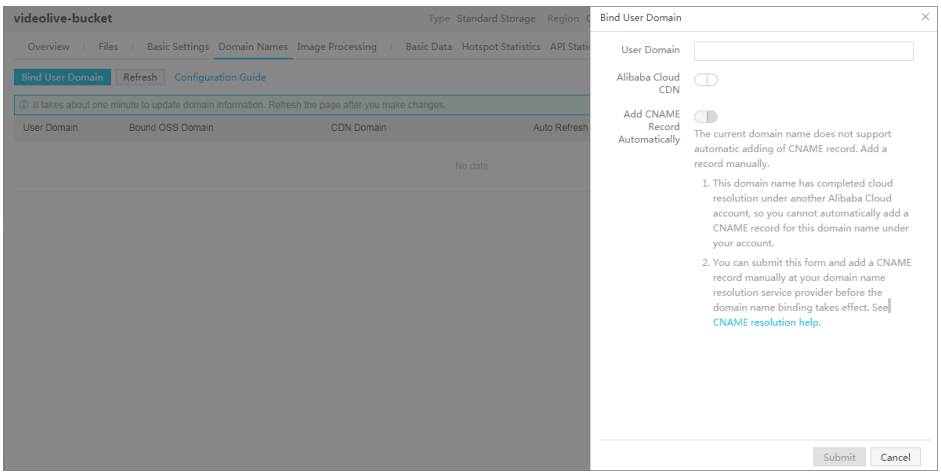
Enter the **Directory Name** and click **OK**.



Configure the CDN domain name.

Recordings are stored in OSS. You can configure a CDN domain name and use CDN acceleration to view the recordings. CDN delivers videos stored in your OSS to nodes throughout China. Users can access the nearest CDN node to read files without accessing the original files in OSS and consuming OSS Internet traffic. By using CDN, the access rate and experience of your edge users are improved, and the CDN Internet traffic cost is only 50% of the OSS Internet traffic cost. This efficiently reduces the network fees for your applications.

Click **Domain Names** > **Bind User Domain** to configure CDN domain name.



You do not need to configure a CDN domain name if you only store your videos.

Note: The CDN domain name and the live video domain name cannot be the same. Set different domain names.

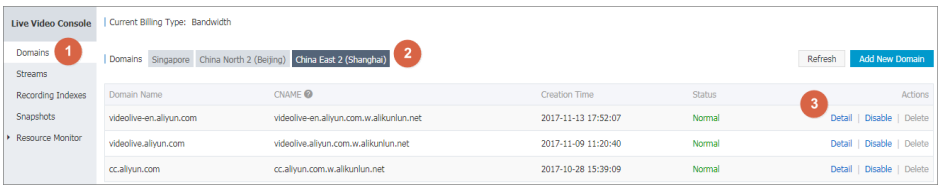
Step 2. Create a live recording

Log on to the ApsaraVideo Live console.

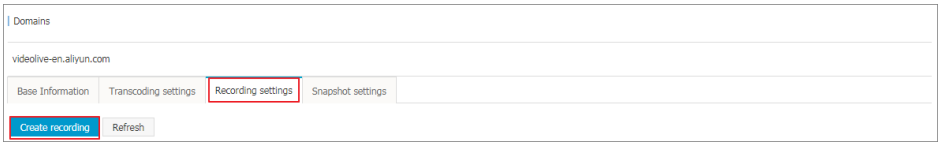
Click **Domains**.

Select the region.

Select the expected domain name and click **Detail** at the right side.

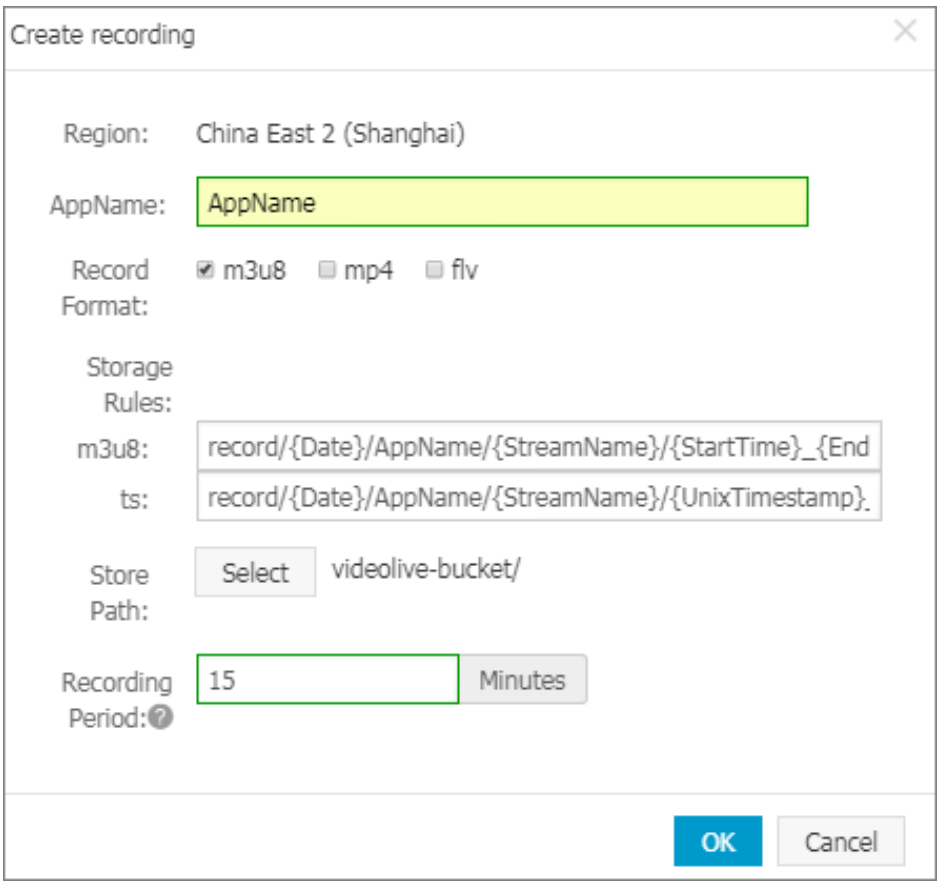


Click **Recording settings** and click **Create Recording**.



Configure recording settings.

In the recording settings window, enter theAppNamefor which to enable the recording function.



Note: The recording AppName and the AppName in the stream push address must be the same. For example, if the 'AppName' in your stream push address is set to 'videolive-en', the recording 'AppName' must also be 'videolive-en'. For more information about the settings, see Live streaming.

Record Format.

Three record formats are supported: flv, mp4, and m3u8. Here, m3u8 format simultaneously outputs ts fragment addresses.

Storage Rules.

The default storage path for recordings is:

m3u8:record/{Date}/{AppName}/{StreamName}/{StartTime}_{EndTime}

ts:record/{Date}/{AppName}/{StreamName}/{UnixTimestamp}_{Sequence}

mp4:record/{Date}/{AppName}/{StreamName}/{StartTime}_{EndTime}

flv:record/{Date}/{AppName}/{StreamName}/{StartTime}_{EndTime}

In the example screenshot, the app name is AppName, so the m3u8 and ts recording files are stored in the following path:

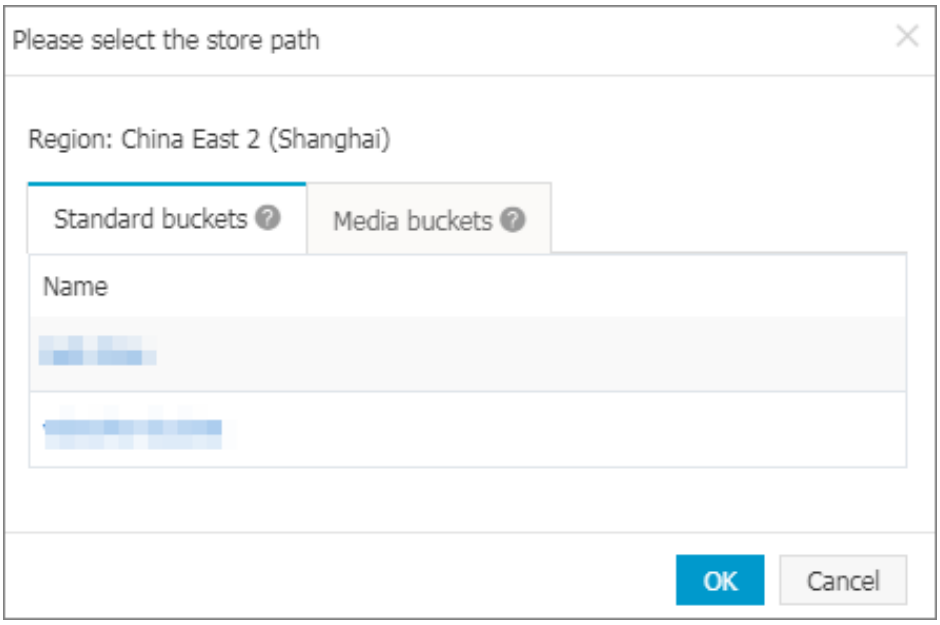
m3u8:record/{Date}/APPName/{StreamName}/{StartTime}_{EndTime}

ts:record/{Date}/APPName/{StreamName}/{UnixTimestamp}_{Sequence}

If the default recording file storage path cannot meet your requirements, you can change it.

Set the **Store Path**.

Click **Select**, then click **Standard buckets** in the dialogue box and select the expected bucket name.



Recording Period.

The system supports recording period from 15 to 360 minutes (6 hours). After a recording exceeds six hours, a new file is generated according to the recording naming rules. However, the default length of ts fragments is 30 seconds.

Recording file names.

Here, { } represents a variable. The flv, mp4, and m3u8 formats support names in the following format: {AppName}, {StreamName}, {Date}, {Sequence}, {StartTime} and {EndTime}. Except for {StartTime} and {EndTime} the other variables can be retained or deleted as needed. TS recording files supports names in the format: {AppName}, {StreamName}, {Date}, {Sequence}, {UnixTimestamp}. These variables

can be retained or deleted as needed.

{date} classifies recording files into folders by date. The default date format is “YYY-MM-DD”.

{StreamName} automatically fetches the StreamName and uses it as the storage path. You can manually change this as needed. You can customize the {streamName} according to your needs.

{Sequence} is the sequence variable.

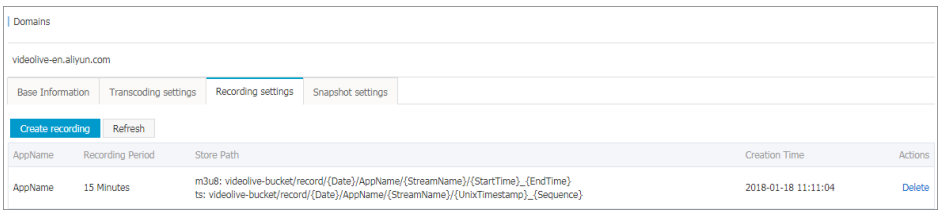
{StartTime} is the recording start time and {EndTime} is the end time. The parameters of flv, mp4, and m3u8 files must have these variables.

{UnixTimestamp}_{Sequence} is the timestamp and sequence variable. In the names of ts files, this variable is automatically specified based on the file generation time and sequence.

To maintain compatibility with the streaming process, the recording system judge a livestream to have ended when an interruption caused by network jitter or another problem persists for **180 seconds** and the stream is not restored. The system independently stores the default recording index files in the format:{AppName}/{StreamName}/{Date}.m3u8(m3u8 format).

Click **OK** to complete recording settings.

In the **Recording Settings** tab, all the recording settings under the selected domain name are listed.



As a result, all the livestreams withAppNameas the AppName under the domain name follow these recording rules. Livestreams that occur before you finish configuring the settings do not trigger recording. Only new livestreams trigger recording (or an existing livestream that is interrupted for more than 180 seconds).

Recording files playback.

You can play back recorded videos on demand.

Note: The AppName in the stream push address and the AppName in the playback address must be consistent with that in the recording template.

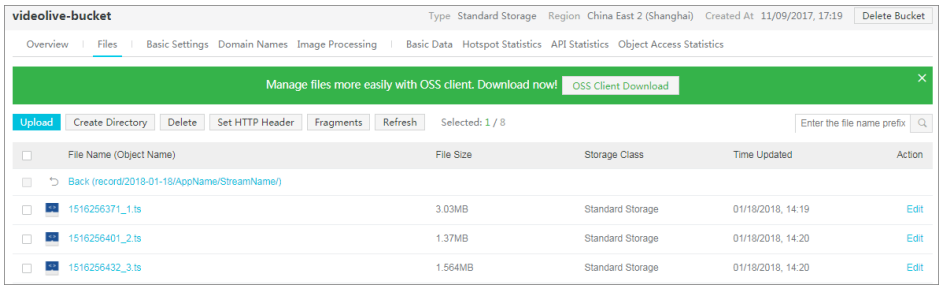
Step 3. View recording files

Recording files are stored in the OSS list. You can use OSS to view, download, and play the recordings. You can also perform list view and playback on the ApsaraVideo Live console.

View recording files on the **OSS console**.

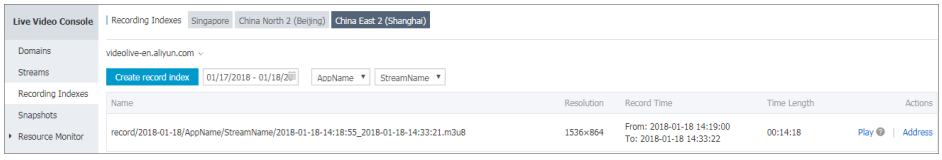
Find the video storage folder on the OSS console. Recording files are stored in OSS in compliance with the aforementioned rules. You can obtain the playback addresses from OSS.

The complete video files are stored in the record/date/AppName/StreamName directory, which is the same as the directory for the TS fragment files. You can click **Object Name** to obtain the address for playback.



View recording files on the **ApsaraVideo Live console**.

You can also use the **Recording Indexes** function on the ApsaraVideo Live console to view the recording files.



Convert live recordings to media files

Live recordings use the original video resolution. You can use Media Processing (MPS) to convert a recorded original-resolution video to multiple media formats. To do this, you must first associate the live recordings with MPS.

> Note: The input bucket for the MPS workflow and the bucket set for the live recordings must be the same. Otherwise, MPS console operations cannot be performed on the live recordings and the videos are not displayed on the MPS console.

Procedure

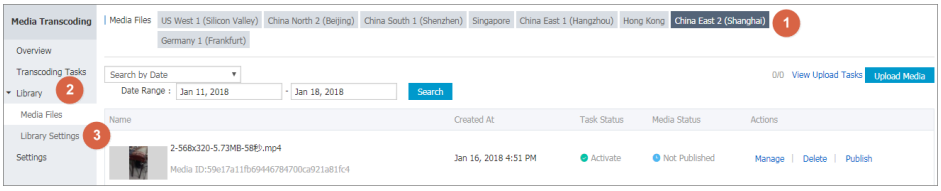
Step 1. Create a workflow

Before creating an MPS workflow, you must have created a **Media Bucket** on the MPS console. For details, see Library Settings. Then, create a workflow on the MPS console. Finally, select a workflow region. Only live videos in the **China East 2 (Shanghai)** and **China North 2 (Beijing)** regions are currently supported. The region in the **Library Settings** must be consistent with the region in the ApsaraVideo Live.

Log on to the MPS console.

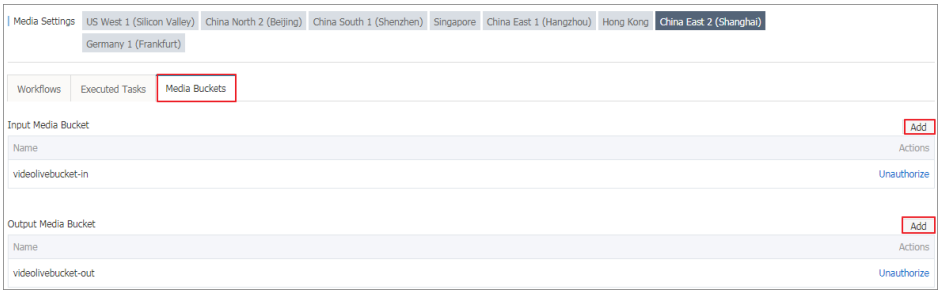
Select the region.

Click **Library** > **Library Settings**.



Click **Media Buckets**.

Click **Add** and set the **Input Media Bucket** and **Output Media Bucket**.



Note:

- To use MPS , you must create an **Input Media Bucket** and **Output Media Bucket**. The **Input Media Bucket** stores the original video files and the **Output Media Bucket** stores the transcoded video files. After the workflow is created, it obtains the original video files automatically from the **Input Media Bucket** and performs the corresponding transcoding operations.
- Only **Input Media Bucket** in **China East 2** are currently supported. When creating a media bucket, select **China East 2**.

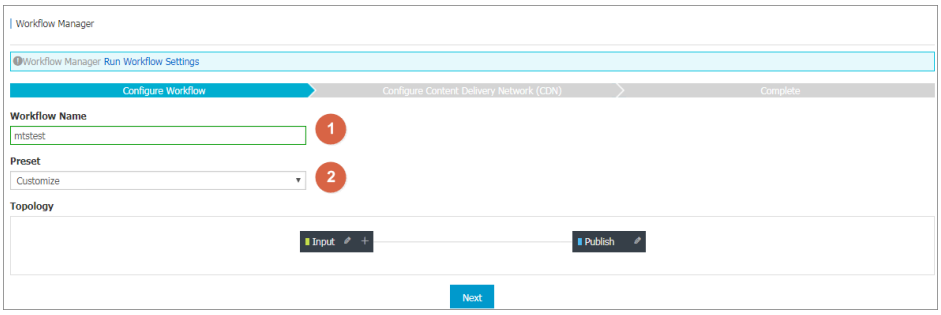
Create a workflow.

In **Workflows**, click **Create Workflow** to go to the **Workflow Manager** page.

Enter the workflow name.

Set the **Preset**.

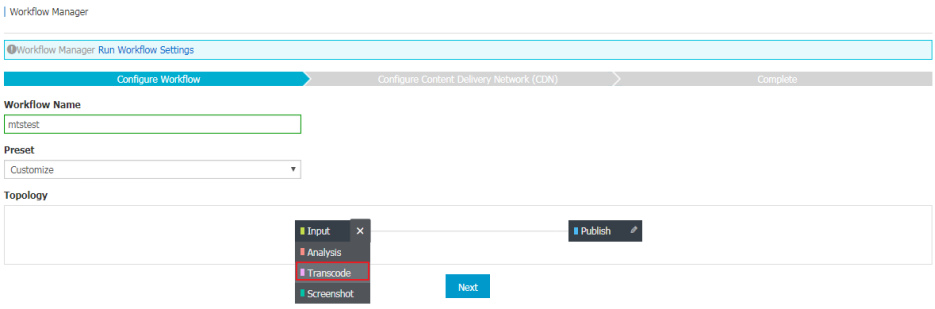
Select **Customize** as the **Preset**. The **Preset** is the output scheme after transcoding and can be configured as needed.



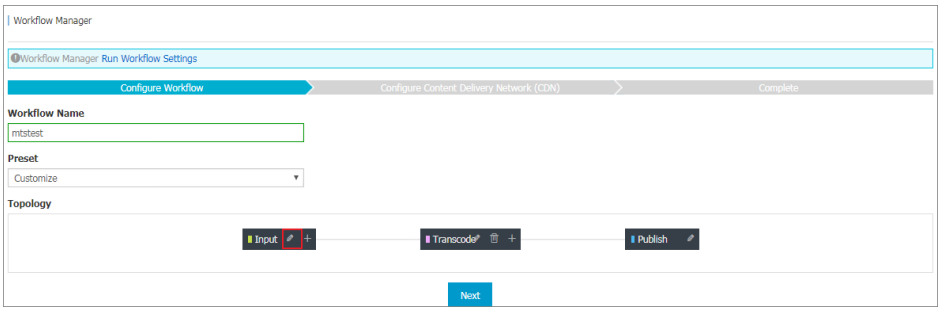
Set the workflow parameters.

The following describes the simplest operations to display quick experience of the live recording to video-on-demand process. For details, see **Workflow settings**.

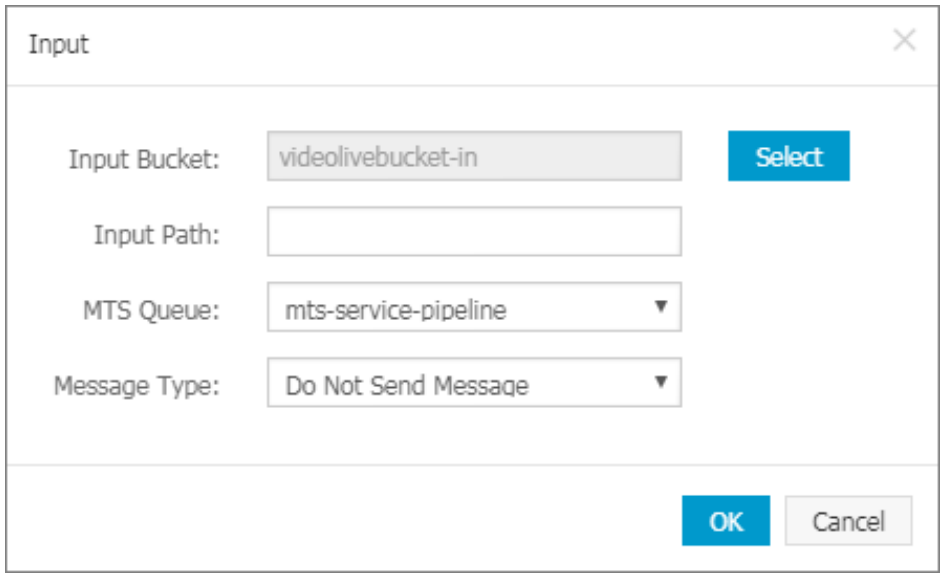
In the **Topology** field, add the **Transcode** node in the **Input** drop-down list.



Click the editting icon at the right side of the **Input** node.

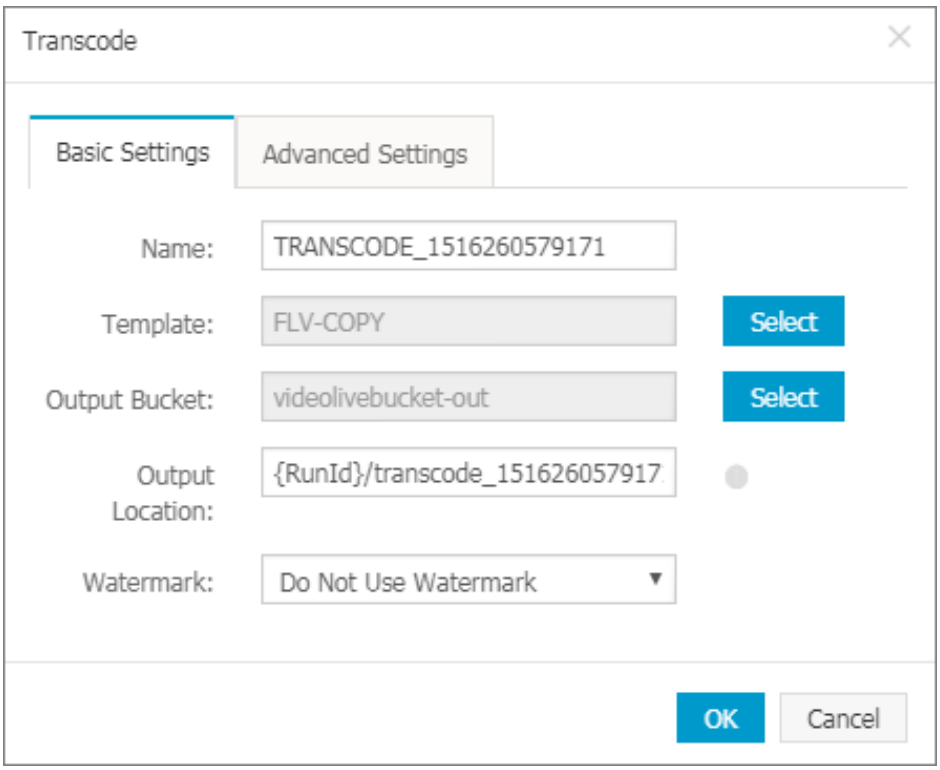


Select the **Input Bucket** you created.

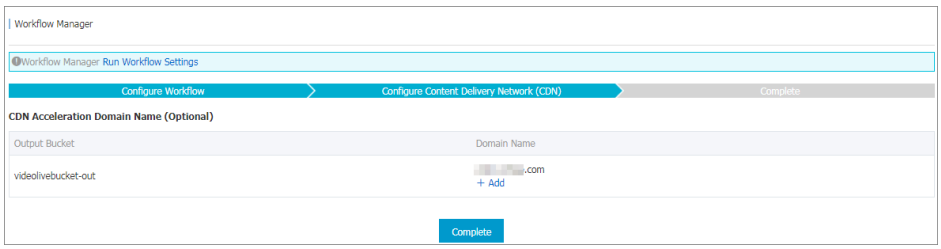


Set **Transcode** node.

Click the editting icon at the right side of the **Transcode** node, select the **Template** and **Output Bucket** and click **OK**.

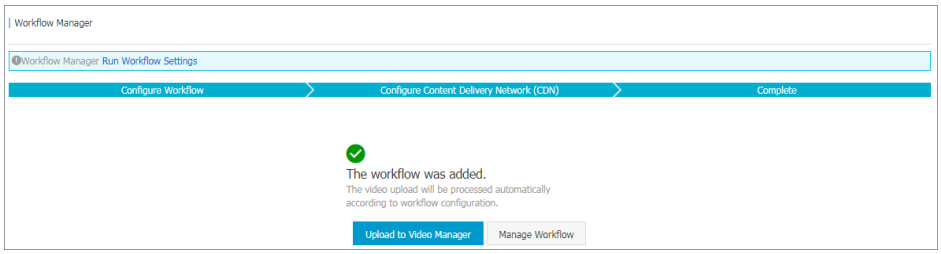


Click **Next** and enter the CDN domain name.



Note: The CDN domain name must complete an ICP filing and CNAME resolution.

The workflow is added.



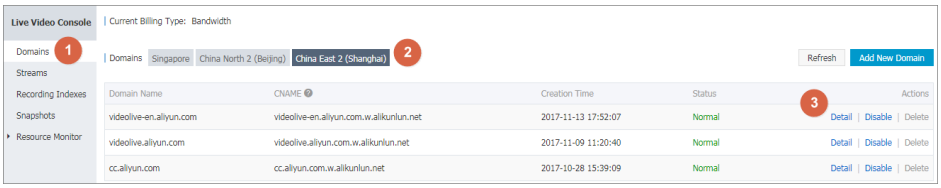
Step 2. Create a live recording

Log on to the ApsaraVideo Live console.

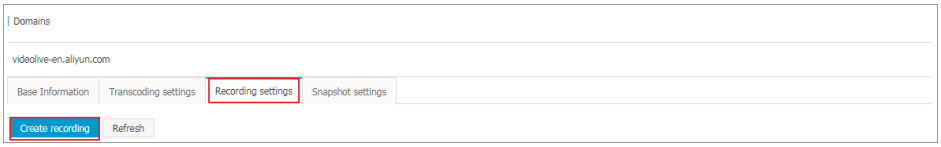
Click **Domains**.

Select the region.

Select the expected domain name and click **Detail** at the right side.

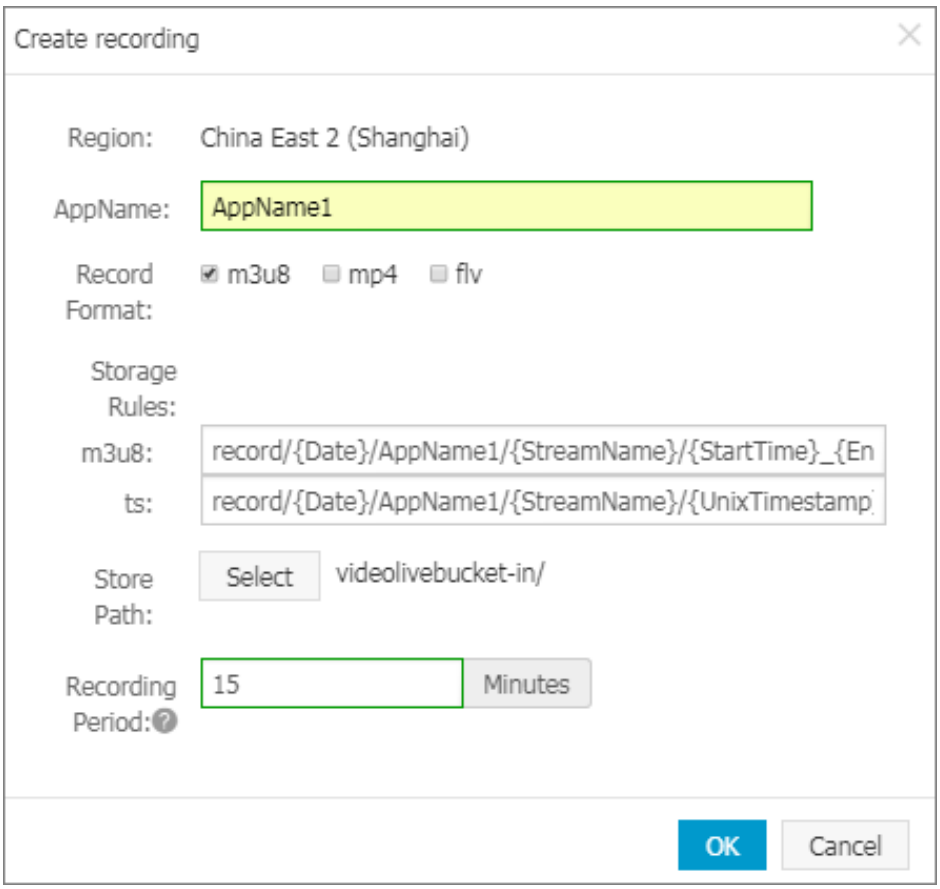


Click **Recording settings** and click **Create recording**.



Add recording settings.

On the **Create recording** page, enter theAppNamefor which to enable the recording function.



Note: The recordingAppNameand theAppNamein the stream push address must be the same. For example, if theAppNamein your stream push address is set tovideolive-en, the recordingAppNamemust also be videolive-en. For details, see Live streaming.

Record format.

Three Record formats are supported: flv, mp4, and m3u8. Here, m3u8 format simultaneously outputs ts fragment addresses.

Storage Rules.

The default storage path for recordings is:

m3u8:record/{Date}/{AppName}/{StreamName}/{StartTime}_{EndTime}

ts:record/{Date}/{AppName}/{StreamName}/{UnixTimestamp}_{Sequence}

mp4:record/{Date}/{AppName}/{StreamName}/{StartTime}_{EndTime}

flv:record/{Date}/{AppName}/{StreamName}/{StartTime}_{EndTime}

In the example screenshot, the AppName is AppName, so the m3u8 and ts recording files are stored in the following path:

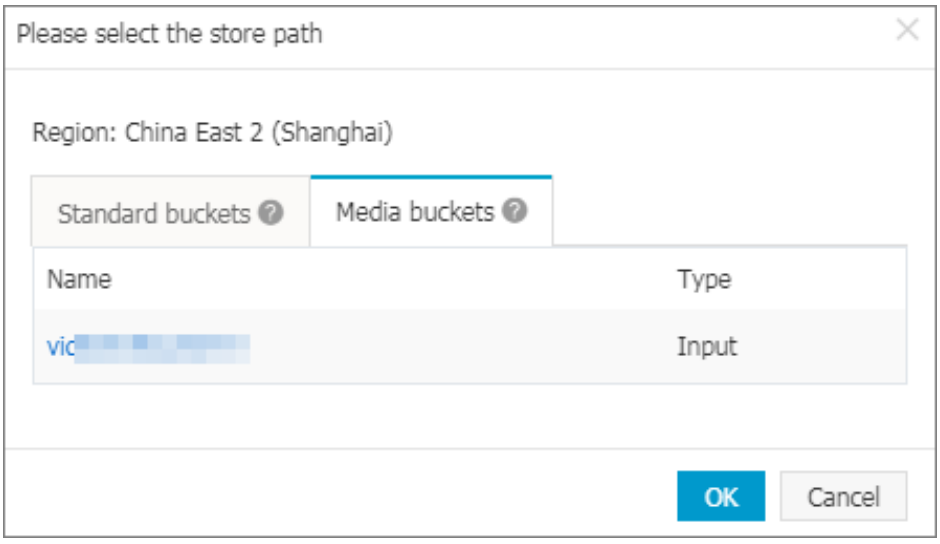
m3u8:record/{Date}/APPName1/{StreamName}/{StartTime}_{EndTime}

ts:record/{Date}/APPName1/{StreamName}/{UnixTimestamp}_{Sequence}

If the default recording file storage path cannot meet your requirements, you can change it.

Set the **Store Path**.

Click **Select**, and in the dialogue box, click **media Buckets** and select the expected bucket name.



Note: Media buckets are primarily used to store videos for secondary transcoding. The live recordings can perform the transcoding workflow operation only when the bucket for storing the live recordings and the media bucket are the same input media bucket, If you haven’ t activated the MPS and created a media bucket, this tag is not displayed.

Recording Period.

The system supports recording durations from 15 to 360 minutes (6 hours). After a recording exceeds six hours, a new file is generated according to the recording naming rules. However, the default length of ts fragments is 30 seconds.

Recording file names.

Here, { } represents a variable. The flv, mp4, and m3u8 formats support names in

the following format: {AppName}, {StreamName}, {Date}, {Sequence}, {StartTime}, {EndTime}.Except for {StartTime} and {EndTime} the other variables can be retained or deleted as needed.TS recording files supports names in the format: {AppName}, {StreamName}, {Date}, {Sequence}, {UnixTimestamp}. These variables can be retained or deleted as needed.

{date} classifies recording files into folders by date. The default date format is “YYY-MM-DD”.

{StreamName} automatically fetches the StreamName and uses it as the storage path. You can manually change this as needed.You can customize the {streamName} according to your needs.

{Sequence} is the sequence variable.

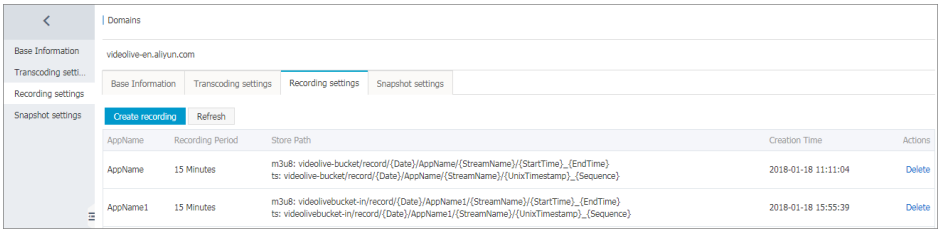
{StartTime} is the recording start time and {EndTime} is the end time. The parameters of flv, mp4, and m3u8 files must have these variables.

{UnixTimestamp}_{Sequence} is the timestamp and sequence variable.In the names of ts files, this variable is automatically specified based on the file generation time and sequence.

To maintain compatibility with the livestream push process, the live recording system judge a livestream to have ended when an interruption caused by network jitter or another problem persists for **180 seconds** and the stream is not restored.The system independently stores the default recording index files in the format:{AppName}/{StreamName}/{Date}.m3u8(m3u8 format).

Click **OK** to complete recording settings.

In the **Recording Settings** tab, all the recording settings for the selected domain name are listed.



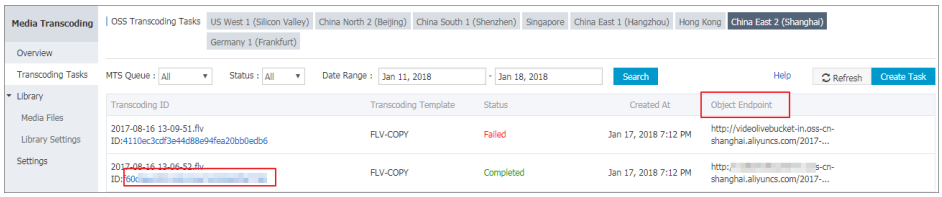
As a result, all the livestreams withAppName1as the AppName under the domain name follow these recording rules. Livestreams that occur before you finish configuring the settings do not trigger recording. Only new livestreams trigger recording (or an existing

livestream that is interrupted for more than 180 seconds).

Step 3. Recording playback

After MTS transcoding, live recordings are stored in MTS. You can use MTS to play back the videos.

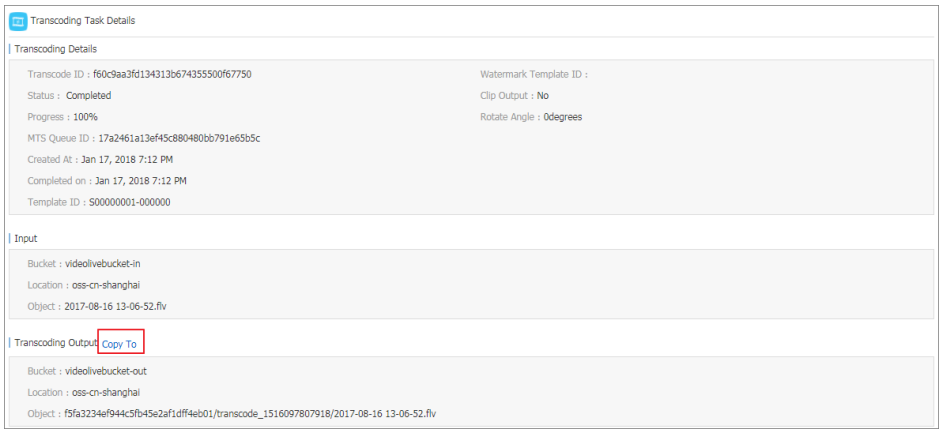
You can obtain the playback address and media ID of a single video file in **Media Files** on the MPS console, and play back the video.



Note:

The **Transcoding ID** is the ID of the on-demand video created from the recording file.

The **Object Endpoint** is the original file address of the live recording.



Note: Click **Copy To** to copy the recording file playback address.

To obtain the playback addresses of transcoded videos in batches, if you do not know the media IDs, you can use the media input addresses (the addresses used to store the original recording files) to query the media information using the API QueryMediaListByURL. For details, see Media ID query example.

Note: Encrypted videos must be played using media IDs to ensure their security. Use Flash

Player (HTML 5 does not support playback of encrypted videos) to play encrypted videos on web terminals. For details, see Introduction to media playback.

Recording callback

Function overview

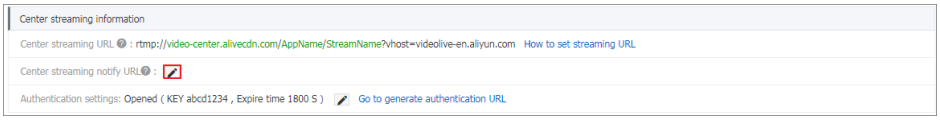
The system calls back the new status of the live recording stream and informs the user of related results and the recording status after recording is completed.

Notes

HTTP/HTTPS URL configurations are supported. The POST request is sent to the user server. The message body is in JSON format. Real-time feedback of the recording result and status information is provided to the user. The user server returns results in the form of 200 responses to the interface. The URL does not need to be identified, but must be accessed properly. If the access times out, you can retry up to five times. The interval between retries is a random value between 100ms and 10s.

Configuration guide

The recording callback address can be manually configured on the console.



Example

User callback address: http:// 1.1.1.1/notify/record, the returned body content is as follows:

File generation event callback example

This indicates that the target recording file was generated.

```
{
"domain": "live.aliyunlive.com",
"app": "live",
```

```
"stream": "hello",
"uri": "live/hello/0_2017-03-08-23:09:46_2017-03-08-23:10:40.flv",
"duration": 69.403,
"start_time": 1488985786,
"stop_time": 1488985840
}
```

Here,domain,app,streamare the recording domain name, application name, and stream name respectively.uriis the path of the target recording file in the user recording OSS bucket.duration,start_time,stop_timeare the duration, start time, and end time of the target recording file respectively.

Example of recording status callback, generated when NeedStatusNotify=true

- Recording start event callback, indicating the recording has started successfully.

```
{
"domain": "live.aliyunlive.com",
"app": "live",
"stream": "hello",
"event": "record_started"
}
```

Here, domain,app, andstreamare the recording domain name, application name and stream name respectively.eventis the event name and it can berecord_started/record_paused/record_resumed.

- Recording pause event callback, indicating the recording is successfully paused

```
{
"domain": "live.aliyunlive.com",
"app": "gs_app",
"stream": "gs_stream",
"event": "record_paused"
}
```

- Recording error callback, indicating an error occurred during recording

```
{
"domain": "gs_domain",
"app": "gs_app",
"stream": "gs_stream",
"event": "record_error"

}
```

View live recordings

You can view recording files in the console' s recording index manager.

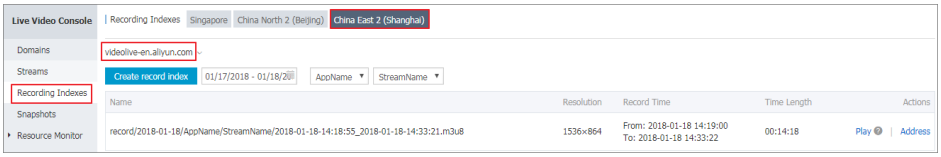
Log on to the ApsaraVideo Live console.

Click **Recording Indexes**.

Select the expected region.

Select the expected domain name.

Select the recording time range, AppName and StreamName to view recordings.



Note: You can click **Create Record Index** to edit existing recording files to create new files. Click **Address** to view the recording playback address. Click **Play** to play back the video recordings.

Create record index

When recording live videos, you can view the recorded content in the recording index area, or perform secondary edits on the recorded videos. After editing the video, a new m3u8 file is generated in the OSS system.

Procedure

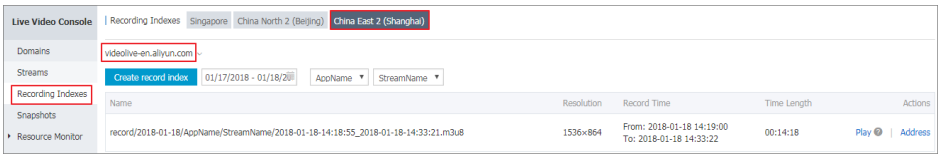
Log on to the ApsaraVideo Live console.

Click **Recording Indexes** in the left-side navigation pane.

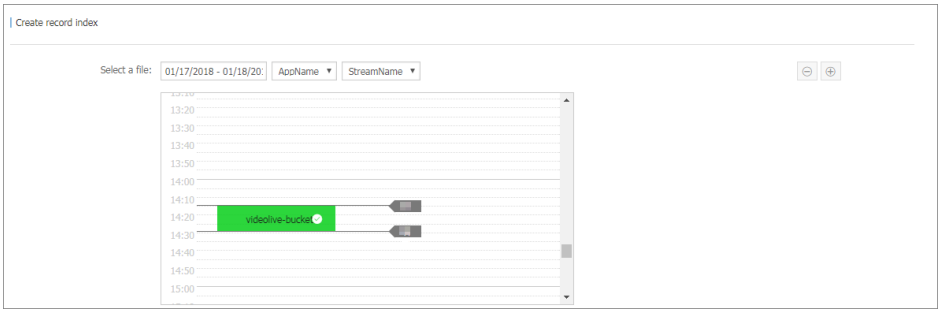
Select the expected region.

Select the expected domain name.

Click **Create record index**.



On the **Create record index** page, select the period of the recording file, the AppName and the StreamName.



Note:

- When broadcasting a livestream, if it is interrupted for more than **180 seconds**, a new recording file is automatically generated and displayed in the timeline. You can splice the recording fragments together.
- videolive-bucket is the name of the bucket. For details on media buckets setting, see Library settings.
- In the green area, you can set the start time and end time to determine the video data that needs to be spliced or clipped. All the live recording fragments in this area can be selected for splicing.

Set the **Starting time** and **End time** to splice or clip the selected recording. You can further edit the spliced or clipped video.

Name the new file in **ObjectName** and click **OK**.

Note: The stored m3u8 file can be found in the OSS storage directory indicated by the storage location.

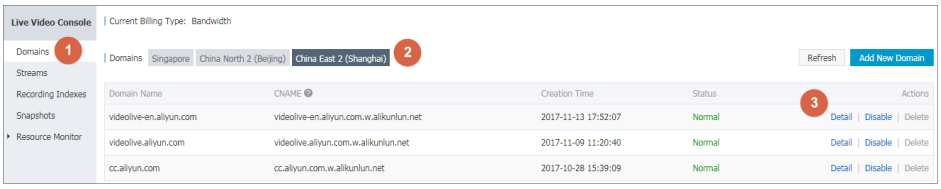
View recording playback address

Directly obtain playback information

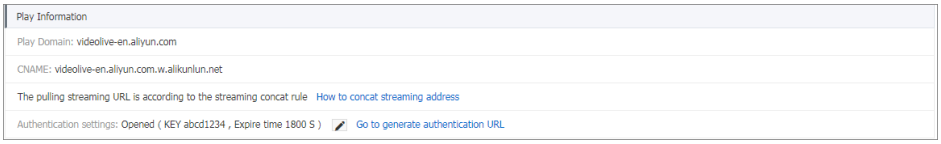
Log on to the AppsaraVideo Live console.

Select the expected **Region**.

Select the expected domain name and click **Detail** at the right side.



In **Base Information** > **Play Information**, obtain the **Playback Information**.



Note: The authentication is set at the domain name level. If the authentication status is **Opened**, all the streaming addresses under the domain name must perform authentication operation. Meanwhile, the playback address corresponding to the streaming URL must complete authentication operation. Use the authenticated adderss for playback operation.

Preview at the webpage background

Use OBS for streaming by adopting an authenticated URL, and go to the **ApsaraVideo Live**

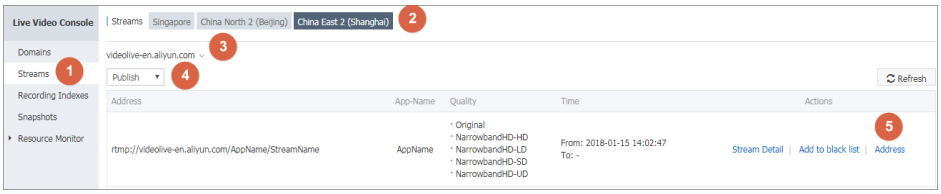
console > **Streams**.

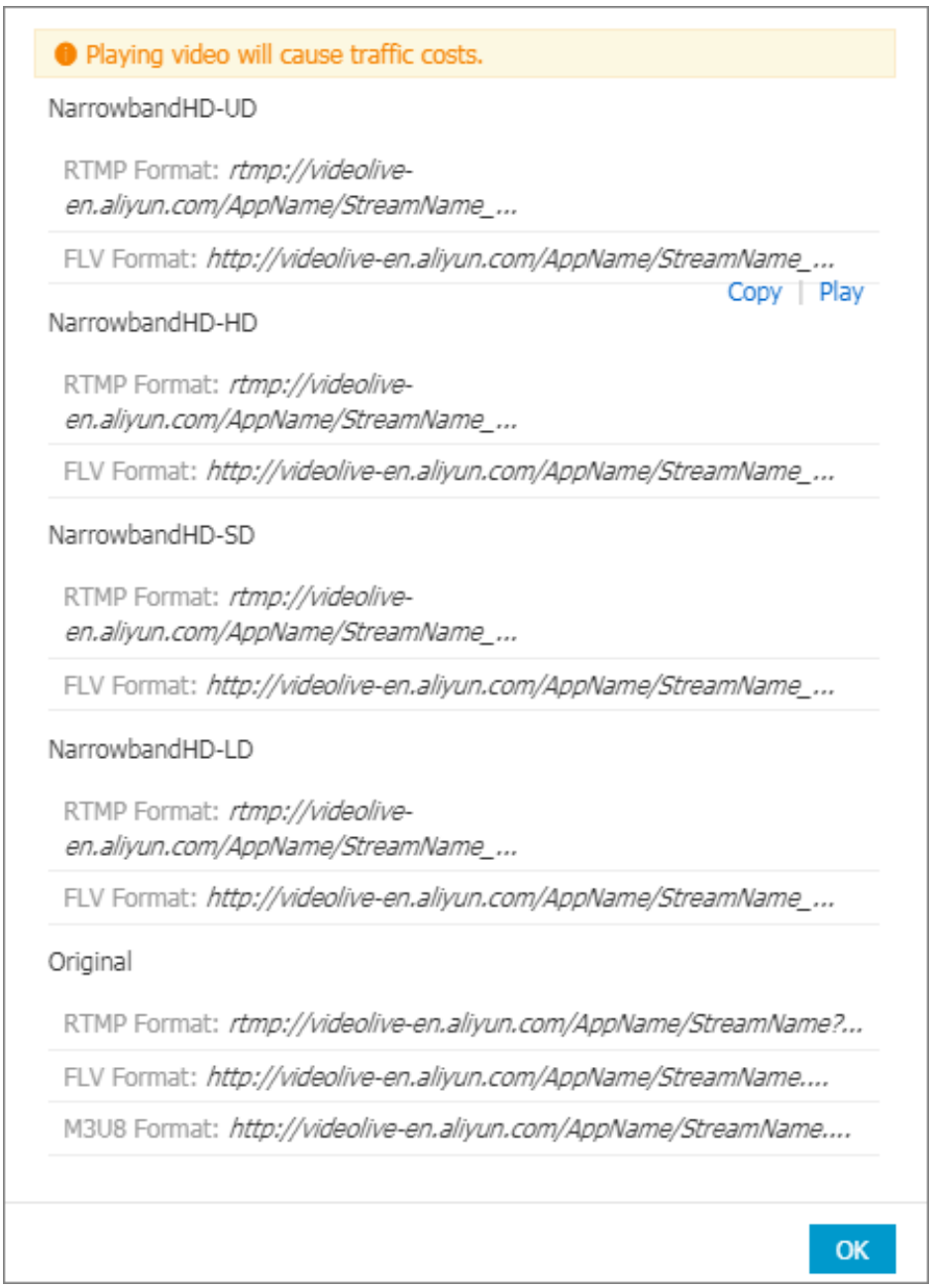
Select the expected region.

Select the expected domain name.

Select the expected stream status.

Select the expected streaming address, and click **Address** at the right side to view the playback address and preview the video.





Play back live recordings

After recording a video, you can directly preview the video in the webpage background, or preview it using VLC.

Direct webpage background preview

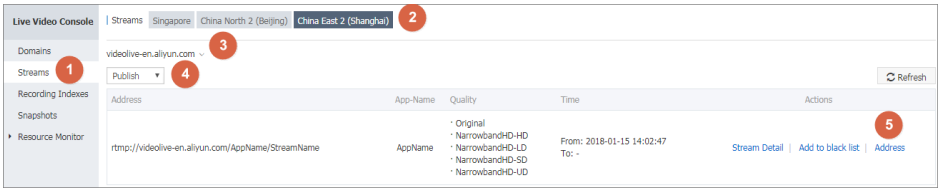
Use OBS for streaming by adopting an authenticated URL, and go to the **ApsaraVideo Live console** > **Streams**.

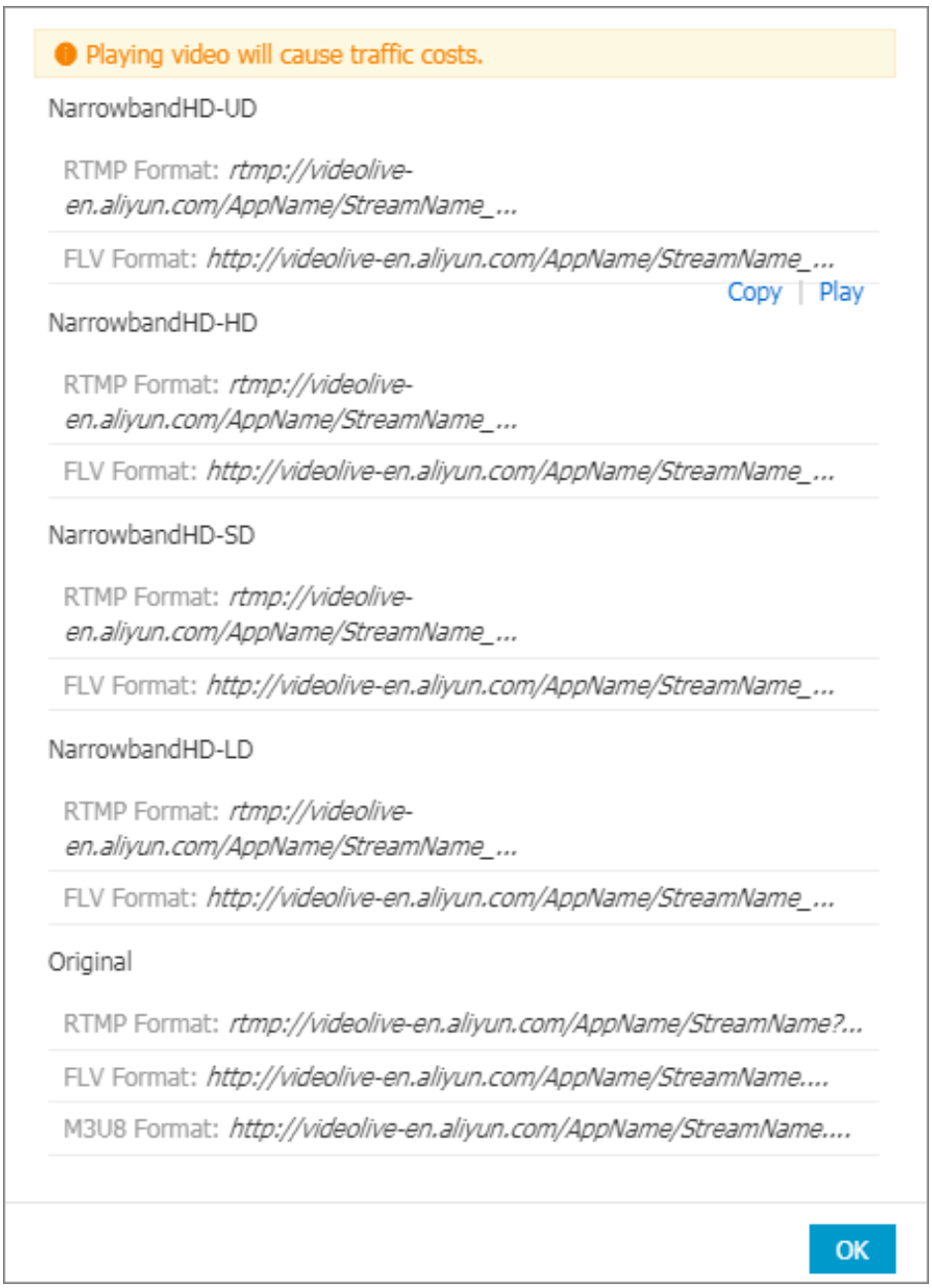
Select the expected region.

Select the expected domain name.

Select the expected stream status.

Selected the expected streaming address, and click **Address** at the right side to view the playback address and preview the video.





VLC preview

Download VLC. After installing it, you do not need to modify the settings. Click **Media** > **Open Network Streaming**, enter the livestream address, and click **Play** to play the video.

Snapshot management

Create a live snapshot

Live video snapshot service supports taking snapshots of the live video being played at a set interval and saving the snapshots as .jpg files to a specified location in OSS.

Under a live video CDN domain, the live snapshot settings are differentiated by the AppName of the live video streaming. That is, streams under the same AppName all perform snapshot operations following the settings of this AppName. The AppName can be set to *, indicating that all the streams under the live video CDN domain follow the snapshot settings.

To conveniently view the snapshots, set a bucket for storage first.

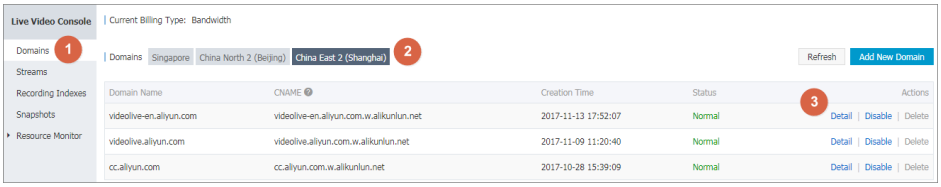
Procedure

Log on to the ApsaraVideo Live console.

Click **Domains**.

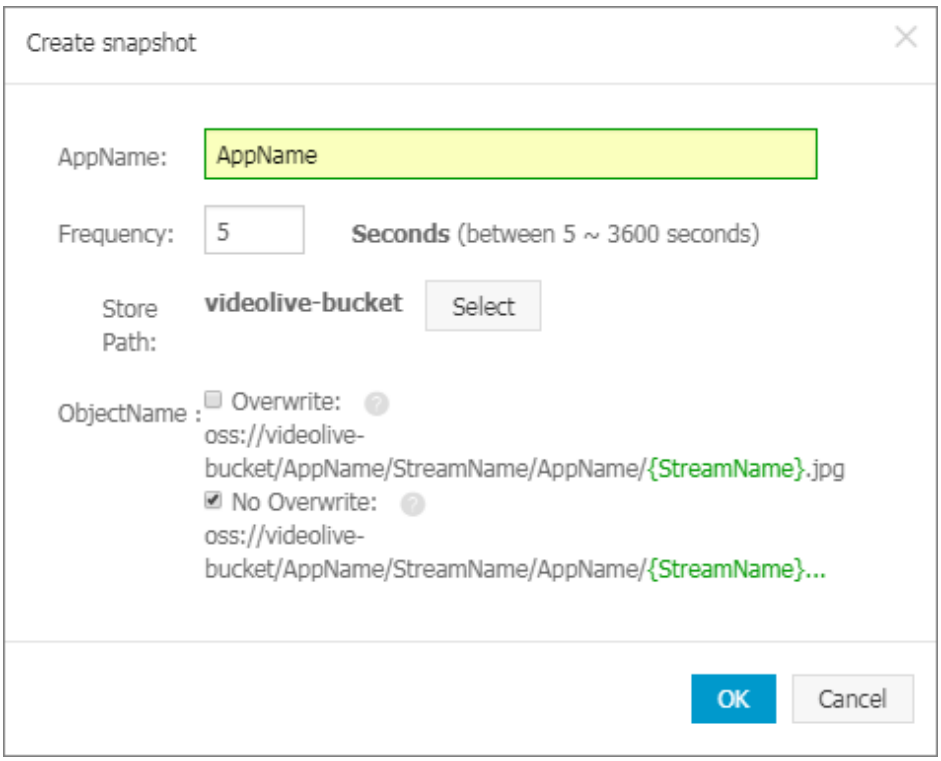
Select the region.

Select the domain name and click **Detail** from the **Actions** column.



Click **Snapshot settings**, and click **Create snapshot**.

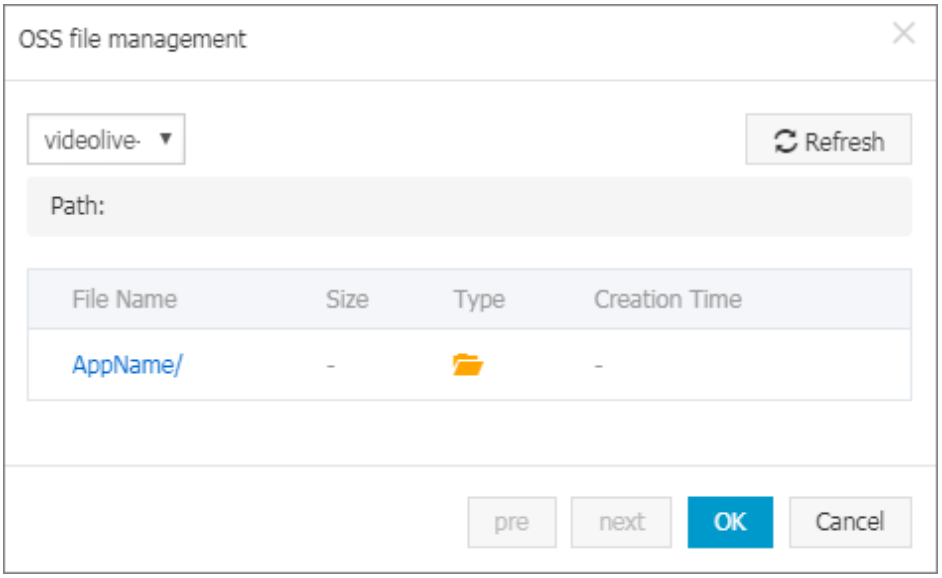
Set the snapshot parameters and click **OK**.



Enter the **AppName** for which the snapshot function must be enabled.

Enter the frequency. It is the snapshot interval. It can be between 5 and 3,600 seconds.

Select the bucket in which the snapshot files are stored, and click **OK**.



Note: The bucket and the current domain name must be in the same region. For example, if the current domain name is located in **China East 2**

(Shanghai), the bucket must also be located in China East 2 (Shanghai). If no bucket list is available in the panel, check that the OSS bucket and the domain name are in the same region.

Select a snapshot type,OverwriteorNo Overwrite. Multiple types can be selected.

Overwrite: The video snapshots are taken in sequence based on the set interval, and the new snapshot can overwrite the previous one.

No Overwrite: The video snapshots are taken in sequence based on the set interval, and the new snapshots are stored in OSS in the order of N+1 (N ≥ 0).

All snapshot settings under the domain name are listed on the Snapshot settings tab. For example, the snapshots of all the live video streams with AppName as the app name under the domain name are captured and exported according to this rule.

Note: The modified snapshot settings are applied to the next live video streaming.

View the live snapshots

Procedure

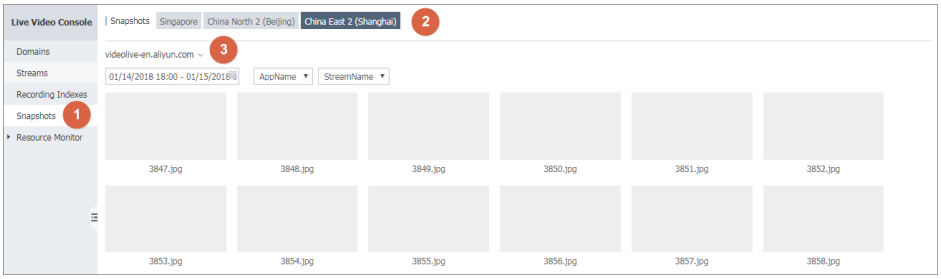
Log on to the ApsaraVideo Live console.

Click Snapshots in the left-side navigation pane.

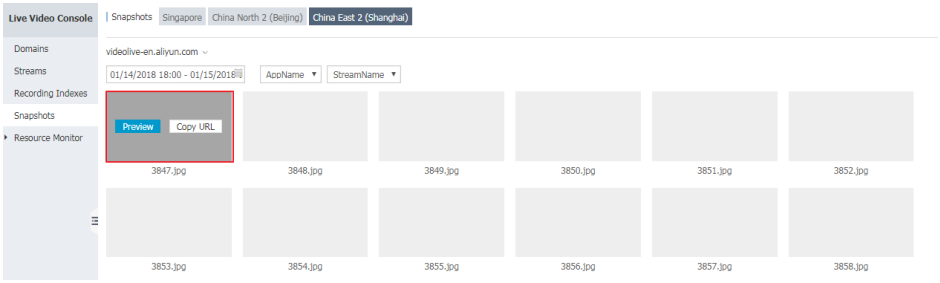
Select the region.

Select the domain name.

Select the expected time period, and select the AppName and StreamName from the drop-down list. The snapshots list is displayed on the basis of your selection.



Hover your cursor over a snapshot in the list. Buttons to enlarge the image and copy the URL are displayed. You can perform the operations as required.



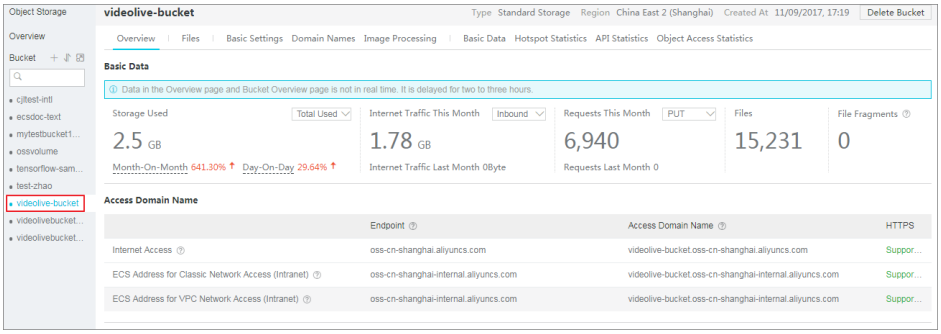
Delete snapshots

You cannot delete the snapshots directly in the ApsaraVideo Live console. Instead, you must perform the deletion operation in the OSS console.

Procedure

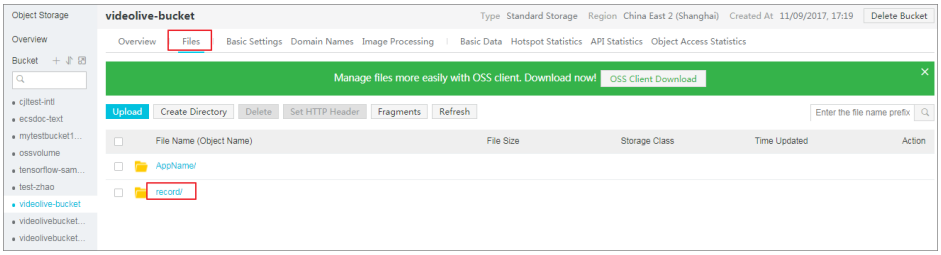
Log on to the OSS console.

On the **Overview** page, select the bucket where the snapshots are stored and click its name.



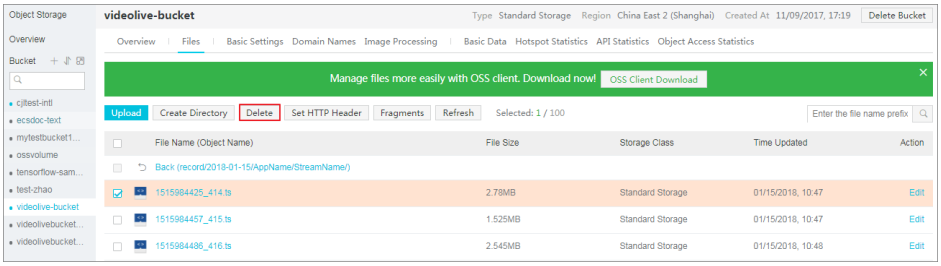
Click **Files**.

Select the folder name.

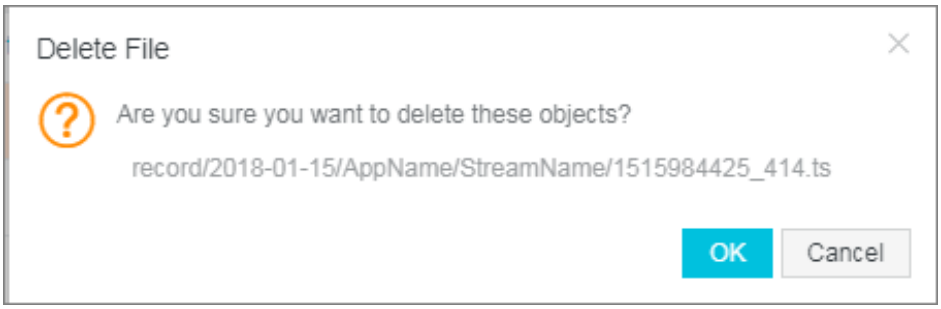


Select the snapshot to be deleted, and click **Delete**.

To delete multiple snapshots at once, select multiple snapshots and click **Delete**.



Click **OK**.



Note: To verify whether the selected snapshot has been deleted, you must return to the **snapshots** page of the ApsaraVideo Live console.

Resource monitoring

Monitoring index

You can view the **traffic bandwidth**, **access overview**, **user access data**, **hot point**, and **security monitor** information on the ApsaraVideo Live console, and select the domain name and time segment to be monitored for each metric. Available metrics that you can monitor are as follows.

Monitoring Metric	Monitoring index
Traffic bandwidth	- **Network bandwidth**: The total traffic and peak bandwidth under the current domain name in the selected acceleration region and ISP within a certain time segment. - **Origin retrieval bandwidth**: The origin retrieval traffic monitored under the current domain name within a certain time segment. - **Daily traffic statistics**: Indexes for which statistics is performed daily, including the traffic, peak bandwidth, peak time point, peak origin retrieval bandwidth, peak origin retrieval bandwidth time point, and number of visits.
Access overview	- **Hit rate**: Traffic hit rate and request hit rate, among which, Traffic hit rate = Number of traffic that is hit/Total traffic; while Request hit rate = Number of requests that are hit/Total requests. - **Access QPS**: The number of accesses per second under the current domain name within a certain time segment. - **HTTP CODE**: The HTTP status code.
User access data	- **PV**: The number of times resource files under the current domain name are accessed within a certain time segment. - **UV**: The number of unique IP addresses that request resources under the current domain name within a certain time segment. - **User region distribution**: Distribution of users in terms of accessed sites, response time, and download speed under the current domain name within a certain time segment. - **Carrier proportions**: Shares of the carrier under the current domain name within a certain time segment.
Hot point	- **Popular URLs**: Popular URLs with a high number of access requests, and popular URLs with heavy traffic. - **Popular referers**: Popular referers with a high number of access requests, and popular referers with heavy traffic. - **File response proportions**: Response of files with a high number of access requests, and response of files with heavy traffic.

Security monitor	- **CC monitoring**: Number of attacks under the current domain name within a certain time segment.

View the monitoring information

You can select **Traffic&Bandwidth**, **Overview**, **User Access Data**, **Hot point** and **Security Monitor** from the **Resource Monitoring** page.

Log on to the **ApsaraVideo Live console**.

Click **Resource Monitor** in the left-side navigation pane.

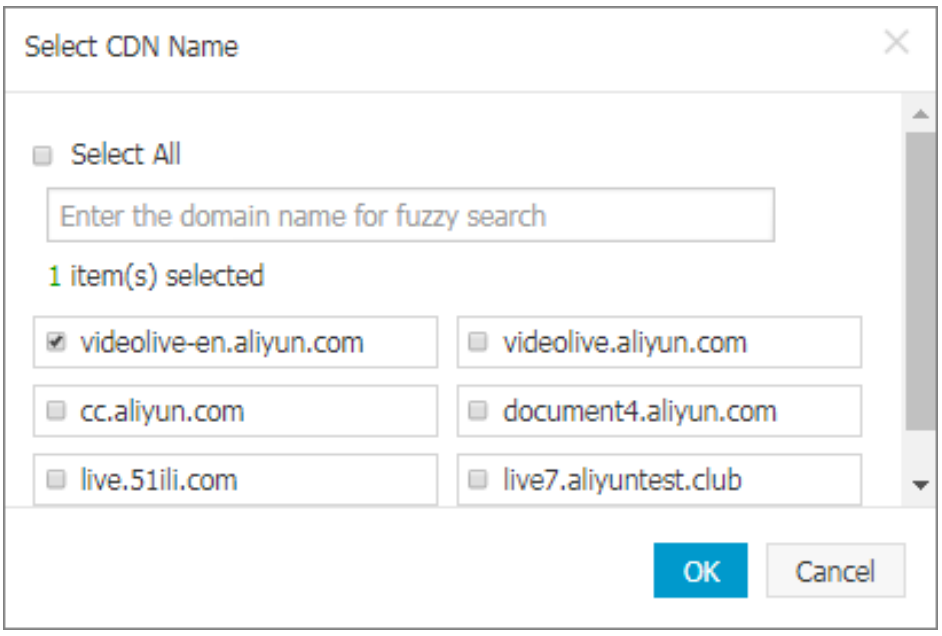
Click **Traffic&Bandwidth**.

Select **Monitored Domain Names**.

Click **Select CDN Name**.

Select the domain names.

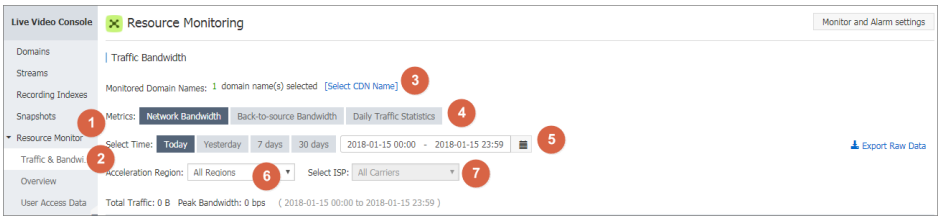
Click **OK**.



Select a monitoring metric.

Select the time period you want to monitor.

Select the acceleration region and ISP.



Create a monitoring alarm

You can access **Monitor and Alarm settings** from **Traffic Bandwidth**, **Access Overview**, **Visitor Data**, **Hot Spot Analysis** or **Security Monitoring** pages.

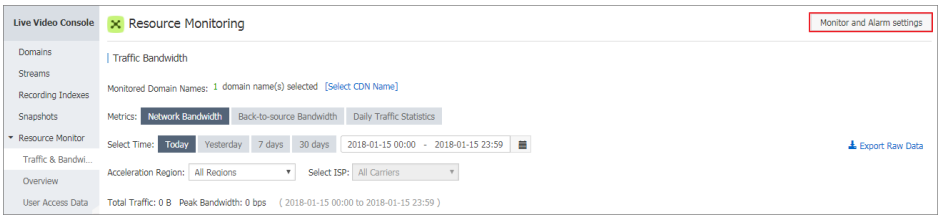
Procedure

Log on to the ApsaraVideo Live console.

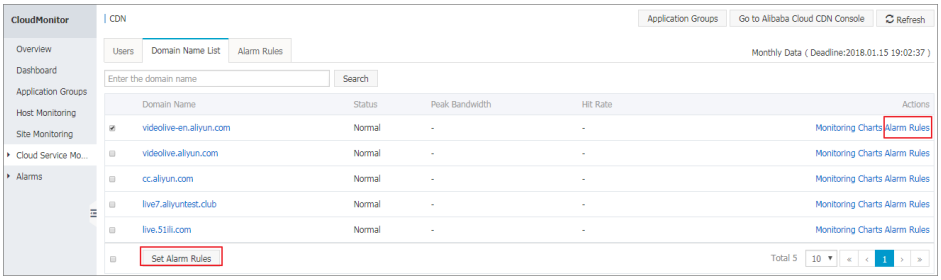
Click **Resource Monitoring** in the left-side navigation pane.

Click **Traffic & Bandwidth**.

Click **Monitor and Alarm settings** in the upper-right corner to go to the CloudMonitor console.

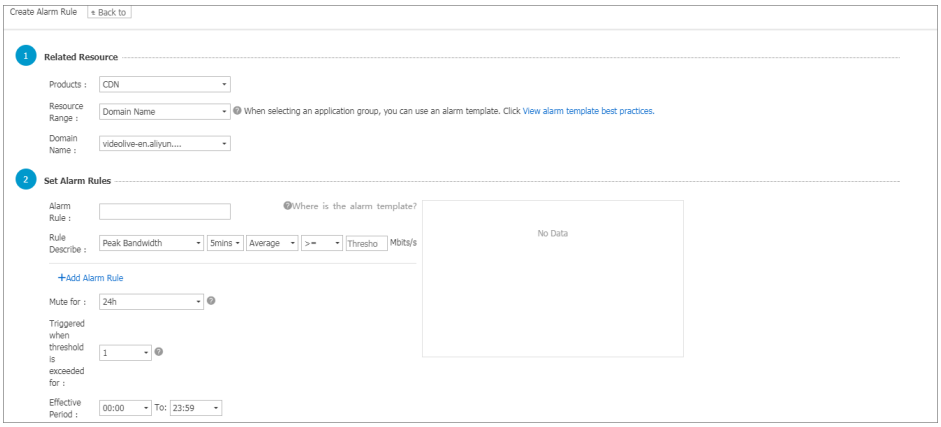


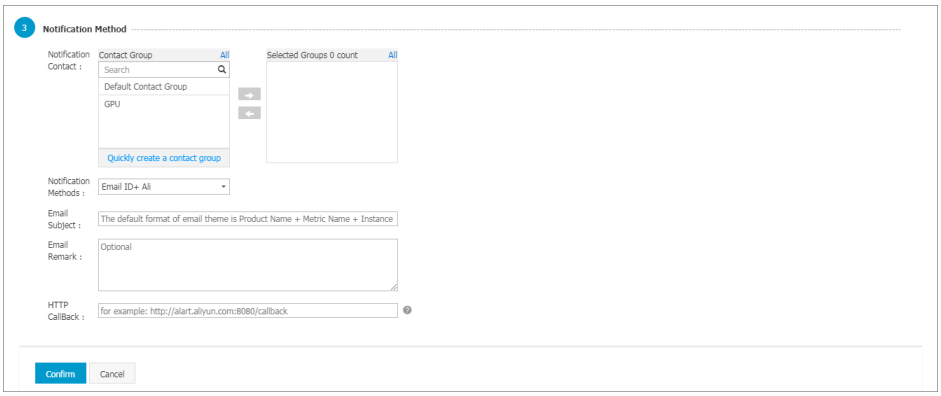
Select the domain name, and click **Alarm Rules** at the right side or **Set alarm rules** at the lower-left corner.



Click **Create Alarm Rule** in the upper-right corner to go to **Create Alarm Rule** page.

For more details, see **Alarm template best practices**.





Set subaccounts to log on to the ApsaraVideo Live console by using RAM set

What is RAM

Through Alibaba Cloud Resource Access Management (RAM), you can provide required permissions

to the subaccounts for the live broadcast in the ApsaraVideo Live console.

One primary account can create multiple subaccounts. By authorizing the subaccounts certain access functions, you can restrict their use of resources and functions for the purpose of unified management. For more inforamtion, see What is RAM.

Subaccount permissions mainly include authorization to use ApsaraVideo Live and OSS and CDN resource objects. We recommend that you plan the resource instances of such services for a subaccount, create authorization policies based on the corresponding authorization templates, and then grant the permissions to the subaccount.

RAM restrictions

RAM users cannot possess resources and they are not billed independently. These users are centrally controlled and billed under your Alibaba Cloud account. You can create separate passwords or keys for each RAM user, but these users do not have any operation permissions by default. RAM provides an access-policy-based authorization to help you grant fine-grained authority to the RAM users.

You must grant the following permissions to your subaccounts to use ApsaraVideo Live console functions:

Live (Required): Grants permission to use ApsaraVideo Live and uses the built-in **AliyunLiveFullAccess** authorization policy;

OSS (Required): Grants permission to use the screenshot storage service, which can be customized as needed;

CDN (Required): Grants permission to play videos, which can be customized as needed.

Authorization operations

Authorization on ApsaraVideo Live

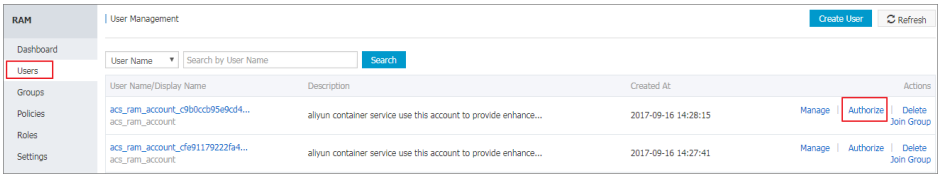
If a subaccount is required to use ApsaraVideo Live, you must grant the subaccount the permission to use ApsaraVideo Live. You can directly use the built-inAliyunLiveFullAccessauthorization policy as follows:

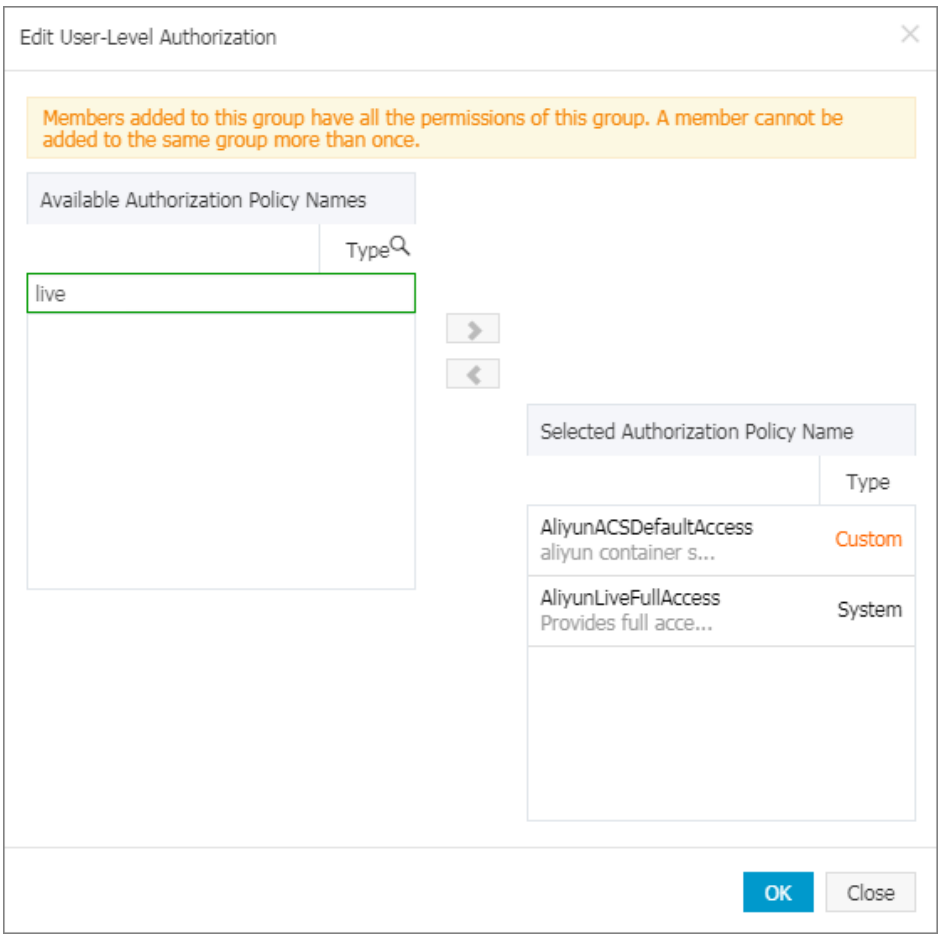
Log on to the RAM console.

Click **Users**.

Select **User Name** and click **Authorize** from the **Actions** column to grant

theAliyunLiveFullAccesspermission to the specified subaccount.





Description of custom authorization policy creation

You can customize authorization policies and assign them to specified subaccounts as follows:

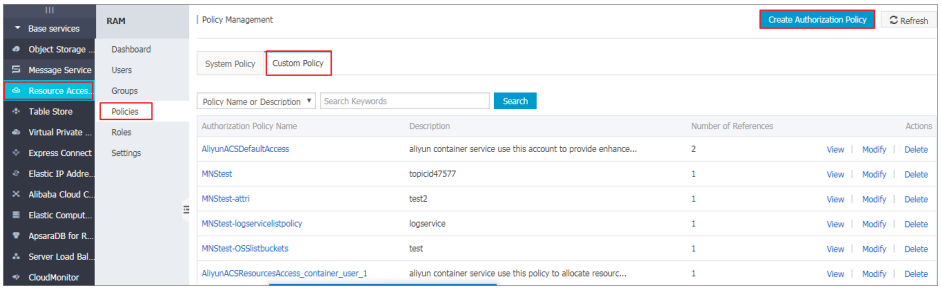
Log on to the **RAM console**.

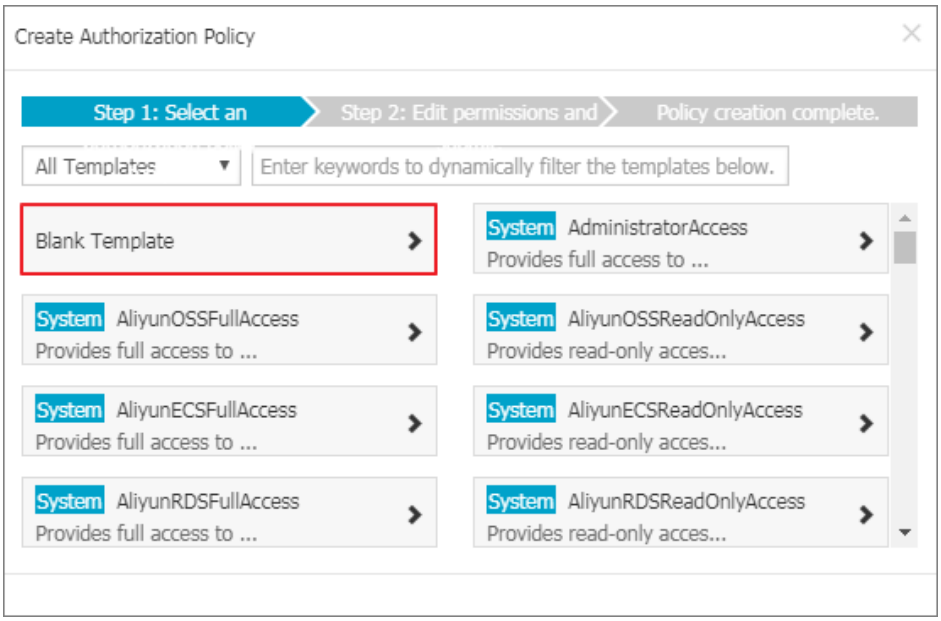
Click **Policies**.

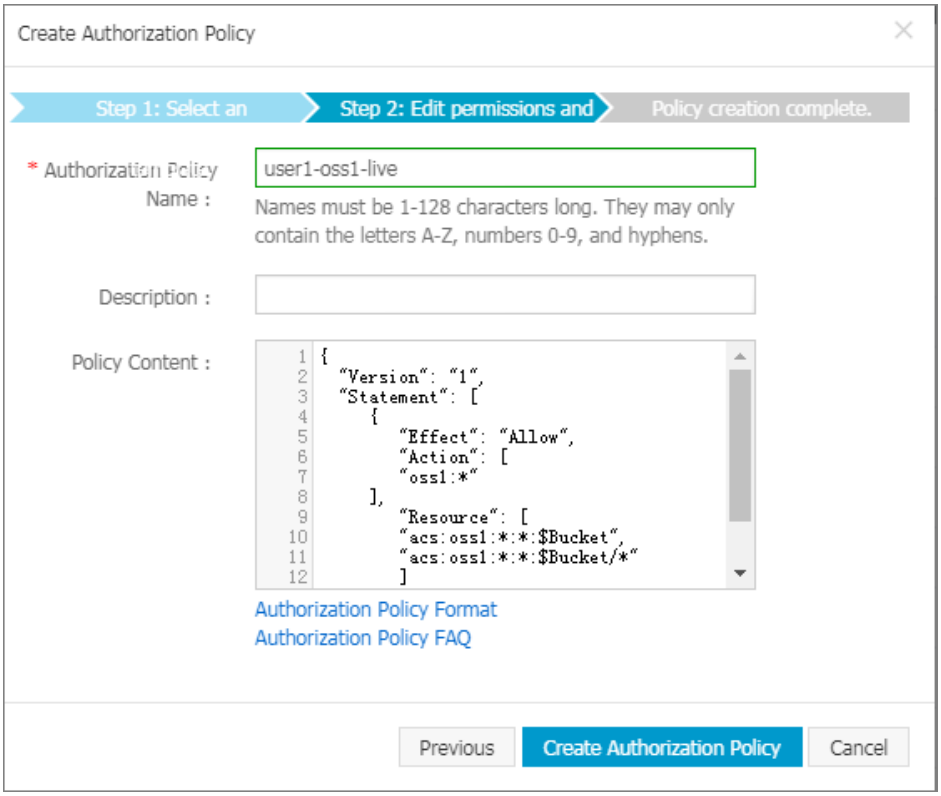
Click **Custom Policy** .

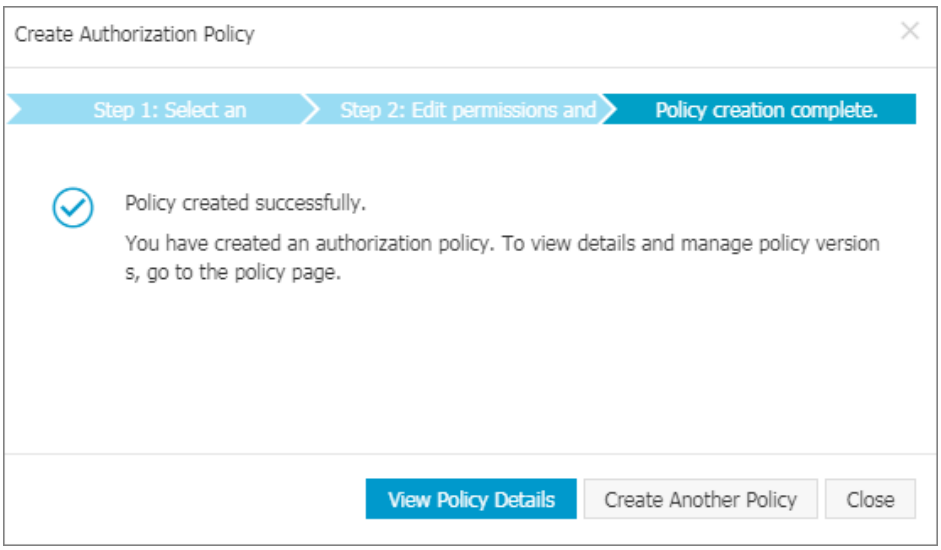
Click **Create Authorization Policy** to create custom authorization policies as the following samples for the specified resource instance and grant the policies to the specified

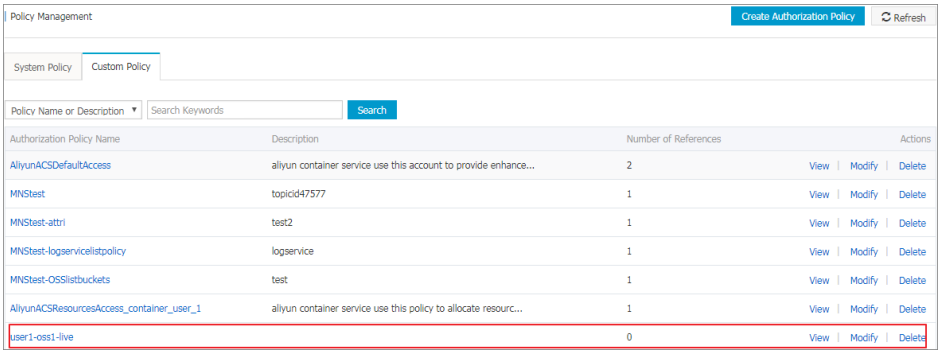
subaccount.


RAM
Policy Management
Create Authorization Policy
Refresh
Dashboard
Users
Groups
Policies
Roles
Settings
System Policy
Custom Policy
Policy Name or Description
Search Keywords
Search
Authorization Policy Name
Description
Number of References
Actions
AliyunACSDefaultAccess
aliyun container service use this account to provide enhance...
MNStest
topicid47577
MNStest-attri
test2
MNStest-logservicelistpolicy
logservice
MNStest-OSSlistbuckets
test
AliyunACSResourcesAccess_container_user_1
aliyun container service use this policy to allocate resourc...
View
Modify
Delete


Create Authorization Policy
Step 1: Select an
Step 2: Edit permissions and
Policy creation complete.
All Templates
Enter keywords to dynamically filter the templates below.
Blank Template
System AdministratorAccess
Provides full access to ...
System AliyunOSSFullAccess
Provides full access to ...
System AliyunOSSReadOnlyAccess
Provides read-only acces...
System AliyunECSFullAccess
Provides full access to ...
System AliyunECSReadOnlyAccess
Provides read-only acces...
System AliyunRDSFullAccess
Provides full access to ...
System AliyunRDSReadOnlyAccess
Provides read-only acces...


Create Authorization Policy
Step 1: Select an
Step 2: Edit permissions and
Policy creation complete.
* Authorization Policy Name :
user1-oss1-live
Names must be 1-128 characters long. They may only contain the letters A-Z, numbers 0-9, and hyphens.
Description :
Policy Content :
{
"Version": "1",
"Statement": [
{
"Effect": "Allow",
"Action": [
"oss1:*"
],
"Resource": [
"acs:oss1:*:*:$Bucket",
"acs:oss1:*:*:$Bucket/*"
]
Authorization Policy Format
Authorization Policy FAQ
Previous
Create Authorization Policy
Cancel





Note: After the authorization policies are created for various service resource objects, you can grant the permissions to the corresponding subaccounts.

The following are OSS and CDN authorization policies. You can grant corresponding permissions to subaccounts as needed.

OSS authorization policy

Permission description:

```
All operation permissions on specified buckets;
Permission to view the bucket list;
```

```
{
"Version": "1",
"Statement": [
{
"Action": [
"oss:*"
],
"Resource": [
```

```
"acs:oss:*:*:$Bucket",
"acs:oss:*:*:$Bucket/*"
],
"Effect": "Allow"
},
{
"Action": [
"oss:ListBuckets"
],
"Resource": "*",
"Effect": "Allow"
}
]
}
```

CDN authorization policy

Permission description:

```
All permissions on specified CDN domains;
Permission to query CDN domains;
```

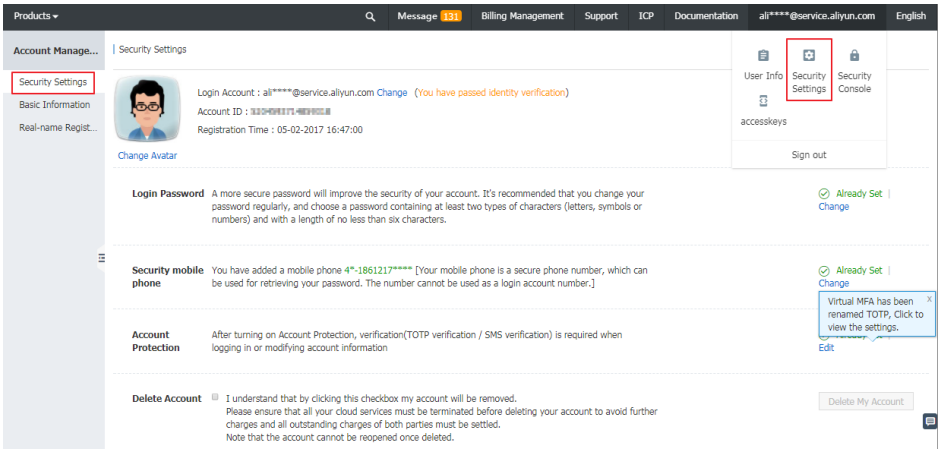
```
{
"Version": "1",
"Statement": [
{
"Action": "cdn:*",
"Resource": [
"acs:cdn:*:$Uid:domain/$DomainName"
],
"Effect": "Allow"
},
{
"Action": "cdn:Describe*",
"Resource": "*",
"Effect": "Allow"
}
]
}
```

The following variables are used in the resource authorization policies of each service. Replace them with your actual resource instance name:

Description of variables

Uid

$Uid: Alibaba Cloud account ID. You can query it through **Alibaba Cloud console** > **Account Management** > **Security Settings**.



Bucket

$Bucket: OSS Bucket.

CDN

$DomainName: Name of the CDN domain.