Alibaba Cloud ApsaraVideo for Live

User Guide (New console)

Issue: 20190917

MORE THAN JUST CLOUD | Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

Legal disclaimer..... I
Generic conventions..... I
1 About ApsaraVideo Live console.....1
2 Getting started.....2
3 Domain names management.....4
3.1 Manage a domain name.....4
3.1.1 Add a domain name..... 4
3.1.2 Associate domain names..... 5
3.1.3 Disable a domain name..... 6
3.1.4 Enable a domain name..... 7
3.1.5 Delete a domain name..... 7
3.2 Configure CNAME..... 8
3.3 Configure HTTPS..... 10
3.4 Access control.....17
3.4.1 Configuration authentication..... 17
3.4.2 Configure hotlinking protection..... 23
3.4.3 Configure IP address blacklist..... 25
3.5 Configure premium streaming (Formerly global acceleration)..... 27
4 Configure push streaming and live streaming..... 31
4.1 Configure edge ingestion.....31
4.2 Stream ingest and live streaming at mobile end..... 35
4.3 Stream ingest and live streaming at PC end.....36
4.4 Stream pulling..... 40
4.5 Ingest URL and streaming URL.....42
4.5.1 Ingest URL and streaming URL (Original)..... 43
4.5.2 Ingest URL and streaming URL (Encoding)..... 45
4.6 Ingest URL and streaming URL (Not authenticated).....53
4.6.1 Ingest URL and streaming URL (Original)..... 54
4.6.2 Ingest URL and streaming URL (Encoding)..... 56
4.7 Create multiple live activities..... 63
5 Transcoding management..... 67
5.1 Universal Transcoding..... 67
5.2 Custom transcoding..... 69
6 Recording management..... 73
6.1 Save live recordings to OSS.....73
6.1.1 Configure OSS.....73
6.1.2 Store live recordings to OSS..... 77
6.1.3 Recording callbacks.....81
6.1.4 Record indexes..... 84

7 Screenshots management....87
7.1 Configure snapshots....87
8 Streams Management....90
8.1 Ingest Callback URL....90
8.2 View frame rate and bit rate....92
8.3 View a live stream....95
9 Real-time monitoring....96
9.1 Push streaming monitoring....96
10 Statistics-Visits....97
11 Set subaccounts to log on to the ApsaraVideo Live console by using RAM....98

1 About ApsaraVideo Live console

The new version of the ApsaraVideo Live console adopts the latest interaction interface and provides various configuration functions, such as edge ingestion, acceleration configuration, resource monitoring, and log management. The new version of the console enables you to rapidly manage ApsaraVideo Live domain names, and live streams, and configure basic functions, such as transcoding and recording. Meanwhile, the new console provides the resource monitoring service to facilitate real-time data analysis.

Functions of the new console

Functions	Description
Live Management	You can manage online streams, historical streams, and disabled push streams.
Domain Names	You can add, manage, and delete domain names, modify basic information or configuration of domain names.
Resource Monitoring	You can monitor the usage, and analyze user access.
Logs	You can download traffic log.

2 Getting started

This article describes how to quickly use ApsaraVideo Live service to perform push streaming and live streaming operations.

Prerequisites

- Domain names that have completed ICP filing.

  Alibaba Cloud provides live service. You must prepare domain names that have completed ICP filing. For more information, see ICP Filing Process.

- Push streaming tool and live streaming tool
  - PC-end push streaming/live streaming tool

    Many PC-end push streaming tools are available in the market. You can select one based on your needs. This article takes OBS as an example to introduce live activity process for you.
  - Mobile-end push streaming tool/live streaming tool

    Alibaba Cloud provides push streaming SDK and player SDK demo. You can use the Demo for push streaming and live streaming operations.

Procedure

1. Log on to the ApsaraVideo Live console.
2. Add an Ingest Domain Name. For more information, seeAdd a domain name.
3. Add a Streaming Domain Name. For more information, see Add a domain name.
   - Ingest Domain Name: In the live service, you can use the Ingest Domain Name to splice the ingest URL. For more information, see Ingest URL and streaming URL.
   - Streaming Domain Name: In the live service, you can use the Streaming Domain Name to splice the streaming URL. For more information, see Ingest URL and streaming URL.

     Note:

You must add the Ingest Domain Name and the Streaming Domain Name. After adding the domain names, you must associate the Ingest Domain Name and the Streaming Domain Name.

- Accelerated Area: Area where the domain name can implement acceleration.

When you configure the domain names successfully, the system automatically configures CDN acceleration function. And you can use the live acceleration function after you configure CNAME.

4. Configure CNAME. For more information, see Configure CNAME.
5. Associate the Ingest Domain Name and the Streaming Domain Name. For more information, see Associate Domain Names.
6. Generate ingest URL and streaming URL. For more information, see Edge ingestion- Generate ingest URL and streaming URL.
7. Push streaming. You can use the Alibaba Cloud push streaming SDK or the third-party push streaming software (for example, OBS) to perform push streaming operation. You can also perform push streaming operation at mobile end and mobile end.

   Push streaming at PC end: This document takes OBS as an example to introduce live activity process for you. For more information about OBS download and configuration, see Push streaming and live streaming at PC end. Push streaming at mobile end: For more information, see Push streaming and live streaming at mobile end.
8. Live streaming.

   You can playback the live stream at PC end, and mobile end.

   Live streaming at PC end:

   - Use the web player to playback the live stream

     Copy the streaming URL to web player, and click Play.

   - Preview videos in Alibaba Cloud console

     You can log on to the ApsaraVideo Live console, and click Live Management > Streams > Live URLs to get and view the streaming URL. For more information, see View a live stream.

   Live streaming at mobile end:

   For more information, see Push streaming and live streaming at mobile end.

3 Domain names management

3.1 Manage a domain name

3.1.1 Add a domain name

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

Prerequisites

- If you want to use ApsaraVideo Live service in China, you must have a domain name that has completed ICP record filing.
- If the record-filing is pending, you must first apply for ICP record filing.

Procedure

1. Log on to the ApsaraVideo Live console.
2. Click Domains > Add Domain.

   Note:
   You must add an Ingest Domain and a Streaming Domain respectively.
3. Configure the Streaming Domain, and click Next。

   Note:
   - Live Center: refers to the location of the live center. The Ingest Domain and the Streaming Domain must be in the same region.
   - Domain Type: refers to the acceleration type of the domain name. Ingest Domain and Streaming Domain correspond to stream ingest acceleration and live streaming acceleration respectively.
   - Edge Group: refers to the area where the domain name can perform acceleration.

   Streaming Domain is created successfully.
4. Click Back to Domain List.
5. Click Add Domain.

6. Configure Ingest Domain, and click Next.

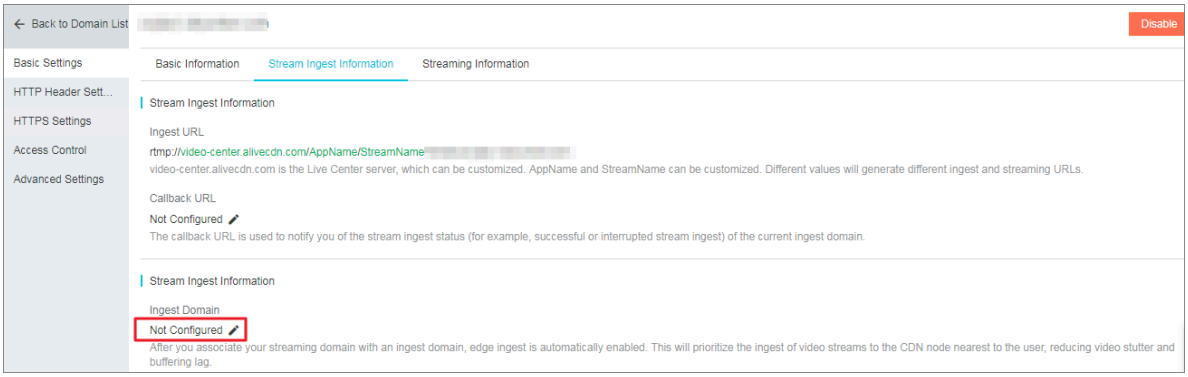
   Ingest Domain is created successfully.

> **Note:**
> After the domain names are created, you must configure CNAME for the domain names. For more information, see Configure CNAME. After the domain names are successfully configured, the domain names automatically configures acceleration function, and you can use the acceleration function immediately.

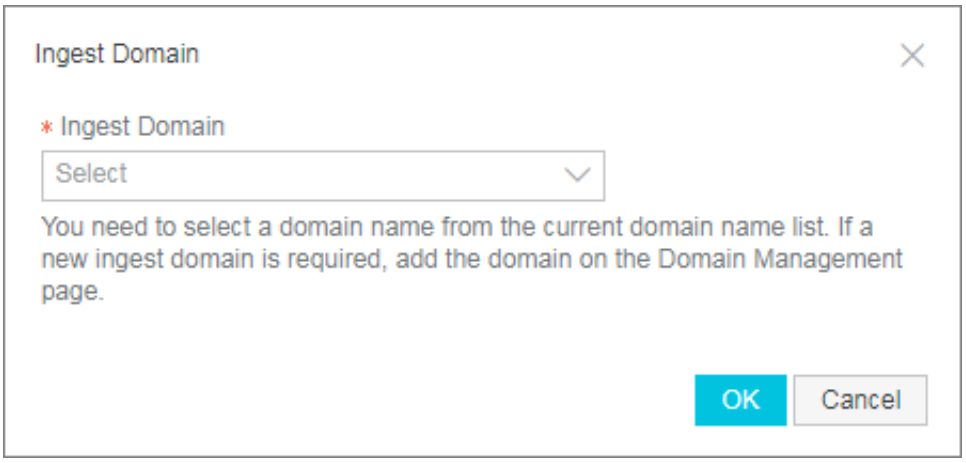
3.1.2 Associate domain names

After both domain names are added successfully, you must associate the ingest domain and the streaming domain so that the domain names take effect.

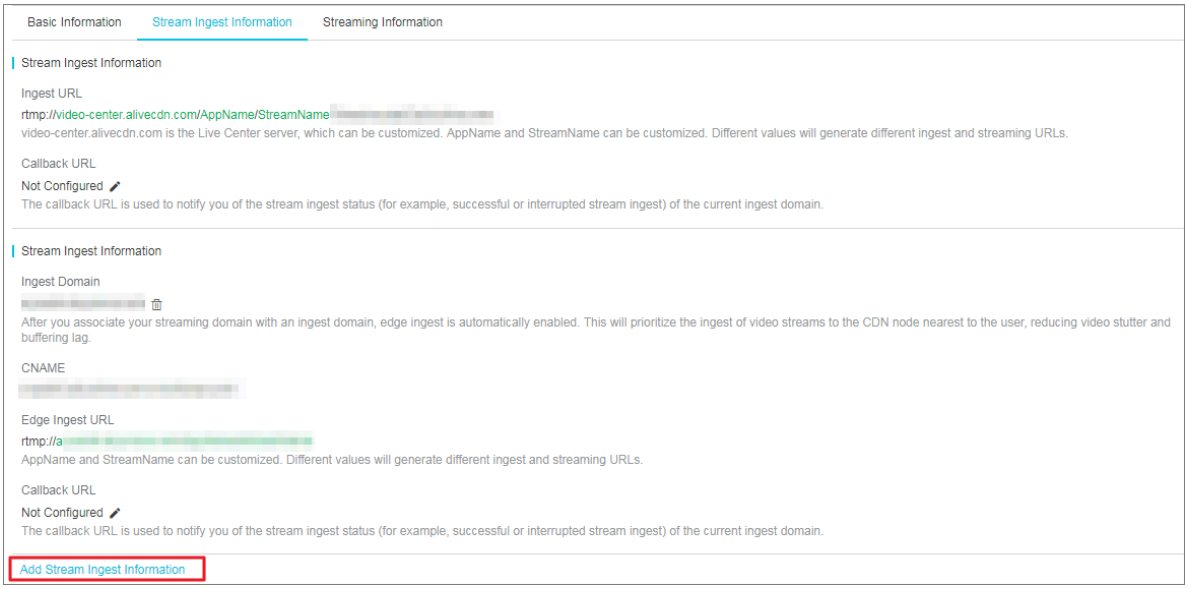
1. Log on to the ApsaraVideo Live console.
2. Click Domains.
3. Select the Streaming Domain, and click Domain Settings at the right side.
4. In Basic Settings > Stream Ingest Information, select Stream Ingest Information, and click Not Configured.



5. In the Ingest Domain drop-down list, select the Ingest Domain and click OK.



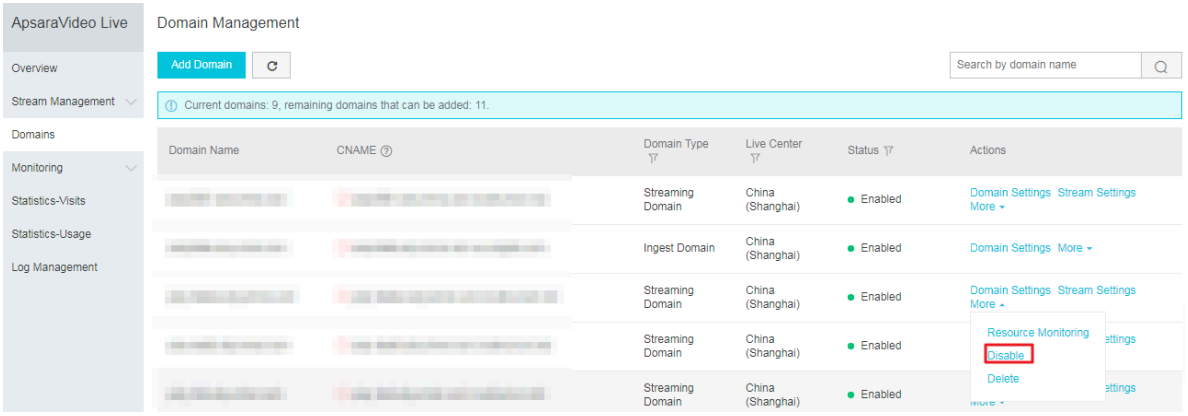
6. If you want to associate more Ingest Domains, click the following Add Stream Ingest Information.



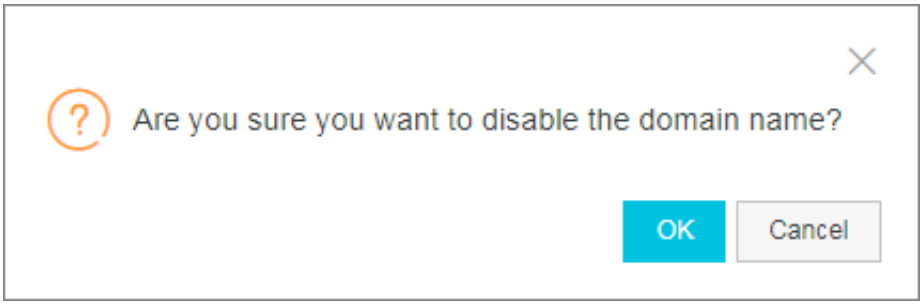
3.1.3 Disable a domain name

Perform the following steps to disable a domain name.

1. Log on to the ApsaraVideo Live console.
2. Click Domains.
3. Select the domain name that you want to disable, and select Disable in the drop-down list of More.



4. Click OK.



The current status of the domain name in Status is Disabled.

3.1.4 Enable a domain name

Perform the following steps to enable the domain name that you have disabled.

1. Log on to the ApsaraVideo Live console.
2. Click Domains.
3. Select the domain name you want to enable, click More at the right side, and select Enable in the drop-down list.
4. Click OK.

In Status, the domain name is currently Enabled.

3.1.5 Delete a domain name

Perform the following steps to delete a domain name.

> Note:
> A domain name can only be deleted when its status is Disabled. Therefore, you must first disable the domain name before you delete it. For more information , see Disable a domain name.

1. Log on to the ApsaraVideo Live console.
2. Click Domains.
3. Select the domain name that you have disabled, and select Delete in the drop-down list of More.
4. Click OK.

3.2 Configure CNAME

Procedure

1. Log on to the ApsaraVideo Live console.
2. Click Domain Names.
3. Select the Streaming Domain Name, and copy the corresponding CNAME.

Note:

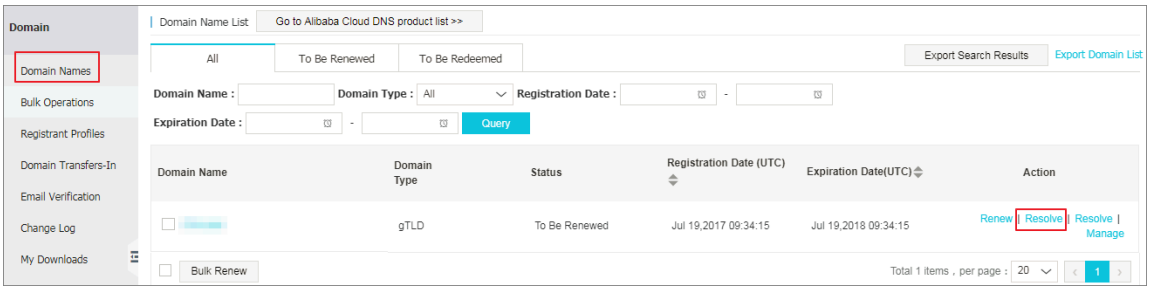
An exclamation mark (!) in CNAME indicates that the domain name has not complete CNAME configuration. For more information about configuring CNAME, see the following steps.

4. Copy CNAME, and perform the CNAME configuration operation.

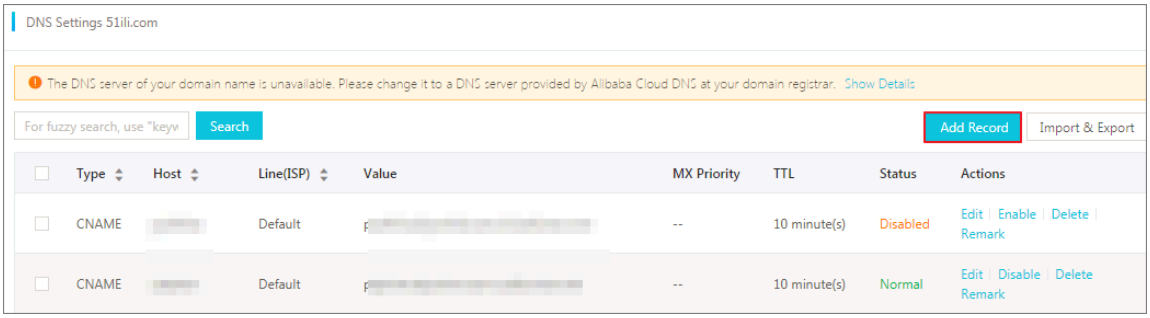
   a. Log on to the Domains console.

   b. Click Domain Names.

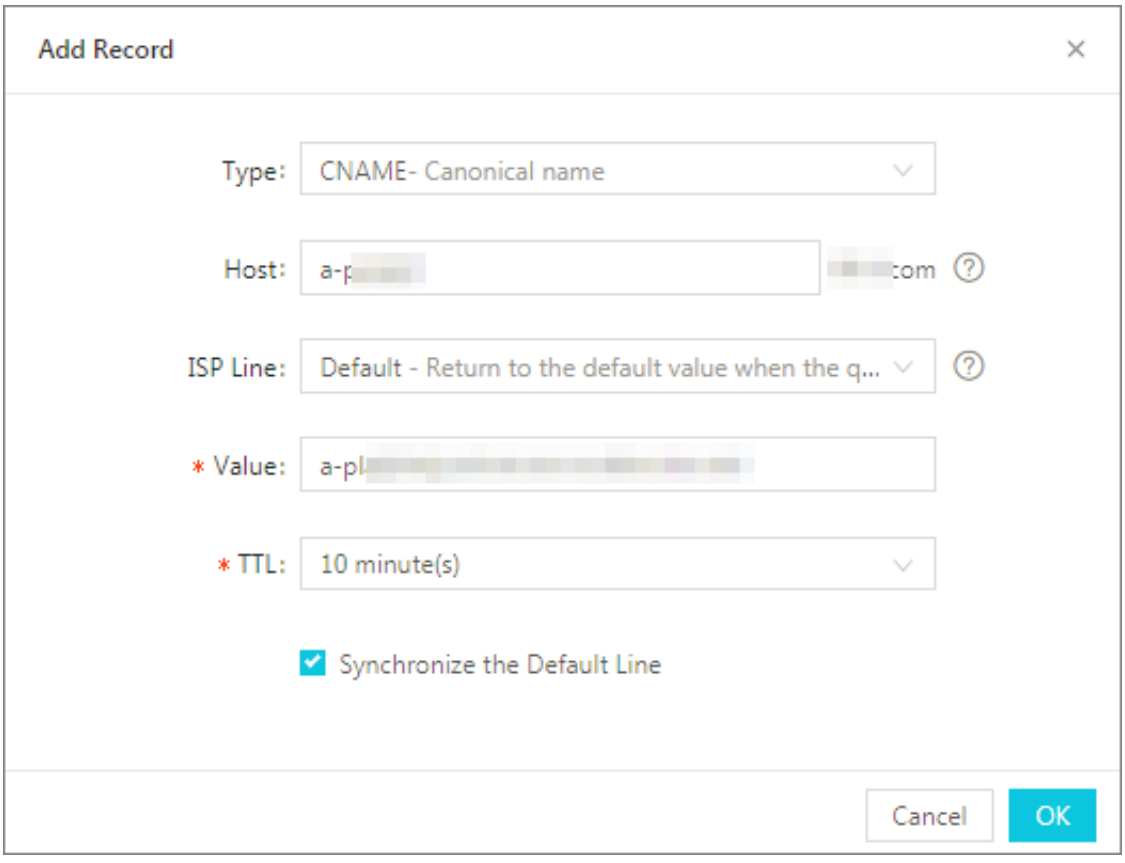
   c. Select the domain name you want to configure CNAME, and click Resolve.



   d. Click Add Record.



   e. Configure parameters, and clickOK.



- In Type, select CNAME-Canonical name.
- In Host, enter the secondary domain name of the Streaming URL. For example: the Streaming Domain Name is `a - play . aliyunlive . com`, then the secondary domain name is `a - play`.
- In Value, enter the CNAME you have copied from the domain name list.

5. After you complete configuring CNAME for the Streaming Domain Name, you must perform the same operations for Ingest Domain Name.

> Note:
> After you configure the resolution parameters, the CNAME configuration normally takes effect quickly.
>
> - If it is a newly created domain name, the resolution are not required 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.

3.3 Configure HTTPS

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a security 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 settings

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 name. 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.

Attentions

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 certificat e are supported, but the effective period for performing these operations is 1 hour . Perform the operation with caution.

Certificate restrictions

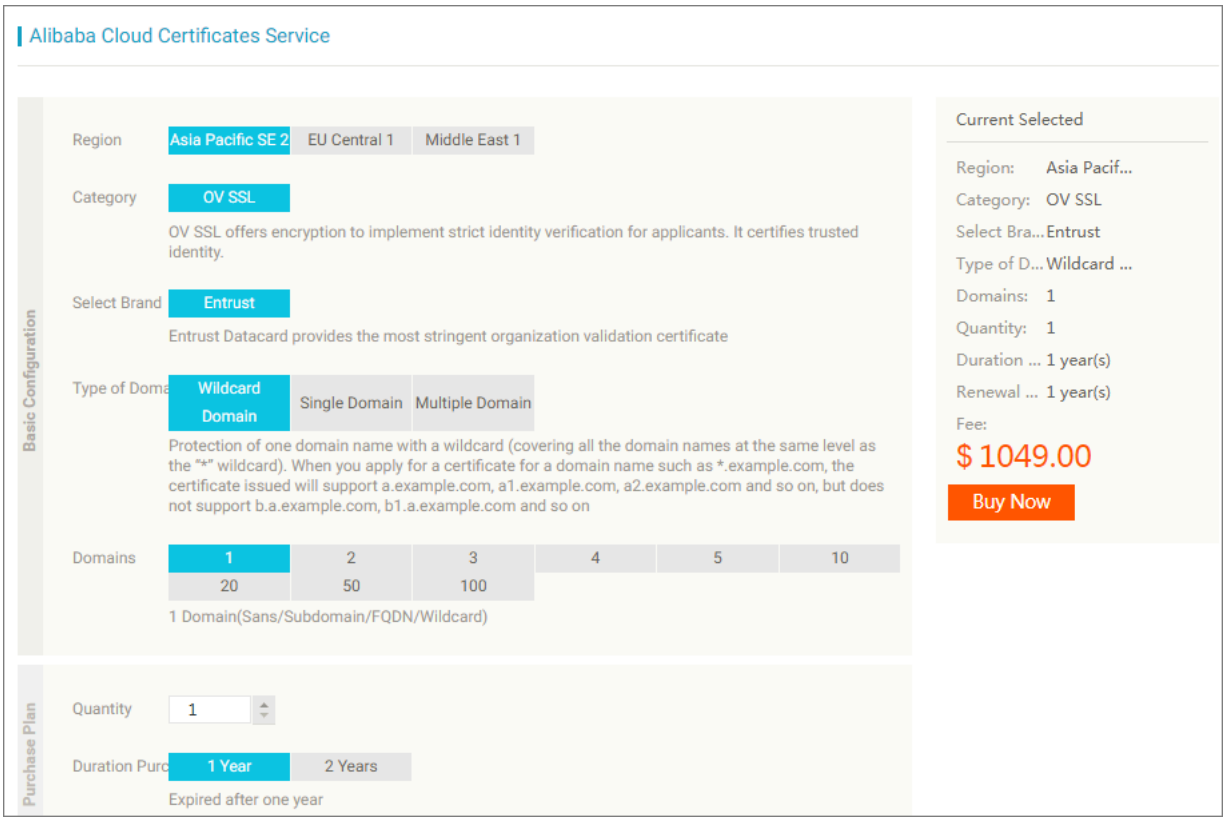
- The certificate and private key of a CDN domain name for which HTTPS Settings is enabled, must be uploaded. Both the certificate and private key must be in PEM format.

  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 correspond ence 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.

Procedure

Step 1. Buy a certificate

To enable HTTPS Settings , you must have a certificate that matches the CDN domain name. Click Buy Now at the ApsaraVideo Live Certificates Service to buy a certificate.



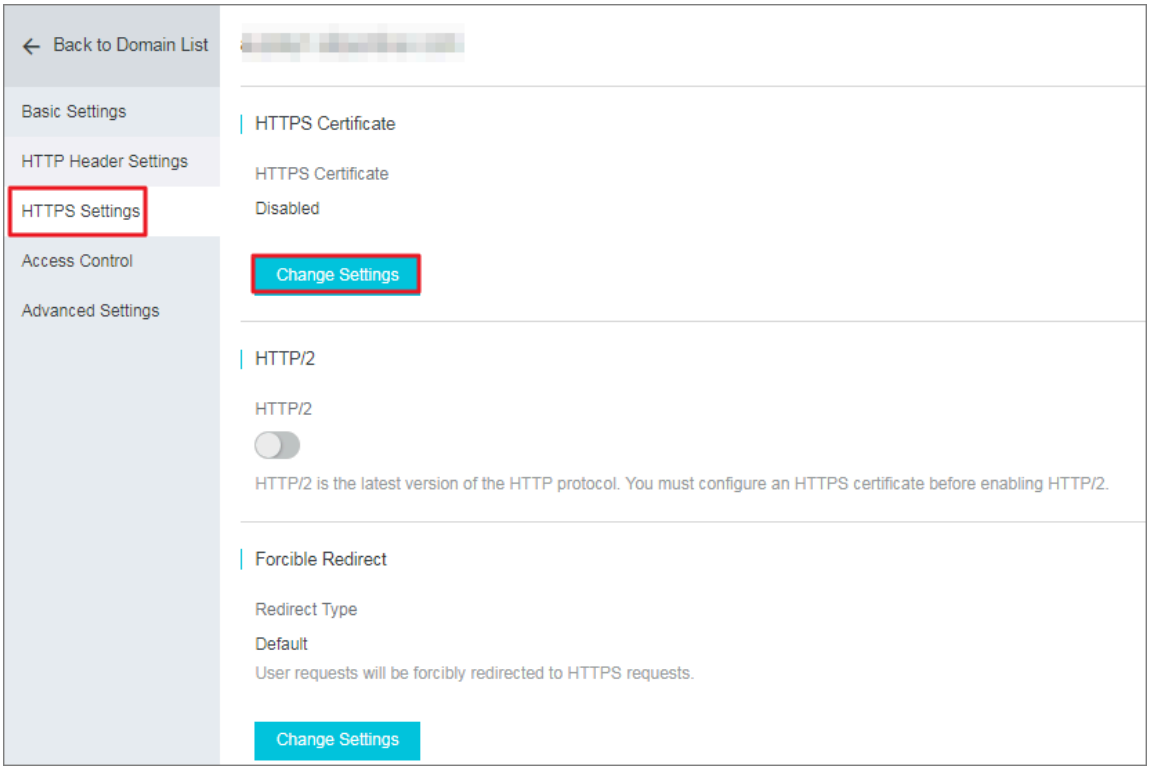
Step 2. Configure the ApsaraVideo Live domain name

1. Enable HTTPS settings.

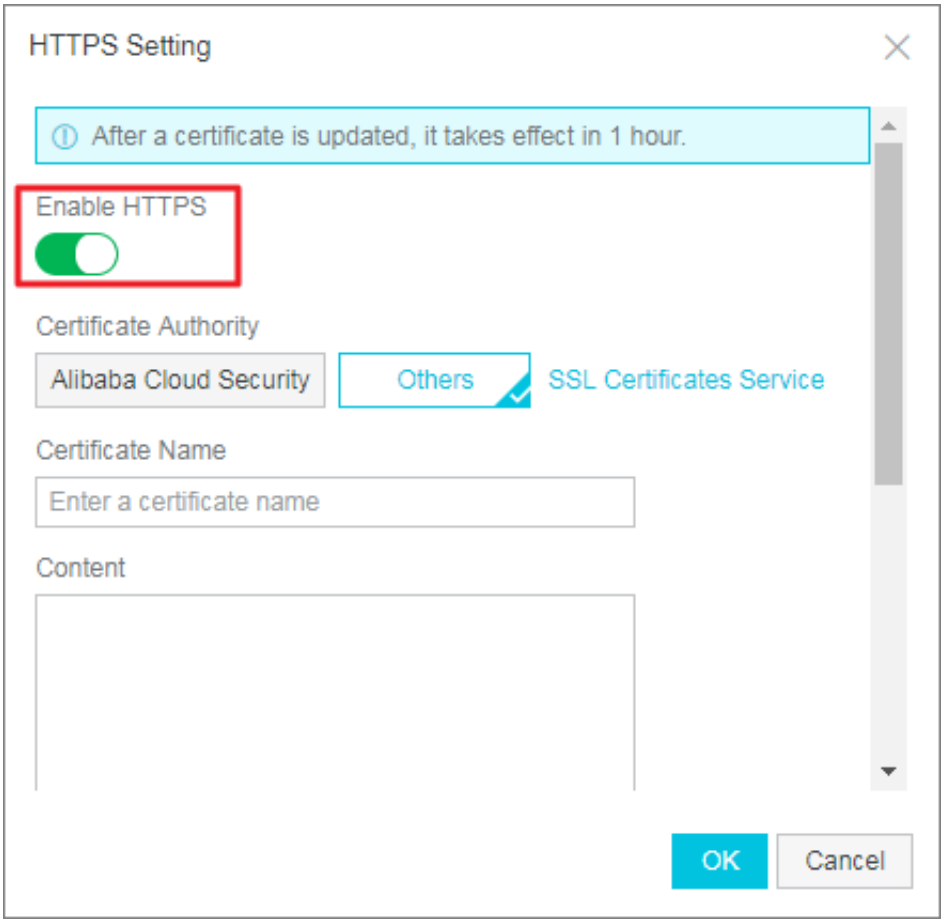
   a. Log on to the ApsaraVideo Live console.

   b. Click Domains, select the Streaming Domain that you want to perform HTTPS settings, and click Domain Settings .

   c. Click HTTPS Settings, and click Change Settings following HTTPS Certificate .



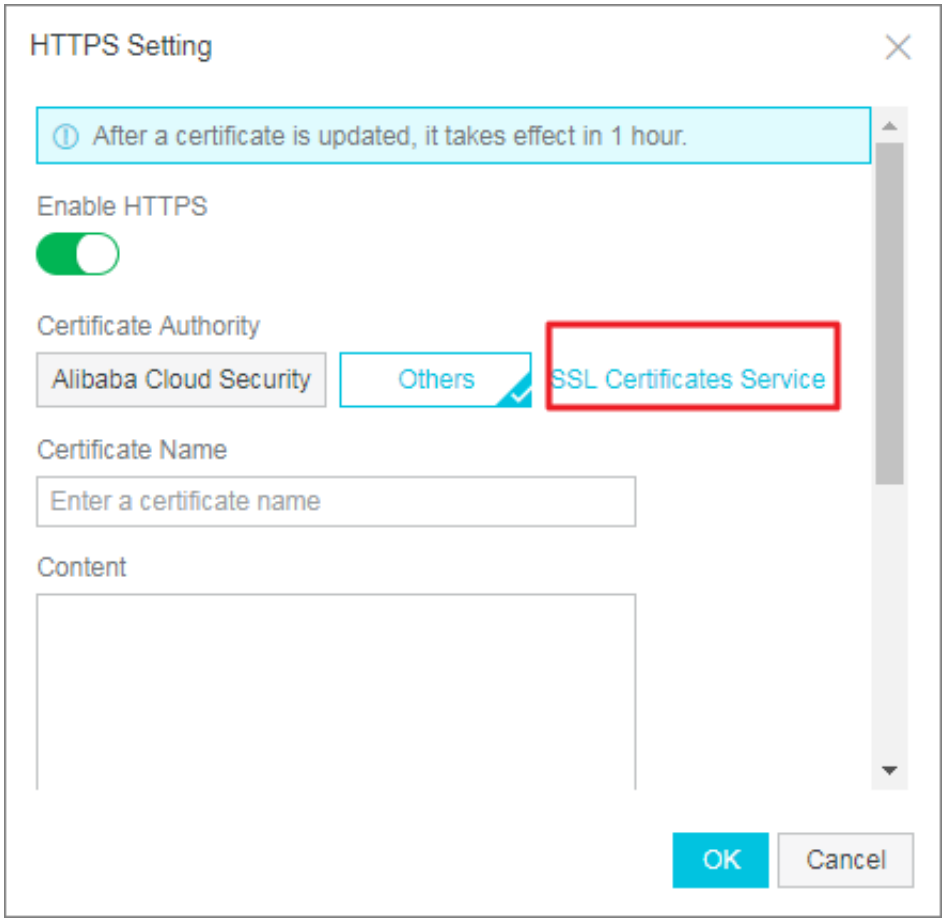
   d. In HTTPS Setting, enable HTTPS to go to the Certificate Status.


HTTPS Setting
After a certificate is updated, it takes effect in 1 hour.
Enable HTTPS
Certificate Authority
Alibaba Cloud Security
Others
SSL Certificates Service
Certificate Name
Enter a certificate name
Content
OK
Cancel

2. Select a certificate.

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

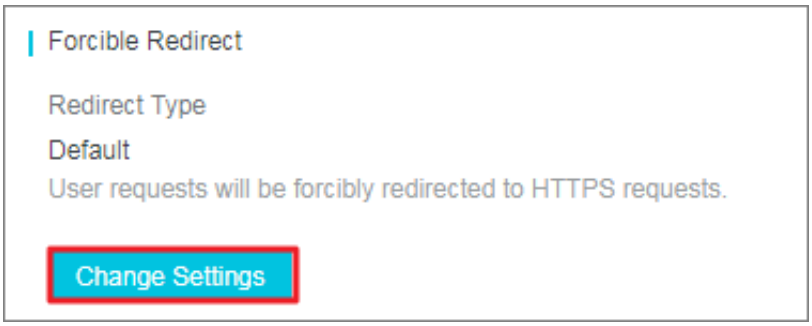
   - Self-owned certificate: You must set the certificate name and then upload the certificate content and private key. The certificate is then saved in the Alibaba Cloud SSL Certificates console. You can view it under My Certificates tab.
   - Self-owned certificate: You must set the certificate name and 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 ApsaraVideo Live Certificates Service are supported. You can select a certificate name to adapt to the CDN domain name.



Note:
Only certificates in PEM format are supported.

3. Set the redirect type.

   Click Change Settings following Redirect Type.



   Forcible Redirect is supported: The system forces redirect of the users' original request methods by default.

   For example, if HTTP > HTTPS redirect 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 configurations are completed and the certificate is enabled now. If a green HTTPS mark appears in your browser, it indicates that currently a private connection is established with the website, and HTTPS settings take effect.

3.4 Access control

3.4.1 Configuration authentication

URL authentication function aims to protect the user’s website content from the illegal or malicious behavior. Using anti-leech to add a referrer whitelist and blacklist can solve some hotlinking problems. However, the referrer anti-leech cannot protect the site resource because the referrer content can be falsified. Therefore, using URL authentication to protect the user’s source site resource is safer and more effective.

It is a safe and reliable anti-theft mechanism that protects site resources by coordinating Alibaba Cloud CDN acceleration node with customer’s resources site . The customer site provides customer with an encrypted URL (including authentica tion 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.

Authentication URL composition

Authentication URL consists of Live streaming address/stream play address + verification string. The verification string is calculated according to md5 algorithm by using authentication key + expiration time. This address is applicable to PC end, mobile end, third-party push streaming and live streaming tools.

- Authentication KEY: The field is assigned randomly, and also support custom configuration.
- Validity Period: The time when user visits customer source server exceeds the self-defined time (timestamp field designation), the authentication is invalid. For example, if the validity period 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	validity period, positive integer, fixed length 10, seconds measured from 1970 -01-01. Used to control validity period, integer of 10 digit, expire time 1800s.
rand	random number, we recommend that you use UUID (which cannot contain en dash” - “. For example, the format can be 477b3bbc253f467b8def6711128c7bec).
uid	not used yet (set to 0)
md5hash	verification string calculated according to md5 algorithm, lowercase letters and numbers 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 validity period 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 (see the following compositio n 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   correspond  ing   to   the   user ' s   request
object ,  not   including   parameters ,  for   example : / Filename
)  HashValue  =  md5sum ( sstring )
HashValue  =  md5sum ( sstring )
```

Examples

1. Use req_auth to request object. `http :// cdn . example . com / video / standard / 1K . html`
2. Set the key to: aliyuncdnexp1234 (set by the user).
3. The expire time of authentication is 2015-10-10 00:00:00, the seconds calculated is 1444435200.
4. The server structures a signature string used to calculate Hashvalue. `/ video / standard / 1K . html - 1444435200 - 0 - 0 - aliyuncdne  xp1234`

5. The server calculates HashValue according to the signature string. `HashValue = md5sum ("/video/standard/1K.html-1444435200-0-0-aliyuncdne xp1234") = 80cd3862d6 99b7118eed 99103f2a3a 4f`
6. The URL, when making a request, is `http://cdn.example.com/video/standard/1K.html?auth_key=1444435200-0-0-80cd3862d6 99b7118eed 99103f2a3a 4f`

   The calculated HashValue is consistent with md5hash = 80cd3862d699b7118eed 99103f2a3a4f in the user's request, and the authentication succeeds.

URL authentication code example

For more information, see Authentication code example.

Procedure

> Note:
> Authentication function is enabled by default. We recommend that you keep it enabled by default, so as to reduce the risk of bootlegging. If you want to disable the authentication function, contact your business manager or open a ticket.

When the authentication function is enabled, you can select default authentication or custom authentication based on your needs.

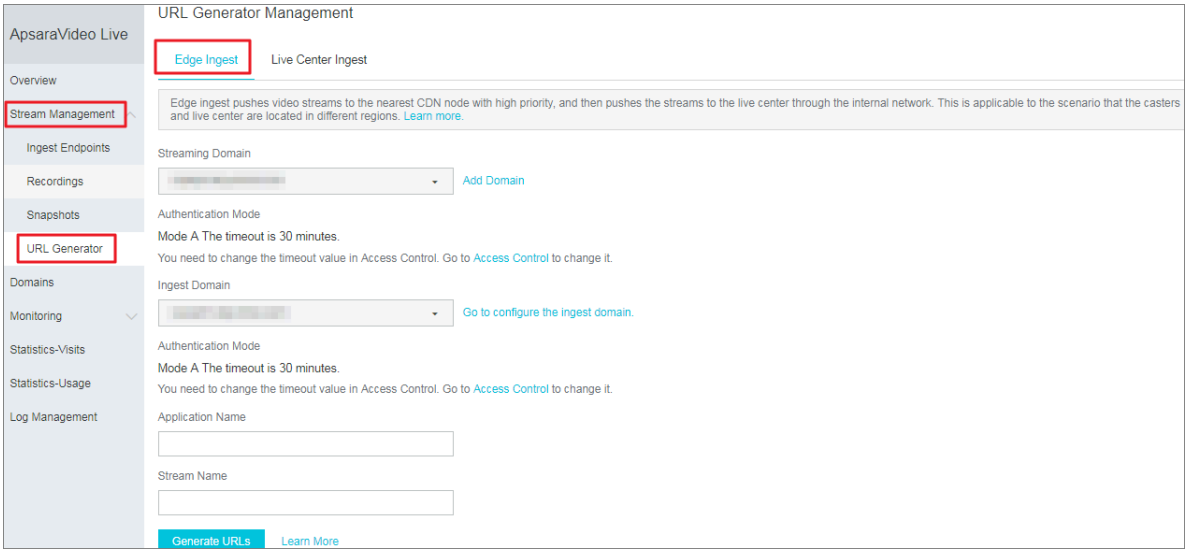
Default authentication

In default authorization, the authorization key is assigned randomly, and the Validity Period is 30 minutes. The authentication expires if the time exceeds 1800s.

1. Log on to the ApsaraVideo Live console.
2. Click Stream Management > URL Generator > Edge Ingest.

> Note:
> The edge ingest function preferentially pushes your video streams to the optimal CDN node to minimize such problems as video lagging and slow stream-pulling ratio. We recommend that you preferentially select Edge Ingest.

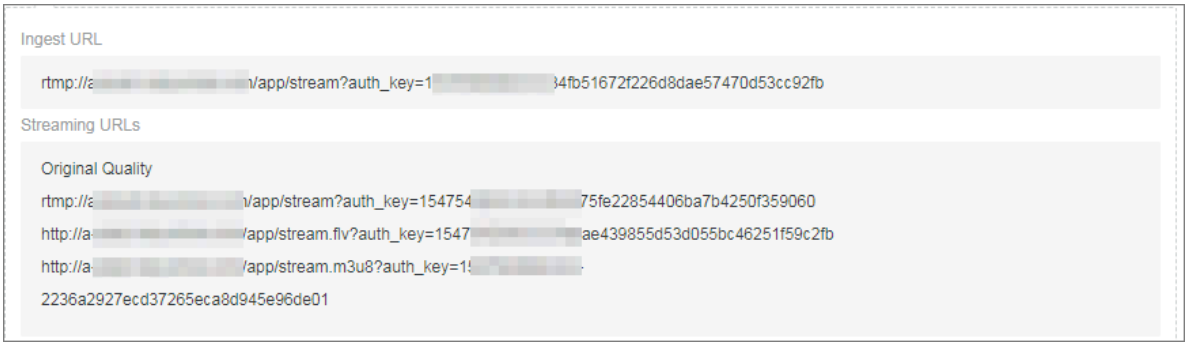
3. Select the Streaming Domain, and the associated Ingest Domain to be authenticated, enter the corresponding Application Name and Stream Name, and click Generate URLs.



Note:

You can configure the authentication for the Ingest Domain and the Streaming Domain as needed. We recommend that you perform authentication on both domains so as to reduce the risk of bootlegging.

You can get the authenticated Ingest URLs and Streaming URLs.

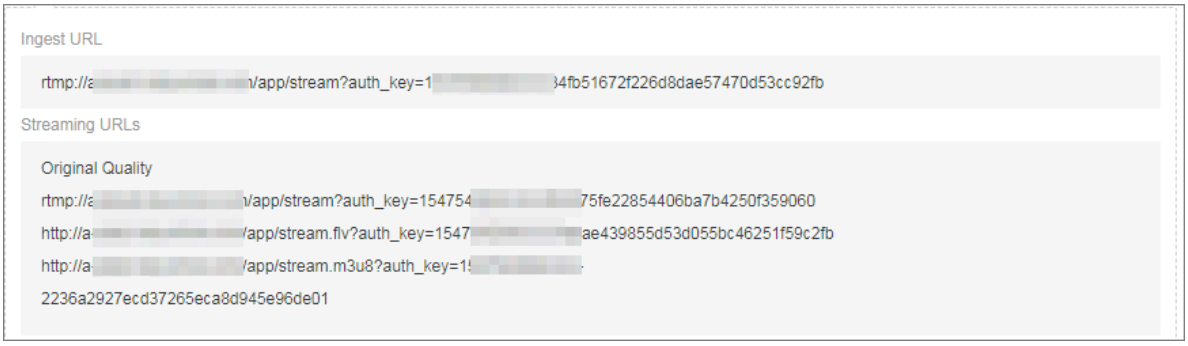


Custom authentication

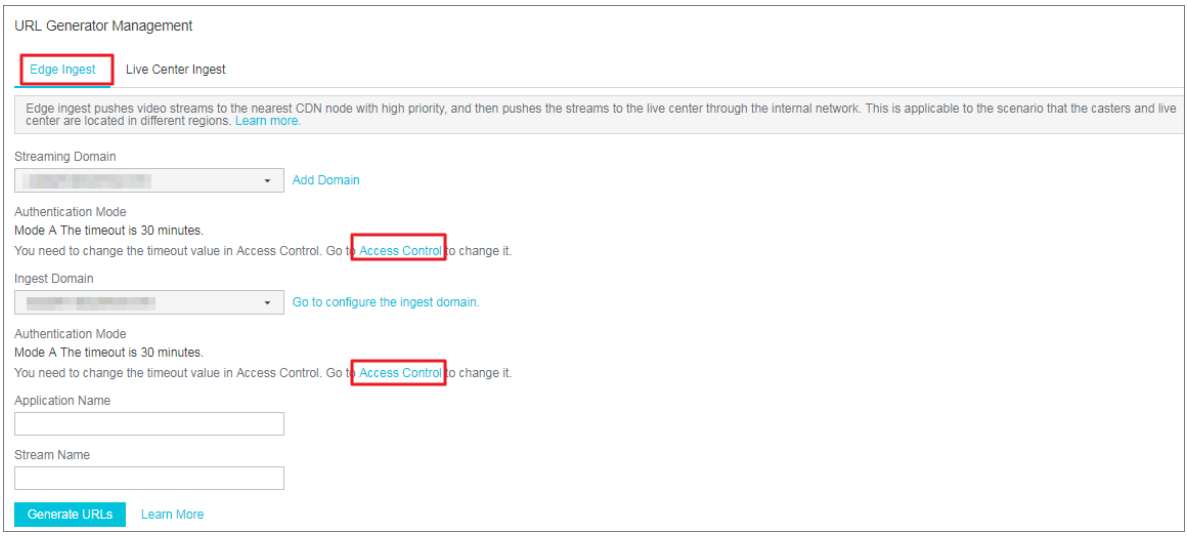
If you don’t adopt default configuration, you can also customize Primary KEY, Secondary KEY, Validity Period, Application Name and Stream Name to generate signed URL for stream ingest.

1. Log on to the ApsaraVideo Live console.
2. Click Domains, select the domain that you want to perform customize authentication, and click Domain Settings.

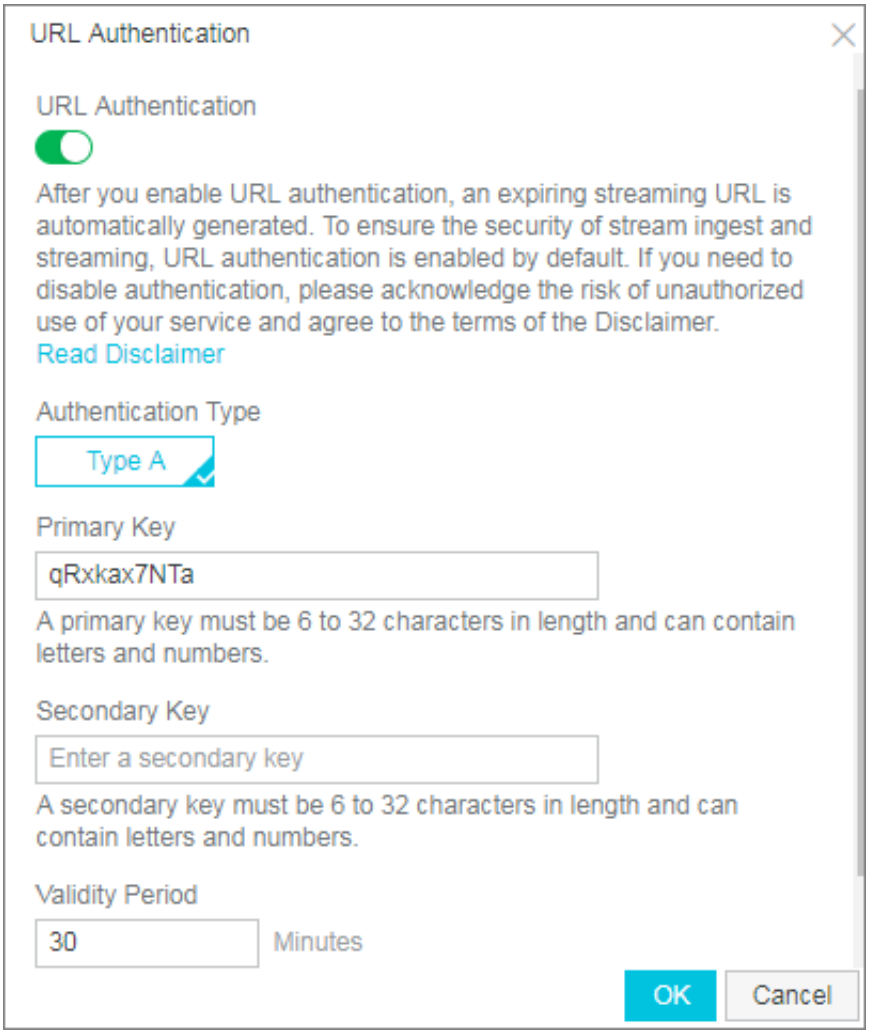
3. Click Access Control, select URL Authentication, and click Change settings.



You can also go to Stream Management > URL Generator > Edge Ingest, click Access Control following Streaming Domain and the associated Ingest Domain to quickly go to the custom authentication page.



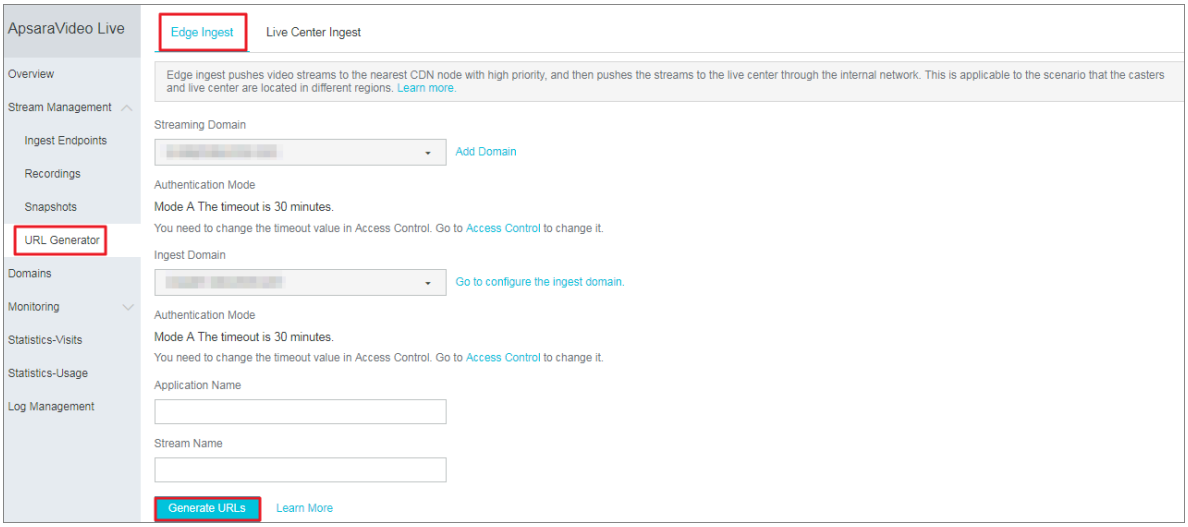
4. In URL Authentication page, customize thePrimary KEY, Secondary KEY, and Validity Period, and click OK.



Note:

Primary KEY is a key for calculating encrypted string. If the Primary KEY is changed, all URLs using the Primary KEY instantly becomes invalid. The Secondary KEYbridges the process of modifying the Primary KEY, that is, when you change the Primary KEY, the ingest URL or streaming URL using the Primary KEY does not become invalid instantly, and the Secondary KEY plays a transition role.

5. In Stream Management > URL Generator > Edge Ingest, select the Streaming Domain, the associated Ingest Domain to be authenticated, and enter the corresponding Application Name and Stream Name, and click Generate URLs.



You can get the signed Ingest URLs and Streaming URLs.

3.4.2 Configure hotlinking protection

The hotlinking protection function is realized based on the HTTP referrer mechanism where the referrer is used for source tracking and source identification. Users can configure a referrer blacklist or whitelist to identify and filter visitors in order to limit access to live video distribution resources.

Currently, the hotlinking protection function supports the blacklist or whitelist mechanism. After a visitor initiates a request for a resource, and the request arrives at a CDN node. The CDN node filters the identity of the visitor based on the preset hotlinking protection blacklist or whitelist. If the identity complies with the rules, the visitor can access the requested resource; and if the identity fails to comply with the rules, the request will be forbidden and a 403 response code is returned.

Attentions

- This function is optional and is disabled by default.
- To enable this function, you can edit Blacklist or Whitelist. The Blacklist and Whitelist are mutually excluded, and you cannot configure both of them. This article takes the blacklist setting as an example.

- You can set whether a null referrer field can be used to access CDN resources (That is, whether to allow direct access to resource URL by using a browser's address bar).

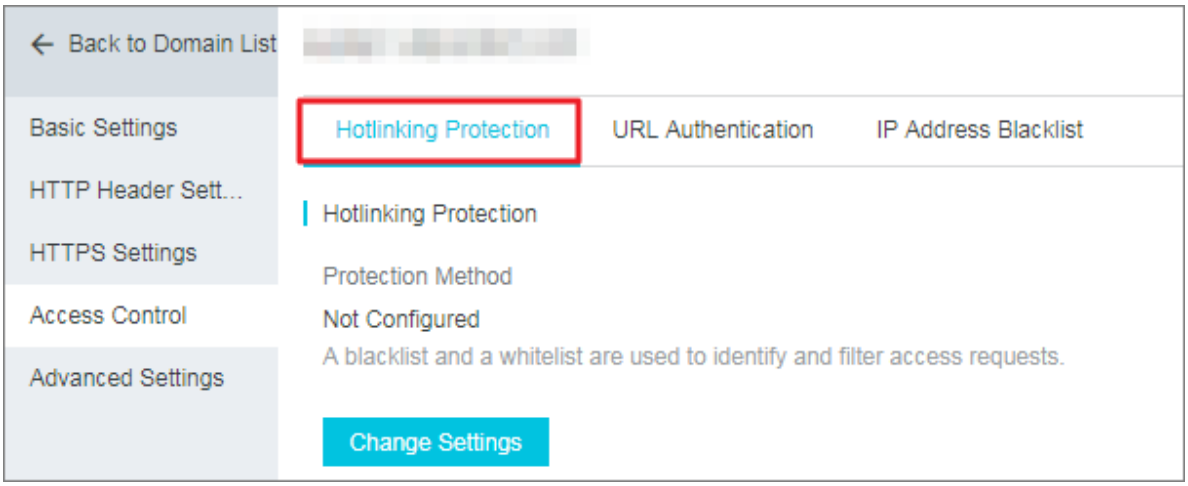
  Note:

  - Generally, mobile ends cannot get referrers. Therefore, the system currently supports access with a null referrer field by default. If you have set the system, and it does not support access with a null referrer field, you can set the referrer in combination with Alibaba Cloud player at the mobile end. For more information, see Basic player.
  - If you forbid access with a null referrer field, make sure to configure HTTPS secure acceleration, and enable force redirection to HTTPS (HTTP > HTTPS). When processing an HTTPS request for HTTP resources, some browsers remove the referred field and result in access failure.

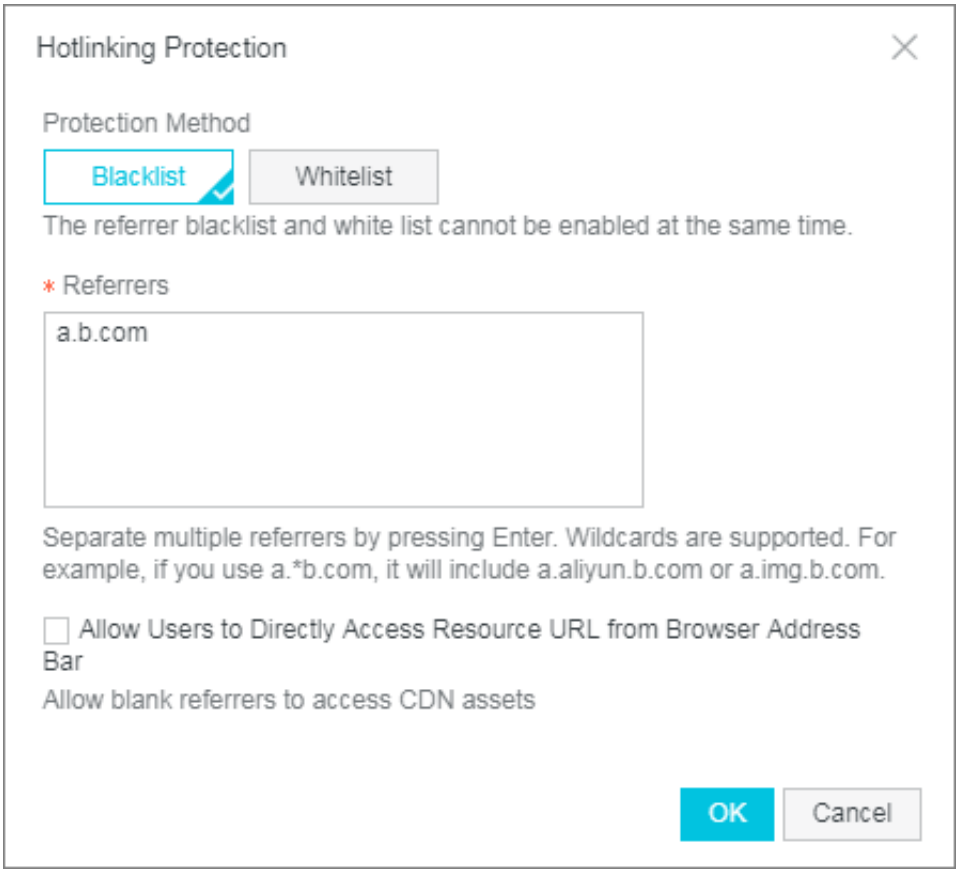
- After this function is enabled, wildcard domain names are automatically supported. For example, if you enter `a . com`, the final effective configuration is `*. a . com`. That is, all the sub-domains take effect.

Procedure

1. Click Domains.
2. Select the Streaming Domain to be configured, and click Domain Settings.
3. Click Access Control.
4. Select Hotlinking Protection, and click Change Settings.



5. Select the Blacklist, and add a specified domain name in Referrers.



Blacklist is added successfully.

Note:
You can configure only one format of the hotlinking protection function, that is, only one of the blacklist and the whitelist can be configured at the same time.

3.4.3 Configure IP address blacklist

ApsaraVideo Live supports blacklist rules. If an IP address is added to the blacklist, the IP address cannot access the current CDN domain name.

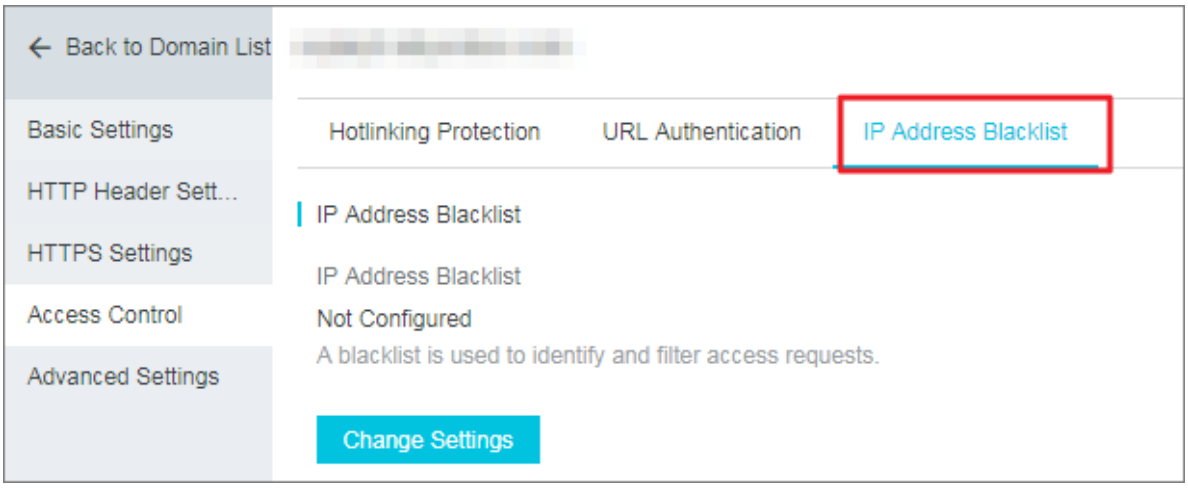
Attentions

IP address blacklist currently supports adding IP network segment. For example, 127.0.0.1/24.

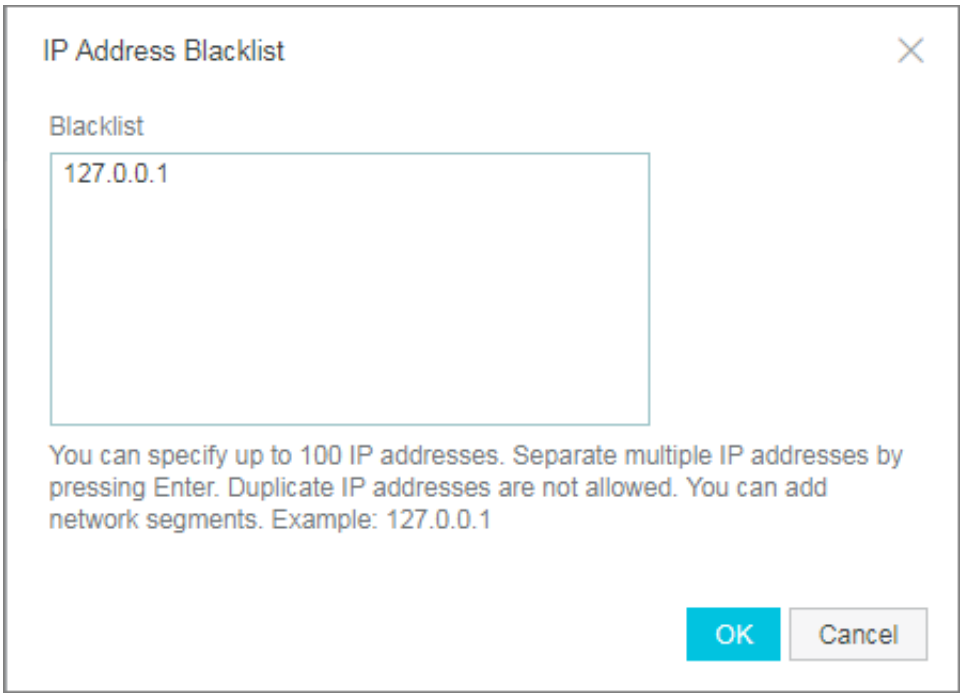
Wherein, 24 indicates that the first 24 bits of the subnet mask are effective. That is, 32-24=8bit indicates host ID, and the subnet can contain $2^8 - 2 = 254$ hosts. Therefore, the 127.0.0.1/24 indicates the IP network segment range is 127.0.0.1~127.0.0.255.

Procedure

1. Log on to the ApsaraVideo Live console.
2. Click Domains, select the domain name, and click Domain Settings.
3. Click Access Control > IP Address Blacklist, and click Change Settings.



4. In IP Address blacklist, enter the blacklist IP address.



IP Address blacklist is configured successfully.

3.5 Configure premium streaming (Formerly global acceleration)

Premium streaming is a high-speed circuit between the region where the streamer is located and mainland China.

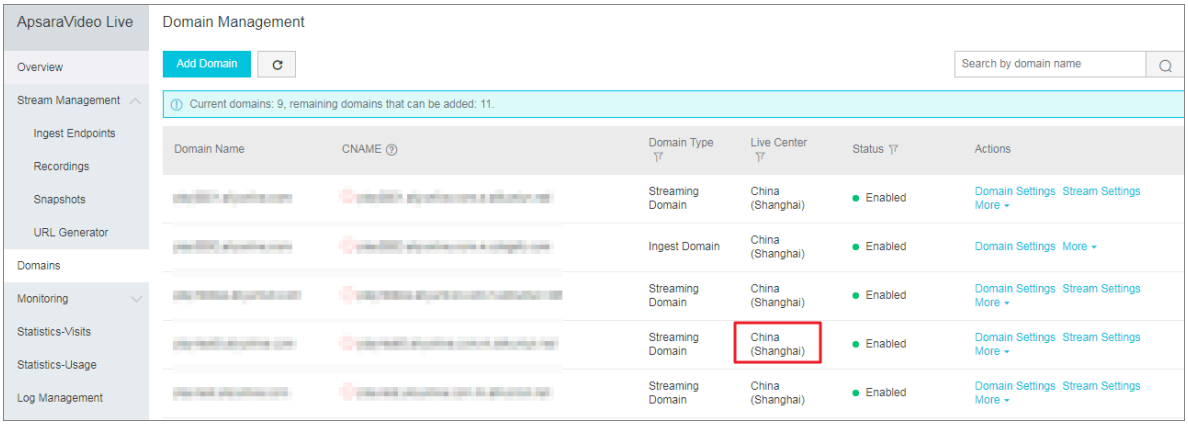
Scenario

- Streamer at abroad or in Hong Kong, Macao and Taiwan region: The premium streaming function is used to stream video streams to mainland China, and distribute the video streams in mainland China.
- Streamer in mainland China: The premium streaming function is used to pull and distribute video streams to specified acceleration region.

Attentions

- Premium streaming service is effective for a domain name only in China (Shanghai) region.

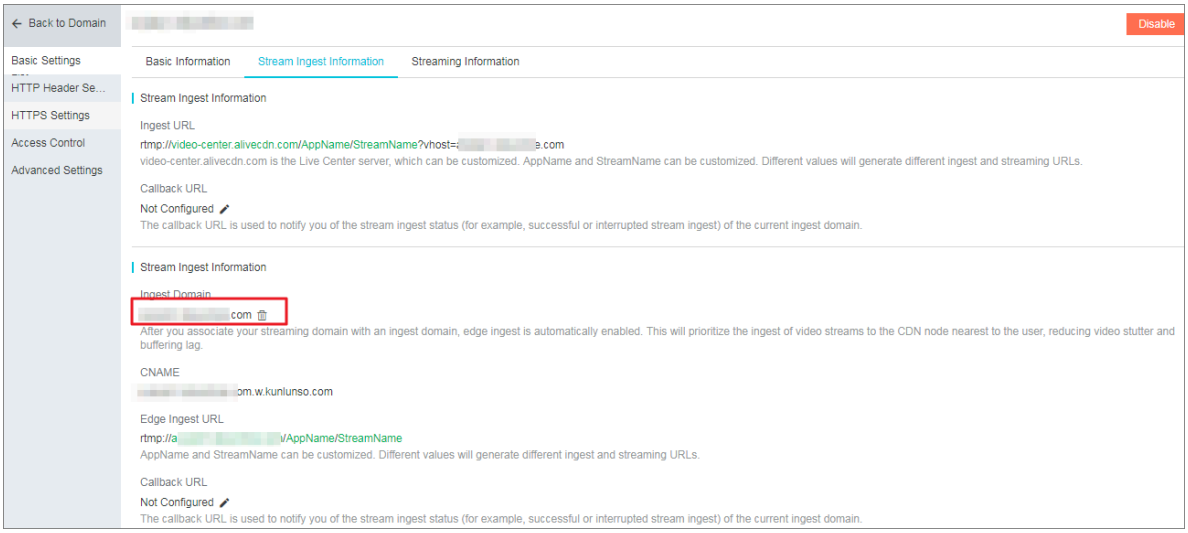
  Before configuring premium streaming, log on to the ApsaraVideo Live console, and confirm the region of the configured domain name in Domains.



- If you want to use premium streaming, you must use edge ingestion function. For more information, see Edge ingestion.

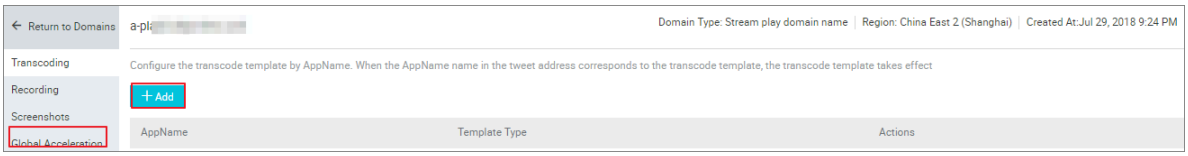
  When you associate domain names, the system automatically enable edge ingestion acceleration service. Before configuring premium streaming, confirm that you have associated ingest domain name and streaming domain name in

Domains > Domain Settings > Basic Settings > Stream Ingest Information. For more information about configuring edge ingestion, see Configure edge ingestion.

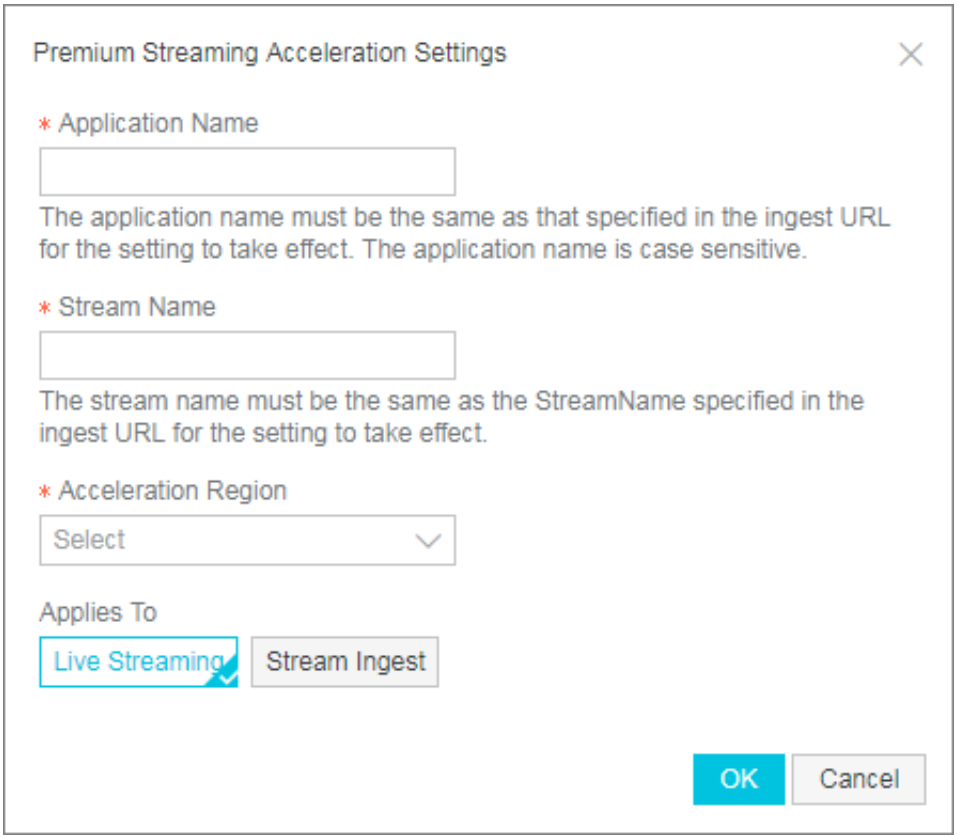


Procedure

1. Log on to the ApsaraVideo Live console.
2. Click Domains.
3. Select the Streaming Domain Name, and click Stream Settings.
4. Click Premium Streaming > Add.



5. In Premium Streaming Acceleration Settings, enter premium streaming parameters.



- Application Name The name of the video app. The Application Name must be the same with the Application Name, or the configuration does not take effect. For example, the Application Name in the ingest URL is app, and the Application Name of the premium streaming must also be app.
- Stream Name: The name of the stream. Enter the specified stream name. If you want to record all the streams under the Application Name, enter wildcard (*).

Note:

Application Name and Stream Name parameters support upper case letters, lower case letters, number, hyphen (-), underline (_) and period (.). The length is limited within 50 characters.

- Acceleration Region:
  - Stream Ingest acceleration: select the region where the streamer is located.
  - Live Streaming acceleration: select the region where the audience is located.

The premium streaming is configured successfully.

Note:
If the Stream Name you configured in Premium Streaming contains wildcard (*), and multiple streams are configured under the same Application Name, then all the streams perform the premium streaming configuration by default.

4 Configure push streaming and live streaming

4.1 Configure edge ingestion

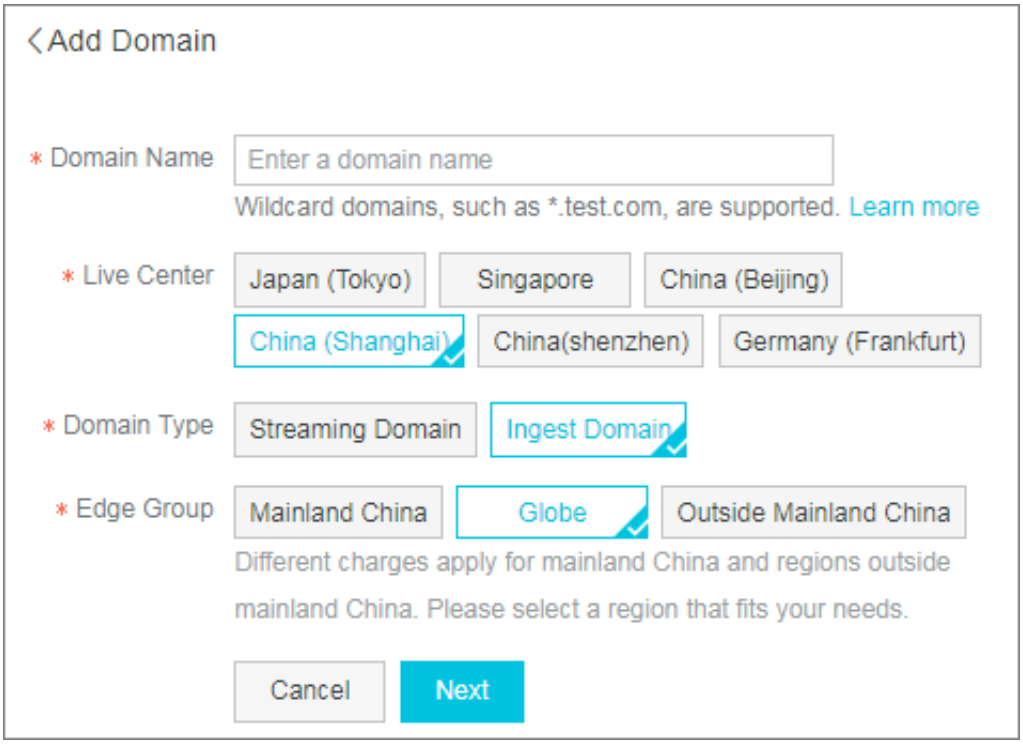
The edge ingestion function preferentially pushes your video streams to the optimal CDN node to ensure that users can access the best uplink network. Besides, it can minimize such problems as video lagging and slow pull streaming caused by uplink transmission.

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

2. Add an ingest domain name.

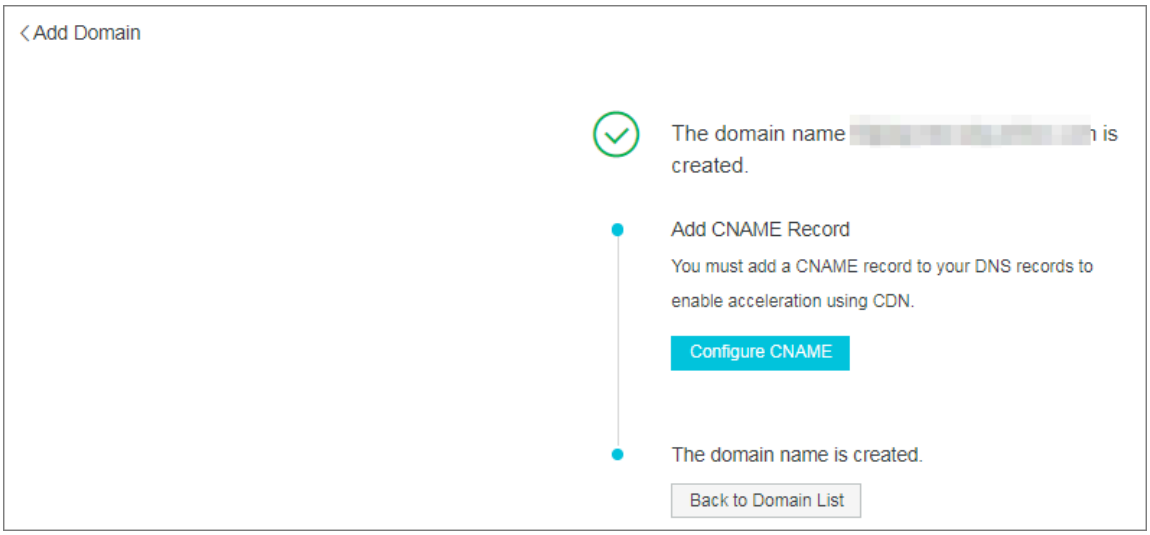
   a. Click Domains > Add Domain.

   b. Enter ingest domain information.



   c. Click Next, and the ingest domain is created successfully.

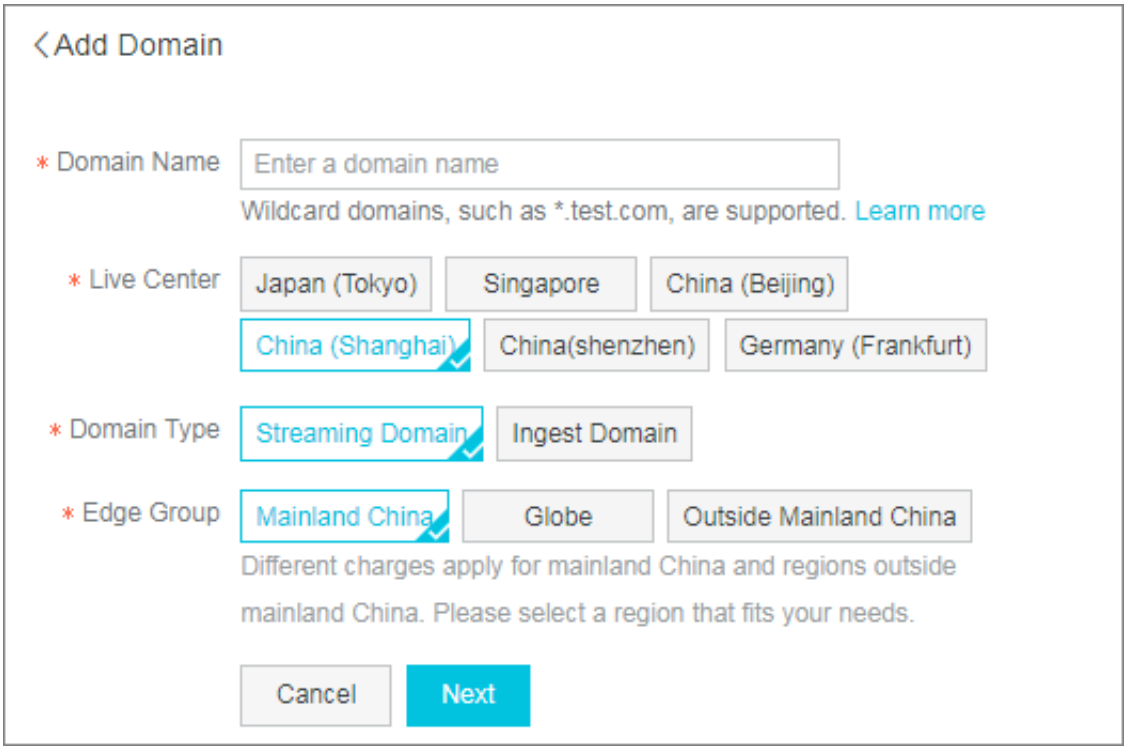
   d. Click Back to Domain List.



3. Create a streaming domain.

   a. In Domains, click Add Domain.

   b. Enter streaming domain information.



> **Note:**
> The Ingest Domain and the Streaming Domain must be in the same region so that you can associate the two domain names.

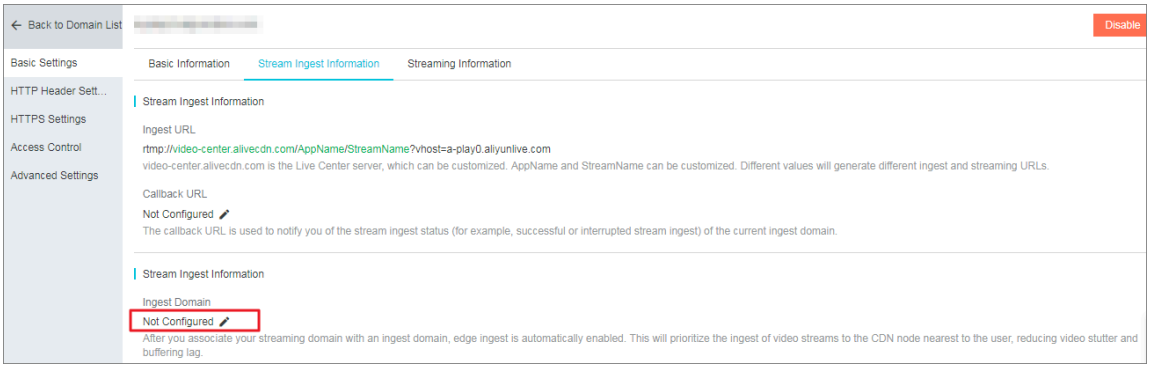
4. Configure CNAME.

   You must configure CNAME for the ingest domain and the streaming domain respectively. For more information, see Configure CNAME.

5. Associate the Ingest Domain and the Streaming Domain.

   a. In Domains, select the created Streaming Domain, and click Domain Settings.

   b. InBasic Settings, click Stream Ingest Information, and click Not configured followingStream Ingest Information.



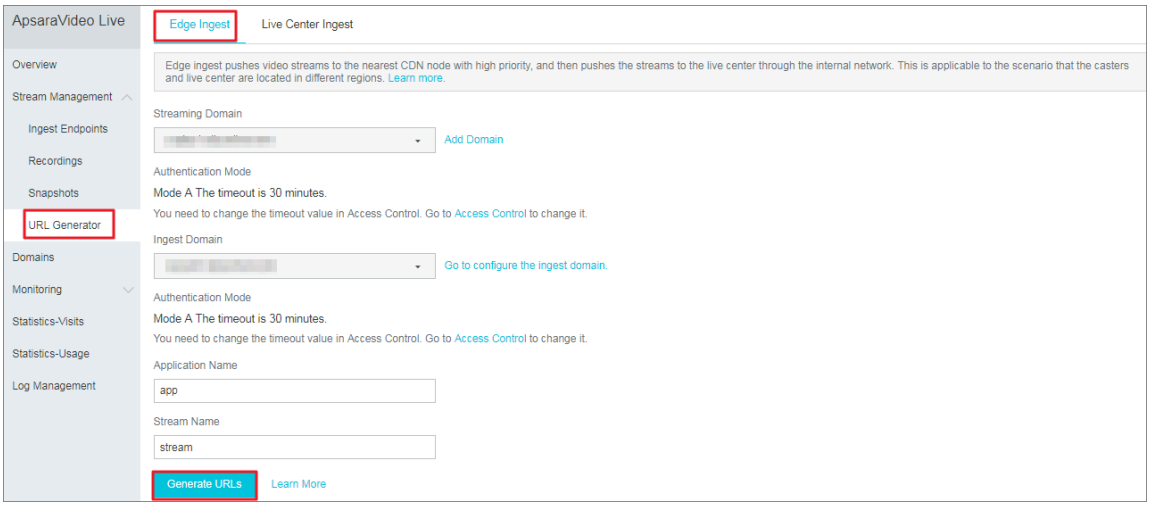
   c. Select the Ingest Domain, click OK, and return to the home page of the ApsaraVideo Live console.

6. Generate ingest URL and streaming URL.

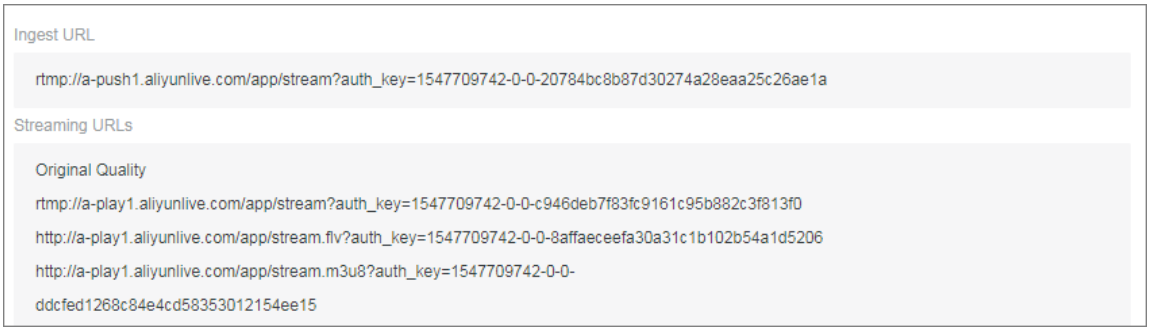
   a. Click Stream Management > URL Generator.

   b. Select the Streaming Domain and Ingest Domain.

   c. Enter Application Name and Stream Name, and click Generate URLs.



   d. Copy the URLs to stream ingest and live streaming tools for ingestion and playback.



4.2 Stream ingest and live streaming at mobile end

You can use Alibaba Cloud’s stream ingest and live streaming demo for stream ingestion and playback. Perform the following steps to complete stream ingest and live streaming at mobile end.

Download stream ingest and live streaming demo

You can use DingTalk app to scan the following QR code, install the mobile-end Demo integrated in Alibaba Cloud.

Note:

- You must install stream ingest and live streaming demo at two mobiles respective ly, so that one is used for stream ingestion, and meanwhile, the other is used for stream playback.
- Due to restrictions to Wechat and QQ, you can use DingTalk app or a third-party software to scan the QR code for installation.

Get ingest URL and streaming URL

- You can get ingest URL and streaming URL in the new console. For more information, see Configure edge ingestion.
- You can also get ingest URL and streaming URL at the mobile-end demo.

  In Pusher setting, click NEW at the right side of the streaming URL. The system automatically creates a streaming URL, and meanwhile, generates a corresponding QR code of a stream play URL (The stream play URL is automatically copied to the clipboard, you can copy the The stream play URL to the player or scan the QR code for watching). See the following figure:

Configure streaming

In Pusher setting, configure the parameters listed in the page:

Note:
The parameters are not listed here. You can perform streaming operation based on default values. You can also select custom mode in Quality Mode and configure the parameters based on your needs.

Configure stream play

- You can enter the stream play URL that you get from the new ApsaraVideo Live console to perform the stream play operation.
- You can also enter the stream play URL automatically generated by the system, or scan the QR code to perform the stream play operation.

4.3 Stream ingest and live streaming at PC end

You can use stream ingest tools for PC end to push video streams to Alibaba Cloud live center for content processing and distribution. You can set videos that are pushed

to Alibaba Cloud live center based on your needs so that the videos can be used in different scenarios. Perform the following steps to complete stream ingest and playback at PC end.

Prepare tools and environment

Stream ingest and live streaming tools

- Stream ingest tool: You can use OBS stream ingest tool for ingestion. You can download OBS at OBS official download website.
- Live streaming tool: You can use VLC media player to playback video. You can download VLC media player at VLC media player official download website .

Network environment

Network type comparison

Network type	Advantage	Disadvantage
Wired network	Stable	Not convenient
Wi-Fi	Convenient	Not stable

- Wired network is relatively more stable than Wi-Fi, the signal is not easily disturbed. Therefore, we recommend that you use a wired network if conditions permit.
- Wi-Fi is is relatively more convenient than wired network. Therefore, if you perform live activity, we recommend that you use Wi-Fi.

Uplink bandwidth detection

ApsaraVideo Live requires a good network environment which can ensure watching fluency. Uplink bandwidth depends on the video quality and resolution. If the video quality is better, the resolution is higher, and the requirement for the uplink bandwidth is higher. We recommend that you use Speedtest to test the uplink bandwidth condition of your current network.

Note:

We recommend that your uplink bandwidth is not lower than 1Mbps.

Get ingest URL and streaming URL

Perform the following steps to get ingest URL and streaming URL:

1. Add domain names.

   You must have performed ICP filing for your domain names. For more information about adding a domain name, see Add a domain name.

2. Configure the CNAME of a domain name.

   After adding domain names, you must configure CNAME for the ingest domain and the streaming domain. For more information, see Configure CNAME .

3. Associate domain names.

   After adding domain names, you must configure CNAME for the ingest domain and the streaming domain, and associate both domains. For more information, see Associate domain names.

4. Configure authentication.

   Authentication function can protect your live video activities from bootlegging. This function is enabled by default. You can use the default configuration, or you can customize the authentication function.

   - Default authentication: The authentication key is assigned randomly, the expire time is 30 minutes. If the time exceeds expire time, the authentication becomes invalid.
   - Custom authentication: You can also custom authentication based on your needs, such as configure the expire times of the ingest URL and streaming URL. For more information, see Configure authentication.

5. Configure the optional function.
   - You can choose to configure the hotlinking protection function to limit the availability of live video distribution resources. For more information, see Configure hotlinking protection.
   - You can configure IP address blacklist to prevent an IP from accessing your CDN domain name. For more information, see Configure IP address blacklist.
   - You can configure encoding, recording and snapshots based on your needs. For more information, see Configure default encoding, Store recordings to OSS, and Configure snapshots.
   - You can configure HTTPS to prevent the hidden danger of sensitive information from leakage. For more information, see Configure HTTPS.
   - You can also configure notification URL so as to receive prompt feedback when the push streaming succeeds or the stream is disconnected successfully. For more information, see Notification URL.
6. Get ingest UTL and streaming URL.

   You can get ingest URL and streaming URL in ApsaraVideo Live console. For more information, see Configure edge ingestion.

Configure and perform live streaming

Perform the following steps to complete live streaming operations:

1. Install the OBS stream ingest tool you have downloaded.
2. Get the ingest URL.

   You can get the ingest URL in the ApsaraVideo Live console. For more information, see Configure edge ingestion.
3. Configure the basic parameters, and use the streaming URL for streaming operation.

Configure and view stream playback

Perform the following steps to complete stream playback operations:

1. Install the VLC media player you have downloaded.
2. Get the streaming URL.

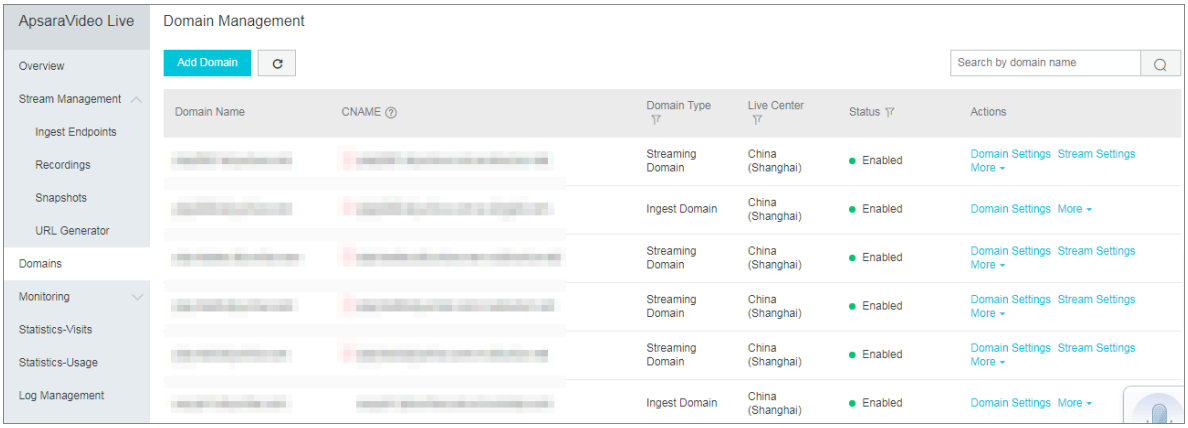
   You can get the streaming URL in the ApsaraVideo Live console. For more information, see Configure edge ingestion.

3. Use the VLC to play the video.

4.4 Stream pulling

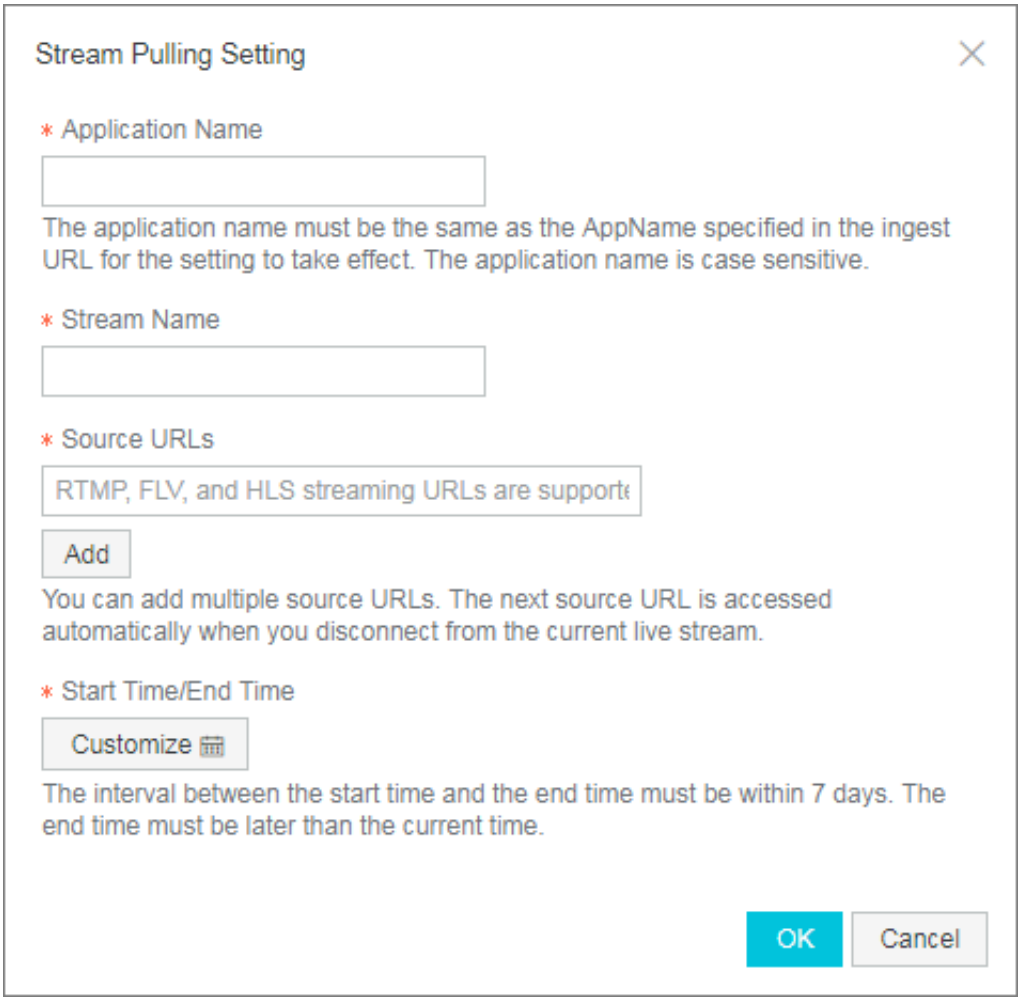
Through the stream pulling, you can pull the third-party live streaming URL to the live center of Alibaba Cloud for content distribution, and push the stream to the desired node.

1. Log on to the ApsaraVideo Live console.
2. Click Domains.
3. Select the Streaming Domain, and click Stream Settings.



4. In the left-side navigation pane, click Stream Pulling Settings.
5. Click Add.

6. In Stream Pulling Settings, enter streaming pulling setting parameters.



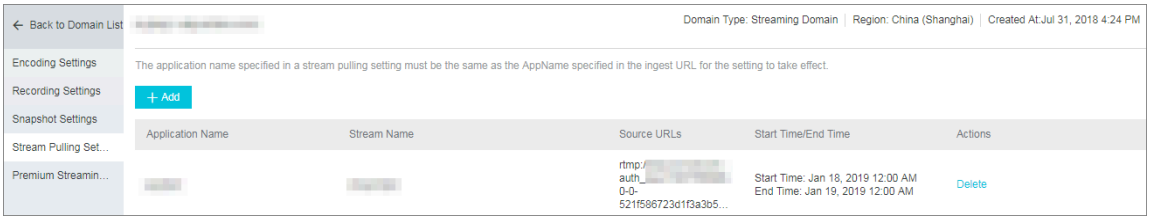
- Application Name: the name of the application.

  When the Application Name must be the same with the Application Name specified in the ingest URL for the setting to take effect.

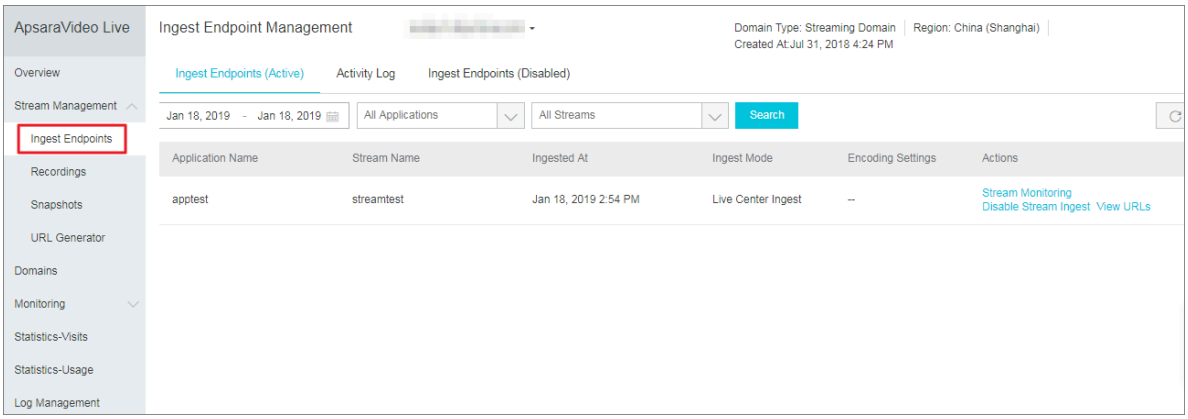
  Note:

Through the live pull-stream, you can pull the third-party live streams to the live center of Alibaba Cloud for content distribution, and push the stream to the desired node.

- **Stream Name: The name of the stream.**
- **Source URLs: the third-party streaming URLs, support one-on-one stream pulling. You can also add multiple source URLs.**
  - **RTMP, HLS, and FLV streaming URLs are supported.**
  - **The next source URL is accessed automatically when you disconnect from the current live stream.**
- **Start Time/End Time: the interval between the start time and the end time must be within 7 days. The end time must be later than the current time.**



After setting the pull-stream, if the third-party streaming URLs have begun to play, you can view the streaming URLs processed in the live center in Stream Management > Ingest Endpoints.



You can also perform recording and encoding operations, and take snapshots of the pull-streams. The operation is the same as the common stream settings. For more information, see Store live recordings to OSS,Configure snapshots, Configure default encoding , and Configure custom encoding.

4.5 Ingest URL and streaming URL

4.5.1 Ingest URL and streaming URL (Original)

Alibaba Cloud’s ApsaraVideo Live service provides stream ingestion and live streaming service which are triggered. You are not required to create resource, but create an ingest domain name and a streaming domain name that have completed ICP filing, CNAME configuration and authorization. And you can quickly get the corresponding ingest URL and streaming URL based on URL splicing rules. This article introduces the splicing method of the ingest URL and the streaming URL of the live activities which do not perform encoding.

Note:

- This article introduces how to get the spliced URLs manually. You can also get the ingest URL and the streaming URL in the console. For more information, see Configure edge ingestion.
- If you want to create multiple live activities , you can also splice the ingest URL and the streaming URL in bulk. For more information , see Create multiple live activities.
- If you configure encoding service for your live activities, for more information about the splicing rules of ingest URL and streaming URL, see Ingest URL and streaming URL (Encoding).
- In this article, the ingest URL and the streaming URL in the example are for your reference only. You can follow the splicing rules to get your own ingest URL and streaming URL by using your ingest domain, streaming domain, Application Name , Stream Name and the authentication string obtained by authentication.

Prerequisites

Perform the following operations to get the authorized ingest URL and streaming URL:

- Add a domain name

  You must first created an ingest domain and a streaming domain that have completed ICP filing. For more information, see Add a domain name.
- Configure CNAME

  After adding a domain, you must configure the CNAME for it to take effect. For more information about how to configure CNAME, see Configure CNAME.

- Associate domain names

  After adding domain names, you must associate the ingest domain and the streaming domain before you perform stream ingestion and live streaming operations. For more information, see Associate domain names.

- Configuration authorization

  The authorization function is enabled by default. We recommend that you keep it enabled; otherwise, a risk of bootlegging may occur. If you want to disable authorization function, contact your business manager or open a ticket You can use the default authorization configuration, or you can customize authorization. For more information, see Configure authentication.

  > Note:
  > If you want to disable the authentication function due to special scenarios, open a ticket. For more information about how to get unauthorized ingest URL and streaming URL, see Ingest URL and streaming URL (Original) and Ingest URL and streaming URL (Encoding).

How do I generate an ingest URL?

- Generation rules of ingest URL

  ApsaraVideo Live service supports ingest URL in RTMP format only.

  The ingest URL format is `RTMP :// ingest domain name / AppName / StreamName ? authentica tion string`

- Example: the ingest domain name is `push . aliyunlive . com` , the Application Name is app, the Stream Name is stream, and the authentication key is 123, then the ingest URL is `RTMP :// push . aliyunlive . com / app / stream ? auth_key = timestamp - rand - uid - md5hash`

How do I generate a streaming URL?

- Generation rules of streaming URL

  Streaming URL support RMTP, FLV, and HLS formats as follows:

  - `RTMP : rtmp :// streaming domain name / AppName / StreamName ? authentica tion string`
  - `FLV : http :// streaming domain name / AppName / StreamName . flv ? authentica tion string`
  - `HLS : http :// streaming domain name / AppName / StreamName . m3u8 ? authentica tion string`

  > **Note:**
  > M3u8 encoding URL is already supported. If you have more requirements, Open a ticket.

- Examples

  For example, the streaming domain name is `play . aliyunlive . com`, the Application Name is app, the Stream Name is stream, and the authentication key is 456, then the streaming URL is:

  - `RTMP : rtmp :// play . aliyunlive . com / app / stream ? auth_key = timestamp - rand - uid - md5hash`
  - `FLV : http :// play . aliyunlive . com / app / stream . flv ? auth_key = timestamp - rand - uid - md5hash`
  - `HLS : http :// play . aliyunlive . com / app / stream . m3u8 ? auth_key = timestamp - rand - uid - md5hash`

4.5.2 Ingest URL and streaming URL (Encoding)

Alibaba Cloud's ApsaraVideo Live service provides stream ingestion and live streaming service which are triggered. You are not required to create resource, but create an ingest domain and a streaming domain that have completed ICP filing, CNAME configuration and authorization. And you can quickly get the corresponding ingest URL and streaming URL based on URL splicing rules. This article introduces the splicing method of the ingest URL and the streaming URL of the live activities which perform encoding.

Note:

- This article introduces how to get the spliced URLs manually. You can also get the ingest URL and the streaming URL in the console. For more information, see Configure edge ingestion.
- If you want to create multiple live activities , you can also splice the ingest URL and the streaming URL in bulk. For more information, see Create multiple live activities.
- If you don't configure encoding service for your live activities, for more information about the splicing rules of ingest URL and streaming URL, see Ingest URL and streaming URL (Original).
- In this article, the ingest URL and the streaming URL in the example are for your reference only. You can follow the splicing rules to get your own ingest URL and streaming URL by using your ingest domain, streaming domain, Application Name , Stream Name and the authentication string obtained by authentication.

Prerequisites

Perform the following operations to get the authorized ingest URL and streaming URL:

- Add a domain name

  You must first created an ingest domain and a streaming domain that have completed ICP filing. For more information, see Add a domain name.
- Configure CNAME

  After adding a domain, you must configure the CNAME for it to take effect. For more information about how to configure CNAME, see Configure CNAME.
- Associate domain names

  After adding domain names, you must associate the ingest domain and the streaming domain before you perform stream ingestion and live streaming operations. For more information, see Associate domain names.
- Configuration authentication

  The authorization function is enabled by default. We recommend that you keep it enabled; otherwise, a risk of bootlegging may occur. If you want to disable authentication function, contact your business manager or open a ticket You can

use the default authentication configuration, or you can customize authentication. For more information, see Configure authentication.

> Note:
> If you want to disable the authentication function due to special scenarios, open a ticket. For more information about how to get unauthorized ingest URL and streaming URL, see Ingest URL and streaming URL (Original) and Ingest URL and streaming URL (Encoding).

How do I get encoding ingest URL?

- Generation rules of ingest URL

  ApsaraVideo Live service supports ingest URL in RTMP format only.

  The ingest URL format is `RTMP :// ingest domain name / AppName / StreamName ? authentica tion string`

- Examples

  Example: the ingest domain is `push . aliyunlive . com`, the Application Name is app, the Stream Name is stream, and the authentication key is 123, then the ingest URL is `RTMP :// push . aliyunlive . com / app / stream ? auth_key = timestamp - rand - uid - md5hash`

How do I get encoding streaming URL?

You must first configure encoding. ApsaraVideo Live supports default encoding and custom encoding. After you configure encoding and obtain the ID, you can generate the encoding streaming URL based on the generation rules.

1. Configure encoding templates.

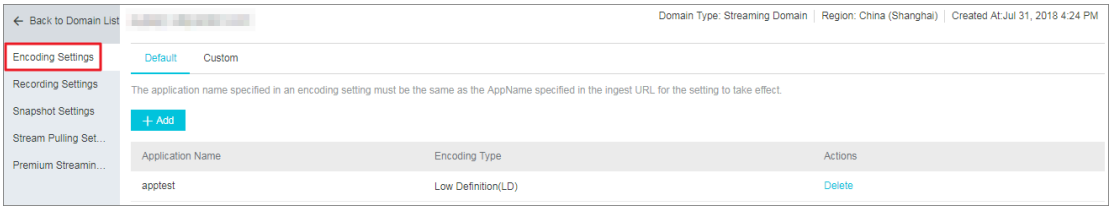
   · Configure default encoding

   a. Log on to the ApsaraVideo Live console.

   b. Click Domains.

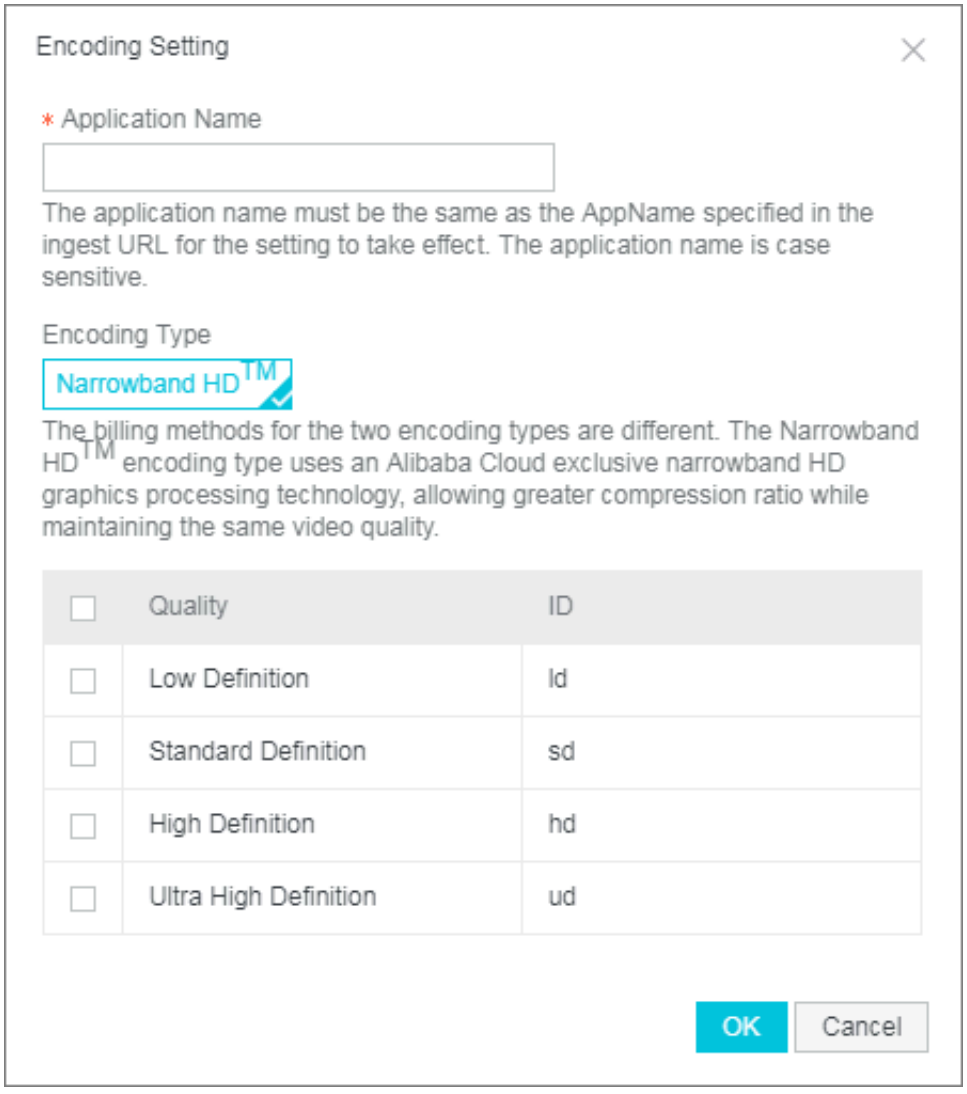
   c. Select the Streaming Domain, and click Stream Settings.

   d. In Encoding Settings, select Default, and click Add.



   e. Enter encoding settings parameters. You can select the corresponding ID based on your settings.

   Narrowband HD™



Note:

For more information about default encoding, see Default encoding.

- Configure custom encoding

  a. Log on to the ApsaraVideo Live console.

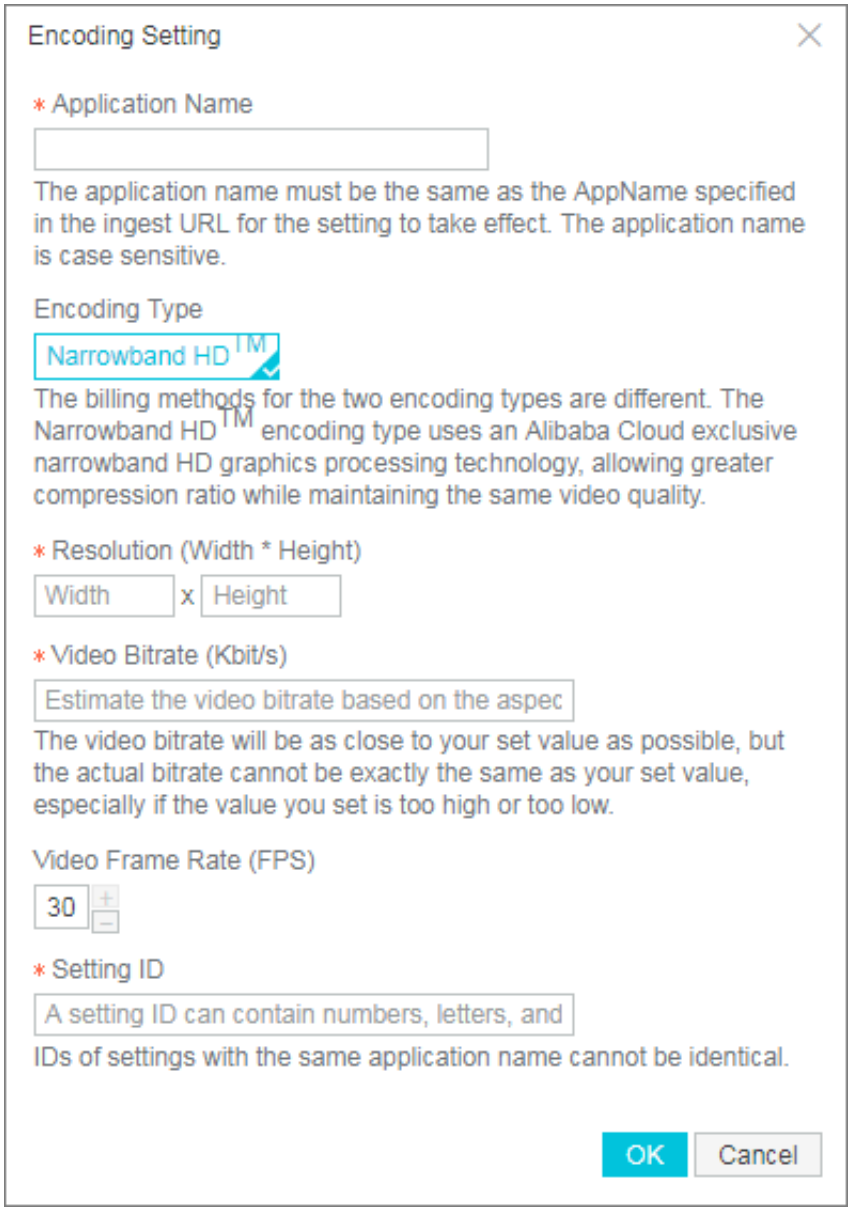
  b. Click Domains.

  c. Select the Streaming Domain, and click Stream Settings .

  d. In Encoding Settings, select Custom, and click Add.

  e. Enter encoding setting parameters. You can select the corresponding ID based on your configuration.

  Narrowband HD™Template



Note:

For more information about custom encoding, see Custom encoding.

2. Get ID.
   - Get the ID in the ApsaraVideo Live console.

     You can obtain the corresponding template ID by following the previous steps.
   - Get the ID by using API.

     You can call the `DescribeLi veStreamTr anscodeInf o` interface, and the system returns the template ID. For more information, see DescribeLi veStreamTranscodeInfo.

     In addition, users can customize encoding settings based on added fields. For more information about getting custom ID, see AddCustomLiveStreamT ranscode.
3. Generation rules of encoding URL.
   - Streaming URL supports RMTP, FLV, and HLS formats. For encoding URLs in different formats, you must add `_templatei d` following `StreamName` .
     - RTMP format: `rtmp :// streaming domain name / AppName / StreamName { _templatei d }? authentica tion string`
     - FLV format: `http :// streamingd omain / AppName / StreamName { _templatei d }. flv ? authentica tion string`
     - HLS format: `http :// streamingd omain / AppName / StreamName { _templatei d }. m3u8 ? authentica tion string`

       Note:

M3u8 encoding URL is already supported. If you have more requirements, Open a ticket.

- Examples

  For example, the streaming domain name is `play.aliyunlive.com`, the Application Name is app, the Stream Name is stream, and the authentication key is 456, then the streaming URL is:

  - RTMP-based streaming URL `rtmp://play.aliyunlive.com/app/stream_sd?auth_key=timestamp-rand-uid-md5hash`
  - FLV-based streaming URL `http://play.aliyunlive.com/app/stream_sd.flv?auth_key=timestamp-rand-uid-md5hash`
  - HLS-based streaming URL `http://play.aliyunlive.com/app/stream_sd.m3u8?auth_key=timestamp-rand-uid-md5hash`

Authentication field description, see Democode.

Field	Description
timestamp	expire time, positive integer, fixed length 10, seconds measured from 1970-01-01. Used to control expire time, integer of 10 digits, expire time 1800s.
rand	random number, we recommend that you use UUID (not including hyphen "-", for example, 477b3bbc253f467b8def6711128c7bec format)
uid	not used yet (set to 0)
md5hash	verification string calculated according to md5 algorithm, lowercase letters and digits (0-9 and a-z) are supported, fixed length 32

4.6 Ingest URL and streaming URL (Not authenticated)

4.6.1 Ingest URL and streaming URL (Original)

The authentication function must be disabled in some special scenarios. This article introduces how to get unauthenticated ingest URL and streaming URL(original).

> Note:
>
> - This article introduces how to get the spliced URLs manually. You can also get the ingest URL and the streaming URL in the console. For more information, see Configure edge ingestion.
> - If you want to create multiple live activities , you can also splice the ingest URL and the streaming URL in bulk. For more information , see Create multiple live activities.
> - If you configure encoding service for your live activities, for more information about the generation rules of ingest URL and streaming URL, see Ingest URL and streaming URL (Encoding).
> - In this article, the ingest URL and the streaming URL in the example are for your reference only. You can follow the generation rules to get your own ingest URL and streaming URL by using your ingest domain name, streaming domain name , Application Name, Stream Name and the authentication string obtained by authentication.

Prerequisites

Perform the following operations to get the ingest URL and streaming URL:

- Add a domain name

  You must first created an ingest domain and a streaming domain that have completed ICP filing. For more information, see Add a domain name.
- Configure CNAME

  After adding a domain name, you must configure the CNAME for it to take effect. For more information about how to configure CNAME, see Configure CNAME.
- Associate domain names

  After adding domain names, you must associate the ingest domain and the streaming domain before you perform push streaming and live streaming operations. For more information, see Associate domain names.

How do I generate original streaming URL?

The streaming URLs are divided into original streaming URL and encoding streaming URL. Original streaming URL is the original video stream without encoding. The splicing rule of URL is `Streaming Domain Name + AppName + StreamName`

- Splicing rules of streaming URL

  The streaming URL supports rtmp, FLV, and m3u8 formats as follows:

  - `RTMP format : rtmp :// Streaming Domain Name / AppName / StreamName`
  - `FLV format : http :// Streaming Domain Name / AppName / StreamName . flv`
  - `M3U8 format : http :// Streaming Domain Name / AppName / StreamName . m3u8`

- Examples

  For example, the streaming domain name is `play . aliyunlive . com` , the Application Name is app, the Stream Name is stream, and the authentication key is 456, then the streaming URL is:

  - `RTMP format : rtmp :// play . aliyunlive . com / app / stream`
  - `FLV format : http :// play . aliyunlive . com / app / stream . flv`
  - `M3U8 format : http :// play . aliyunlive . com / app / stream . m3u8`

  > **Note:**
  > M3u8 encoding URL is already supported. If you have more requirements, Open a ticket.

How do I generate an ingest URL?

- Generation rules of ingest URL

  ApsaraVideo Live service supports ingest URL in RTMP format only.

  The ingest URL format is `RTMP :// Ingest Domain Name / APPName / StreamName`

- Examples

  Example: the ingest domain is `push . aliyunlive . com` , the Application Name is app, the Stream Name is stream, and the authentication key is 123, then the ingest URL is `RTMP :// push . aliyunlive . com / app / stream`

4.6.2 Ingest URL and streaming URL (Encoding)

In some special scenarios, the authentication operation must be disabled. This article introduces how to splice the encoding streaming URL and the corresponding ingest URL when the authentication function is disabled.

Note:

- This article introduces how to get the spliced URLs manually. You can also get the ingest URL and the streaming URL in the console. For more information, see Configure edge ingestion.
- If you want to create multiple live activities , you can also splice the ingest URL and the streaming URL in bulk. For more information , see Create multiple live activities.
- If you don't configure encoding service for your live activities, for more information about the splicing rules of ingest URL and streaming URL, see Ingest URL and streaming URL (Original).
- In this article, the ingest URL and the streaming URL in the example are for your reference only. You can follow the splicing rules to get your own ingest URL and streaming URL by using your ingest domain, streaming domain, Application Name , Stream Name and the authentication string obtained by authentication.

Prerequisites

Perform the following operations to get the ingest URL and streaming URL:

- Add a domain name

  You must first created an ingest domain and a streaming domain that have completed ICP filing. For more information, see Add a domain name.
- Configure CNAME

  After adding a domain, you must configure the CNAME for it to take effect. For more information about how to configure CNAME, see Configure CNAME.

- Associate domain names

  After creating domain names, you must associate the ingest domain and the streaming domain before you perform stream ingestion and live streaming operations. For more information, see Associate domain names.

How do I get encoding ingest URL?

- Generation rules of ingest URL

  ApsaraVideo Live service supports ingest URL in RTMP format only.

  The ingest URL format is `RTMP :// Ingest Domain nName / AppName / StreamName`

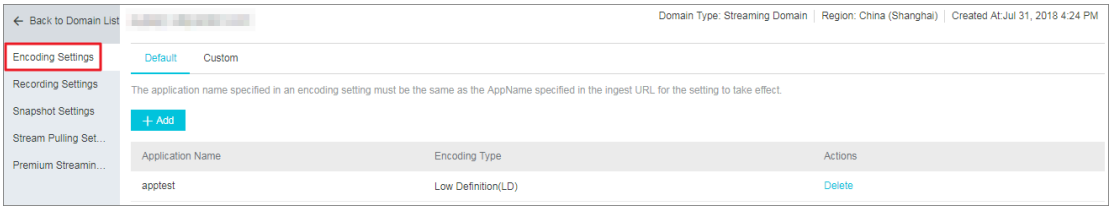
- Examples

  For example, the Ingest Domain Name is `push . aliyunlive . com`, Application Name is app, Stream Name is stream, and the ingest URL is `RTMP :// push . aliyunlive . com / app / stream`

How do I get encoding streaming URL?

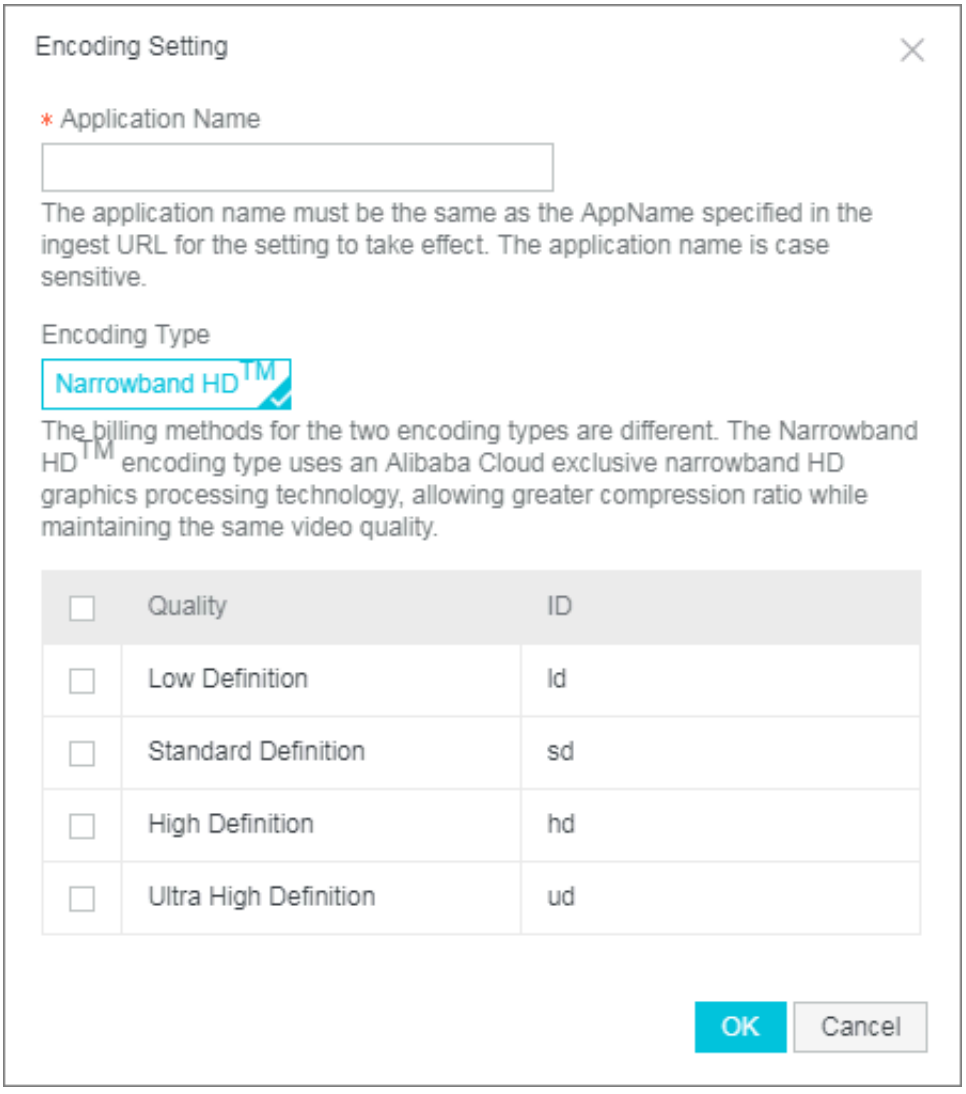
You must first configure encoding. ApsaraVideo Live supports universal encoding and custom encoding. Each encoding provides Narrowband HD™. After you configure encoding and obtain the template ID, you can splice the encoding streaming URL based on the splicing rules.

1. Configure encoding templates.
   - Configure default encoding
     a. Log on to the ApsaraVideo Live console.
     b. Click Domains.
     c. Select the Streaming Domain, and click Stream Settings.
     d. In Encoding Settings, select Default, and click Add.



     e. Enter encoding settings parameters. You can select the corresponding ID based on your configuration.

Narrowband HD™



Note:

For more information, see Default encoding.

- Configure custom encoding

  a. Log on to the ApsaraVideo Live console.

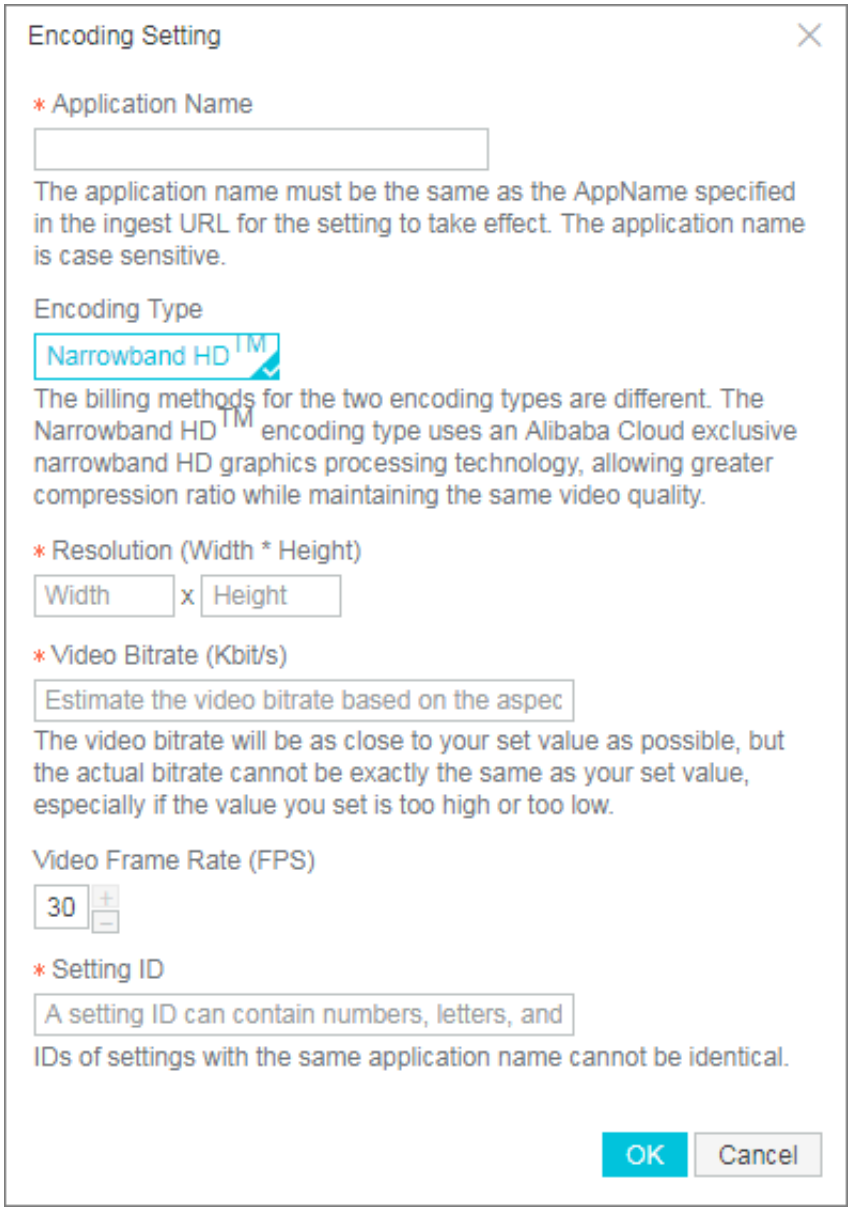
  b. Click Domains.

  c. Select the Streaming Domain, and click Stream Settings.

  d. In Encoding settings, select Custom, and click Add.

  e. Enter the encoding setting parameters. You can select the corresponding ID based on your configurations.

  Narrowband HD™



Note:

For more information about custom encoding, see Custom encoding.

2. Get ID.
   - Get the ID in the ApsaraVideo Live console.

     You can obtain the corresponding template ID by following the previous steps.
   - Get the ID by using API.

     You can call the `DescribeLi veStreamTr anscodeInf o` interface, and the system returns the ID. For more information, see DescribeLiveStreamTranscodeInfo.

     In addition, users can customize template based on added fields. For more information about getting custom ID, see AddCustomLiveStreamTranscode.
3. Splicing rules of encoding URL.
   - Streaming URL supports RMTP, FLV, and HLS formats. For encoding URLs in different formats, you must add `_templatei d` following `StreamName`.
     - RTMP format: `: rtmp :// Streaming Domain Name / AppName / StreamName { _templatei d }?`
     - FLV format: `http :// Streaming Domain Name / AppName / StreamName { _templatei d }. flv ?`
     - HLS format: `http :// Streaming Domain Name / AppName / StreamName { _templatei d }. m3u8 ?`
   - Examples

     For example, the Streaming Domain Name is `play . aliyunlive . com`, the Application Name is app, the Stream Name is stream, and the authentication key is 456, then the streaming URL is:
     - RTMP-based streaming URL `rtmp :// play . aliyunlive . com / app / stream_sd`
     - FLV-based streaming URL `http :// play . aliyunlive . com / app / stream_sd . flv ?`
     - HLS-based streaming URL `http :// play . aliyunlive . com / app / stream_sd . m3u8`

     Note:

M3u8 encoding URL is already supported. If you have more requirements, Open a ticket.

4.7 Create multiple live activities

A live video activity requires an ingest URL. Alibaba Cloud ApsaraVideo Live supports creating activity of a triggered type. You can create multiple live activities on the basis of the activity creation rules without using APIs.

Note:
Terms in the console have been updated, and we will update the documentation as soon as possible. We are sorry for any inconvenience caused.

Descriptions

Ingest URL can be created in batches according to the rules, and live activities can be performed simultaneously. When performing multiple live activities, note that each domain can process a limited number of concurrent streams. A maximum of 20 concurrent streams and 10 encoding streams are allowed for each domain name. Therefore, before performing live activities in batches, you must check whether the current stream limitation meets your requirements. If it does not meet your requirements, You can contact us by Opening a ticket.

Create multiple ingest URLs

A live video service URL consists of three levels of live video management units, namely the domain name (Domain), application (APPName) and live stream (StreamName). You can create multiple applications (APPName) under each domain name (Domain), and multiple live streams (StreamName) under each application.

Note:
For more information about the generation rules of the ingest URL, see Ingest URL and streaming URL.

AppName and StreamName can be customized. Different values generate different ingest URL and streaming URLs.

- You can create multiple live streams under one app.

  Examples

  For example, an application is named "live", you can create multiple live streams under "live". The ingest URL is:

  rtmp://Ingest Domain Name/{live}/{1}? authentication string

  rtmp//Ingest Domain Name/{live}/{2}? authentication string

  rtmp://Ingest Domain Name/{live}/{3}? authentication string

  > Note:
  > The authorization string is an encrypted string obtained based on the authentication algorithm.

- You can also create multiple live streams for the application.

  > Note:
  > ApsaraVideo Live determines whether the live stream is unique based on stream name (StreamName) instead of application name (AppName). If you set a different application name, you must also make sure that the stream name is different to ensure that the final live stream is different.

  Examples

  rtmp://Ingest Domain Name/{live1}/{Stream1}? authentication string

  rtmp://Ingest Domain Name/{live2}/{Stream2}? authentication string

  rtmp://Ingest Domain Name/{live3}/{Stream3}? authentication string

Create multiple streaming URLs

The rules of streaming URLs and the rules of ingest URLs are the same, and the application name (AppName) and stream name (StreamName) of the streaming URLs correspond to the application name (AppName) and stream name (StreamName) of the ingest URLs.

> Note:
> For more information about the generation rules of a single streaming URL, see Ingest URL and streaming URL.

Examples

The ingest URL is:

rtmp://Ingest Domain Name/{live}/{3}? authentication string

The corresponding streaming URL is:

http://Streaming Domain Name/{live}/{3}?authentication string

http://Streaming Domain Name/{live}/{3}.flv?authentication string

http://Streaming Domain Name/{live}/{3}.m3u8?authentication string

How do I get a URL after I enable encoding?

Default encoding

The streaming URL is spliced by using different parameters. The encoding streaming URL consists of the original URL and template IDs.

URL format is `Streaming Domain Name` + `AppName` + `StreamName` + `_` + `Template name`.

Template name	LD	SD	HD	UHD
Narrowband HD™ template ID	ld	sd	hd	ud

Examples

If the template name of the standard template is sd, you can create streaming URLs in batches as follows:

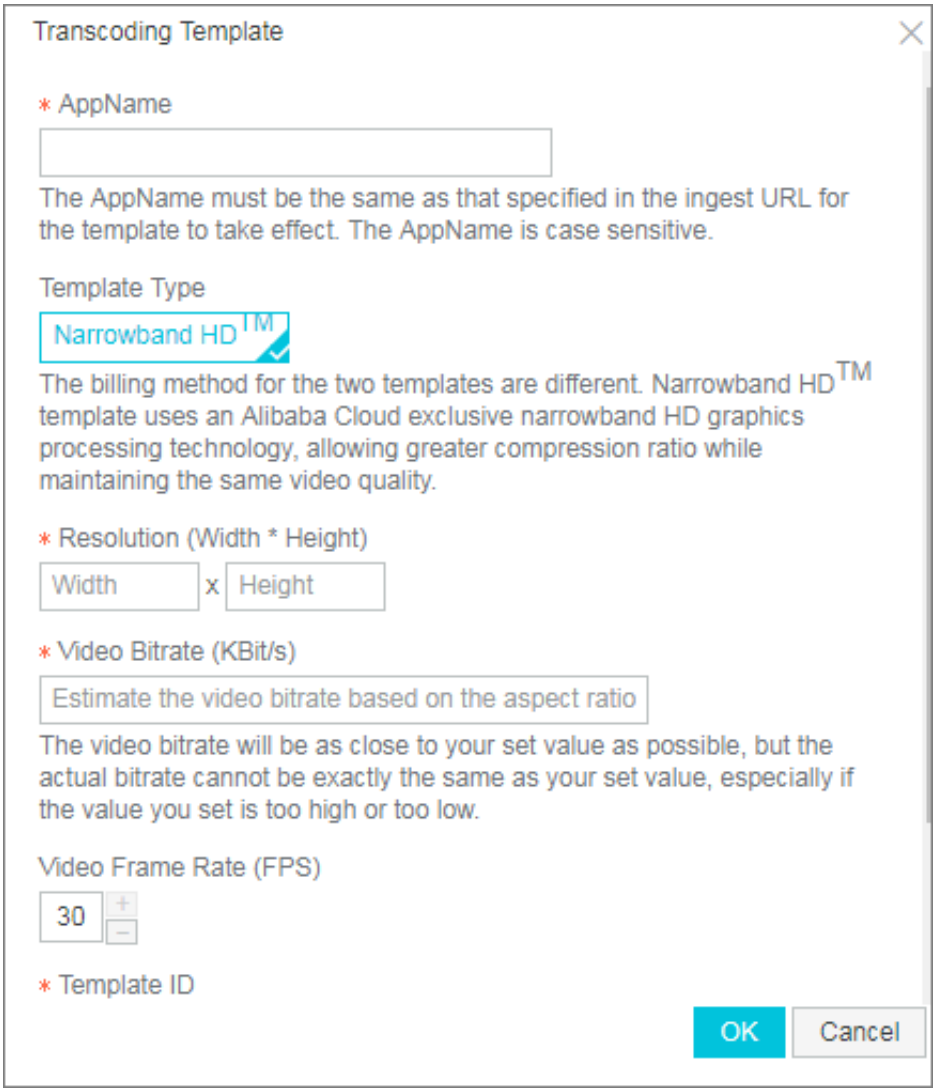
RTMP format: rtmp://Streaming Domain Name/{AppName}/{StreamName} _sd? authentication string

FLV format: http://Streaming Domain Name/{AppName}/{StreamName} _sd.flv? authentication string

HLS format: http://Streaming Domain Name/{AppName}/{StreamName} _sd.m3u8? authentication string

Custom encoding

You can also customize encoding as needed. You must configure the template name of custom encoding Template ID in the console.



The splicing rules of multiple streaming URLs are as follows:

RTMP format: rtmp://Streaming Domain Name/{AppName}/{StreamName} _templateID? authentication string

FLV format: http://Streaming Domain Name/{AppName}/{StreamName} _templateID.flv? authentication string

HLS format: http://Streaming Domain Name/{AppName}/{StreamName} _template ID.m3u8? authentication string

5 Transcoding management

5.1 Universal Transcoding

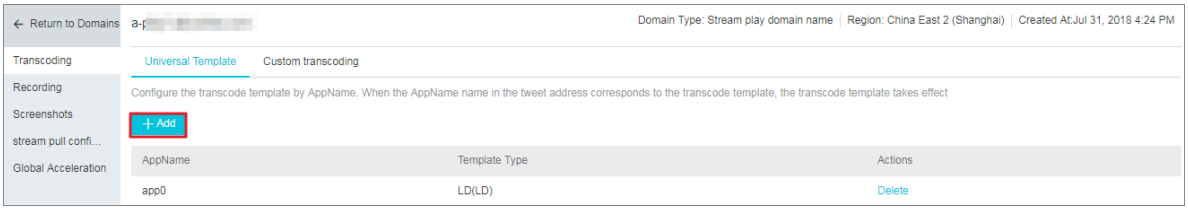
This article introduces the universal transcoding service.

> **Note:**
> Terms in the console have been updated, and we will update the documentation as soon as possible. We are sorry for any inconvenience caused.

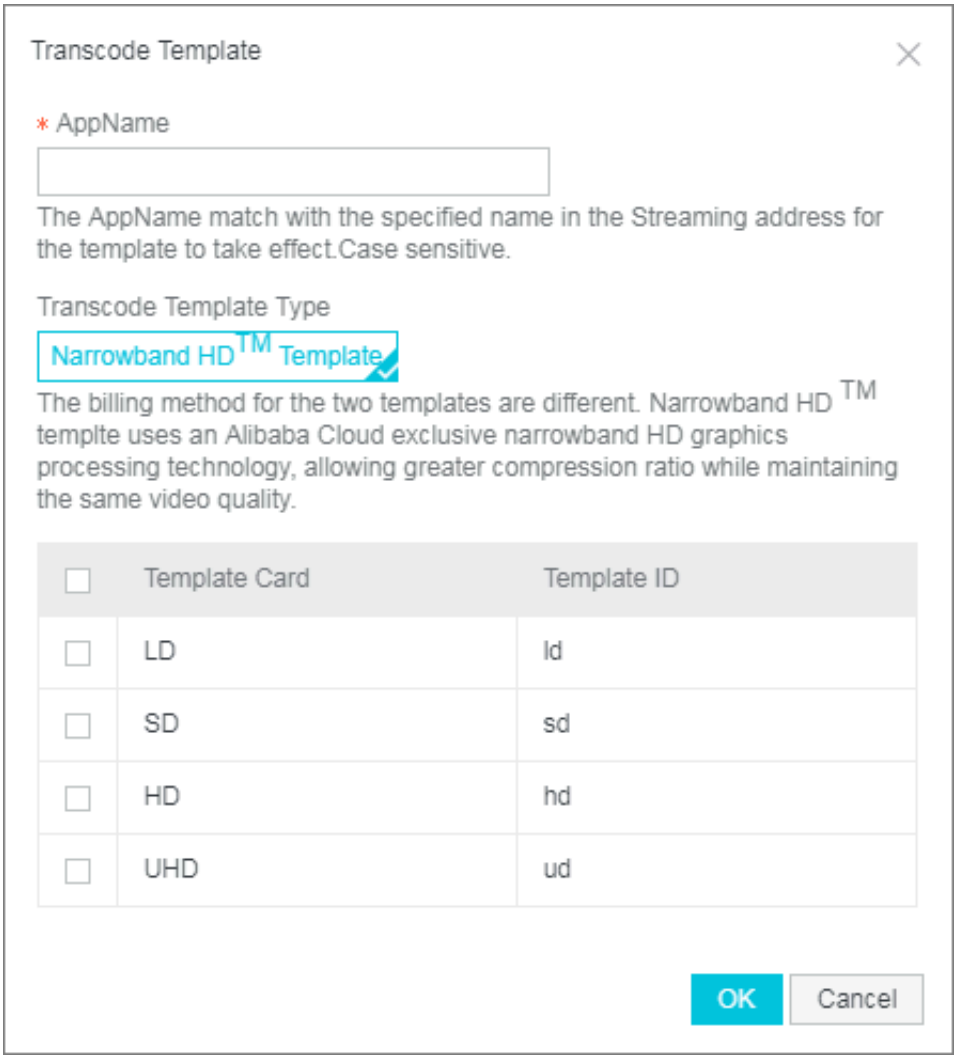
The ApsaraVideo Live console currently supports Narrowband HD™ Template. For more information about the transcoding URL splicing rules, see Ingest URL and streaming URL (Transcoding).

1. Log on to the ApsaraVideo Live console.
2. Click Domain Names.
3. Select the Streaming Domain Name, and click Manage Templates.

4. In Transcoding, select Universal Transcoding.
5. Click Add.



6. In Transcoding Template, enter transcoding templates, and click OK.



- Enter the AppName name. AppName must correspond to the AppName of the ingest URL so that the transcoding template takes effect.
- Select the Template Type , and the Template Name.

> **Note:**
>
> - Template Type is Narrowband HD™ Template. LD, SD, HD, and UHD are available.
> - You can select multiple items in Template Name. You can select only one Template Type.
> - The Template ID is a parameter of the spliced transcoding URL. For more information about splicing rules, see Ingest URL and streaming URL (Transcoding).

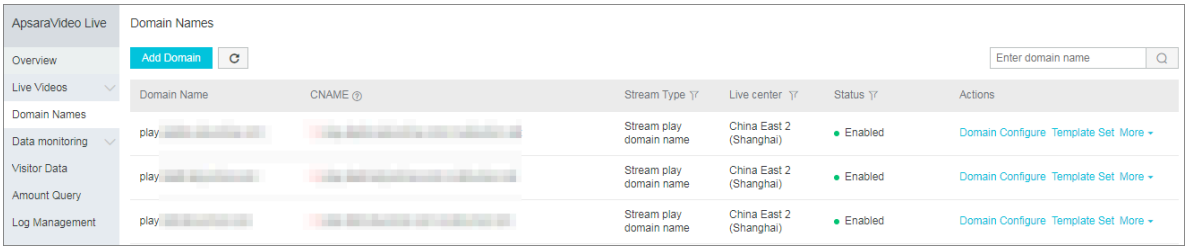
5.2 Custom transcoding

> **Note:**
> Terms in the console have been updated, and we will update the documentation as soon as possible. We are sorry for any inconvenience caused.

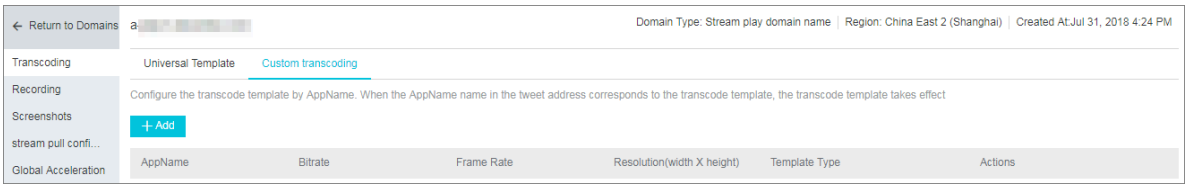
Configure custom transcoding

You can customize the transcoding resolution, frame rate, bit rate, and other parameters based on your actual video output requirements.

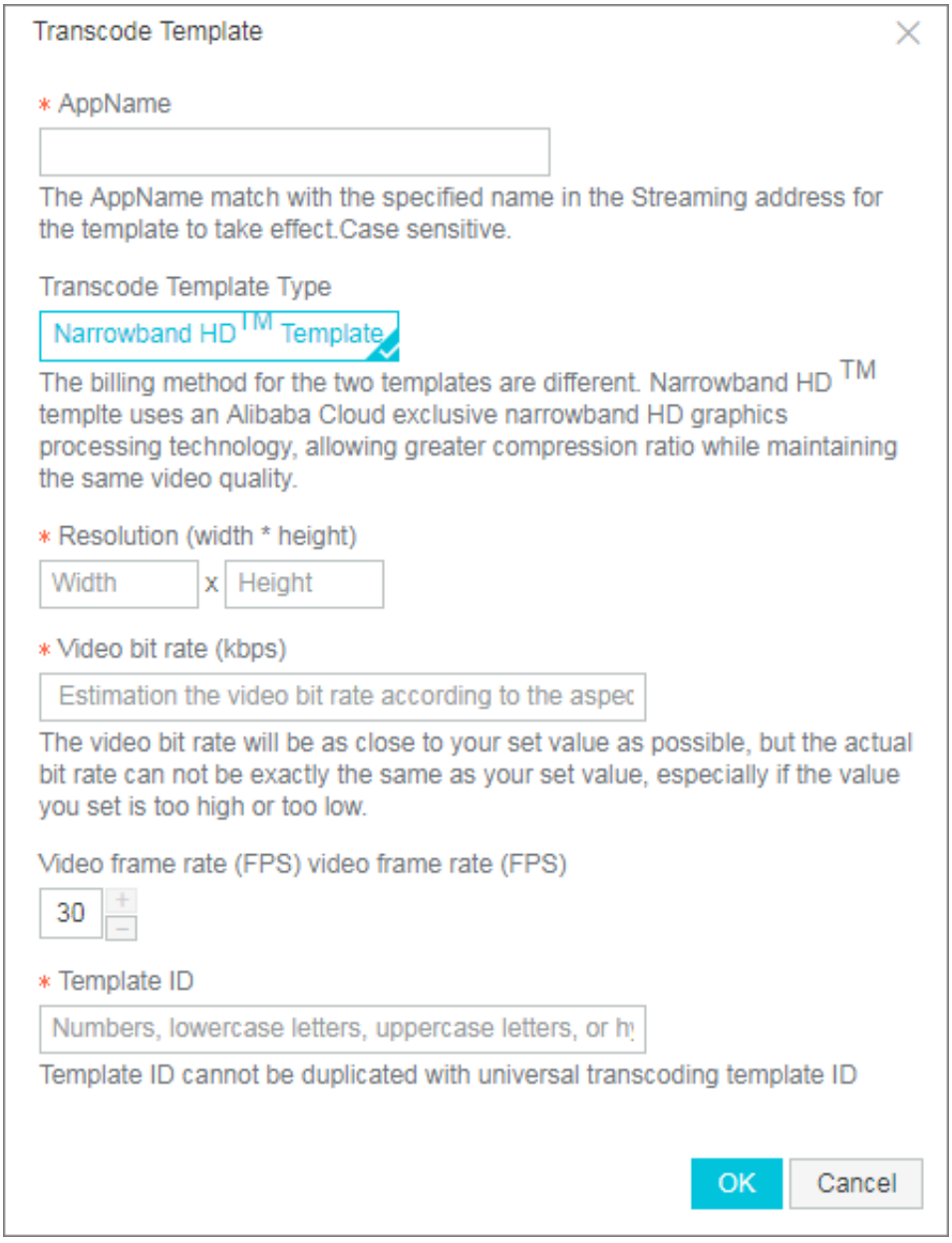
1. Log on to the ApsaraVideo Live console.
2. Click Domain Names.
3. Select the Streaming Domain Name, and click Manage Templates.



4. In Transcoding, select Custom Transcoding, and click Add.



5. In Transcoding Template, add custom transcoding parameters.



- AppName: The application name of the transcoding templates.

  AppName can be the same under the same domain name and in the same template type, but the Template ID cannot be the same.
- Resolution: the resolution of the output video.
  - Different resolution levels correspond to different prices. The resolution levels are as follows:
    - LD: (640x480) and below
    - SD: (1280x720) and below
    - HD: (1920x1080) and below

■ 2K: (2560x1440) and below

■ 4K: (3840x2160) and below

- Resolution level determination rules: The output specifications are determined by whether the long and short edges of the output video resolution fall within the range defined by the output specifications. Take the output specification SD (1280x720) as an example:

  ■ If the long edge of the resolution of the output video is less than or equal to 1280, and the short edge is less than or equal to 720, the video belongs to the output specification.

  ■ If the long edge of the resolution of the output video exceeds 1280, or the short edge exceeds 720, this output video belongs to a higher specification.

- After adding the template, you can access the transcoding stream of a specified resolution by adding Template ID parameter at the end of the output streaming URL.

· Video Bitrate: The Bitrate specified by the resolution.

The bit rate are as follows:

- LD: 100 ~ 800kbps
- SD: 200 ~ 1500kbps
- HD: 500 ~ 4000kbps
- 2K: 2000 ~ 8000kbps
- 4K: 4000 ~ 30000kbps

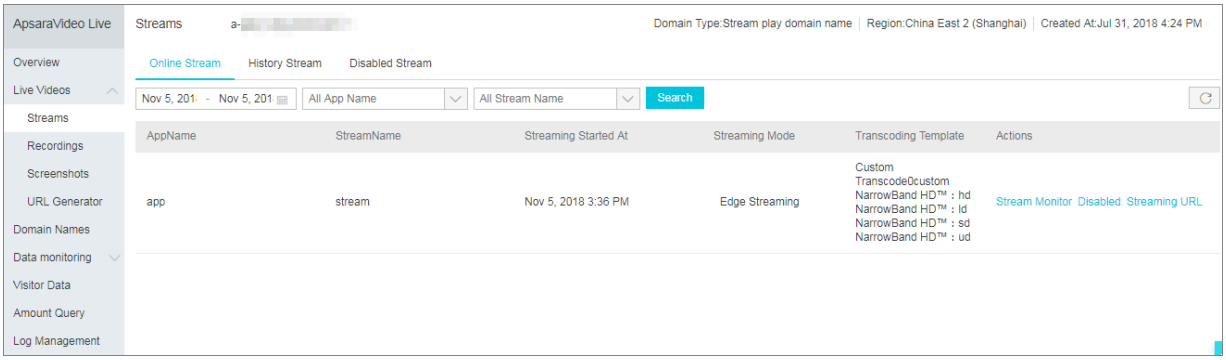
· Video Frame Rate : The output video frame rate, the value of which is less than or equal to the input video frame rate.

· Template ID: The ID of the transcoding template.

> Note:
> Template ID is included in the streaming URL. When you customize template ID, we recommend that you do not configure a template ID different from the template ID of the universal transcoding.

View custom transcoding

You can view which transcoding template are used in the current streams in Streams.


ApsaraVideo Live
Overview
Live Videos
Streams
Recordings
Screenshots
URL Generator
Domain Names
Data monitoring
Visitor Data
Amount Query
Log Management
Streams
a-
Domain Type:Stream play domain name | Region:China East 2 (Shanghai) | Created At:Jul 31, 2018 4:24 PM
Online Stream
History Stream
Disabled Stream
Nov 5, 201 - Nov 5, 201
All App Name
All Stream Name
Search
AppName
StreamName
Streaming Started At
Streaming Mode
Transcoding Template
Actions
app
stream
Nov 5, 2018 3:36 PM
Edge Streaming
Custom
Transcode0custom
NarrowBand HD™ : hd
NarrowBand HD™ : ld
NarrowBand HD™ : sd
NarrowBand HD™ : ud
Stream Monitor
Disabled
Streaming URL

6 Recording management

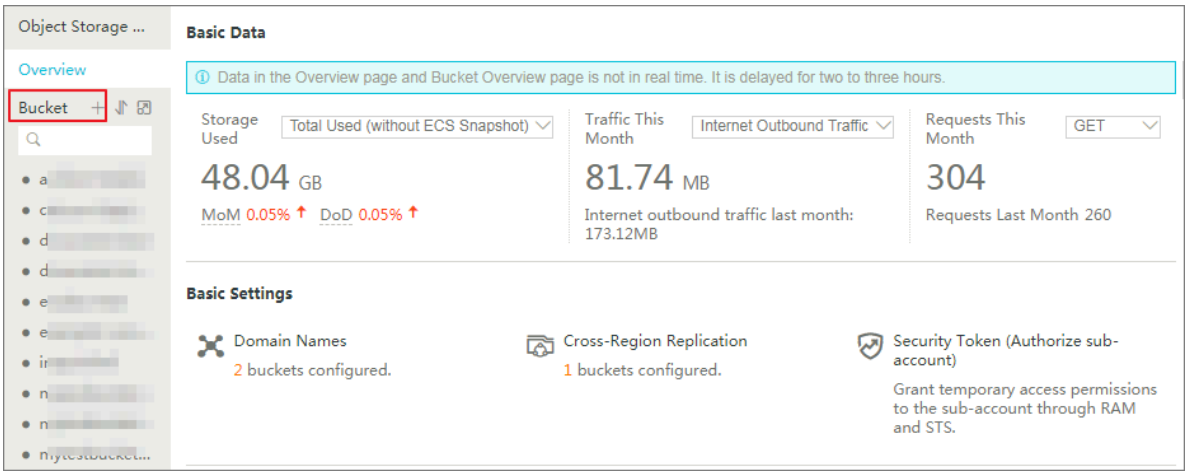
6.1 Save live recordings to OSS

6.1.1 Configure OSS

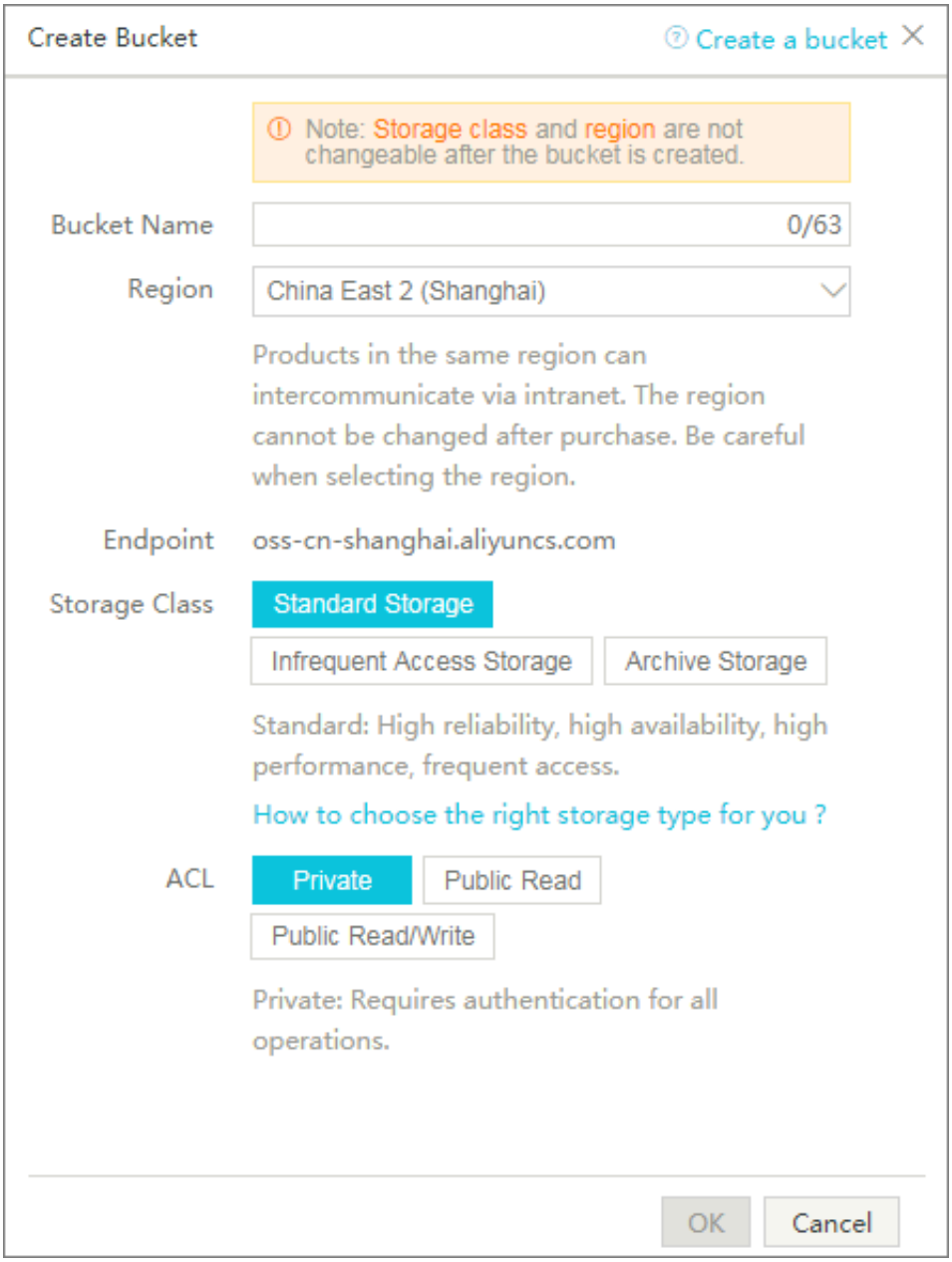
If you want to store live recorded files in the OSS product, you need to create the OSS bucket first, and grant the right to write to the OSS live, in order to view, download, play, and so on in the OSS list.

Create an OSS bucket

1. Log on to the OSS console.
2. Click + following Bucket.



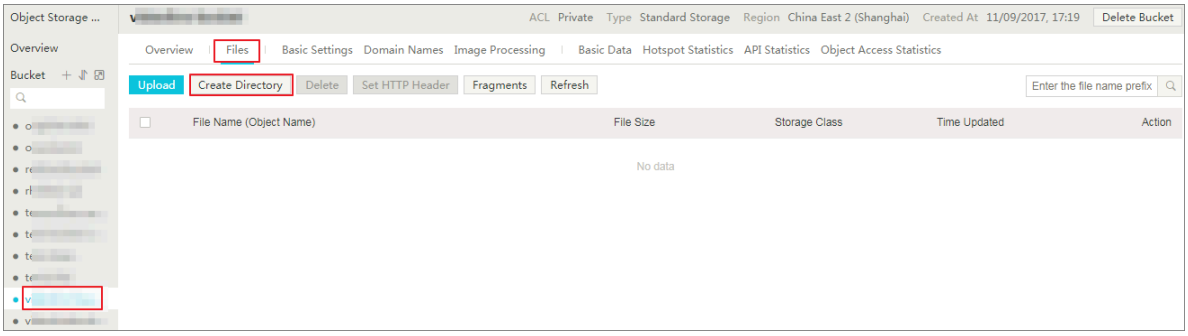
3. Enter Bucket information.



Note:

After the bucket is created, check that the region of the bucket is consistent with that of the live video domain name. For example, the region of the live video domain name is China East 2 (Shanghai), you must also select China East 2 (Shanghai) as the region of the bucket. You can also create bucket folders as needed.

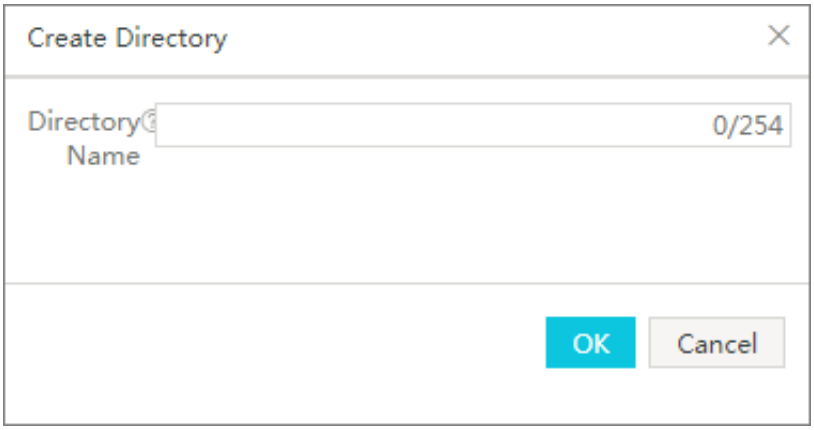
4. In the left-side buckets list, click the bucket you created, and click Files > Create Directory.



Note:

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

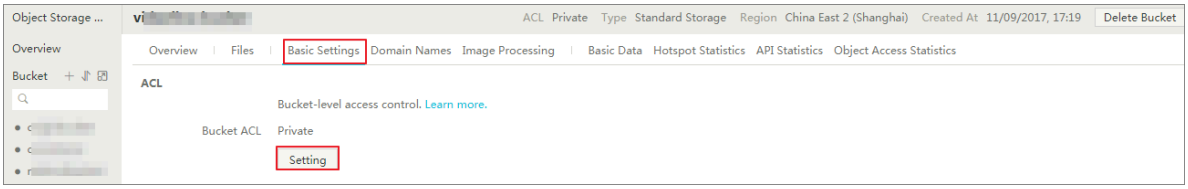
5. In Create Directory, enter Directory Name, and click OK.



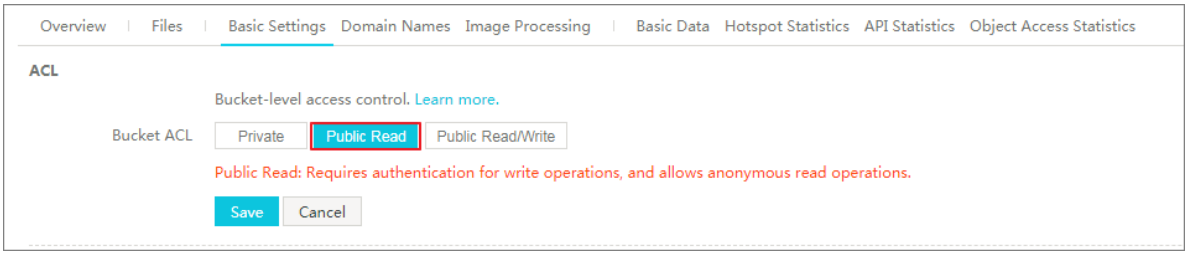
Configure OSS Access Control List (ACL)

If you want to read video information from OSS, we recommend that you configure the OSS bucket ACL as Public Read. The specific access authorization depends on your needs.

1. Log on to the OSS console.
2. In buckets list, select the bucket you created, and click Basic Settings.
3. Click Settings following Bucket ACL.



4. Select Public Read, and clickSave.



Note:

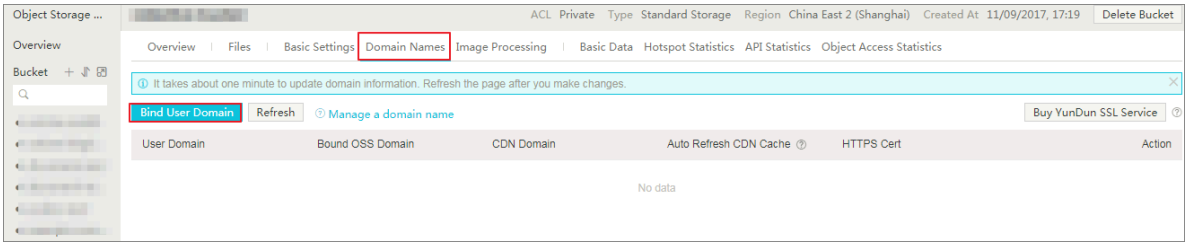
You must first complete real-name registration, if you want to configure the bucket ACL.

After completing configuration, you can log on to the ApsaraVideo Live console > Live Videos > Recordings to preview live recordings.

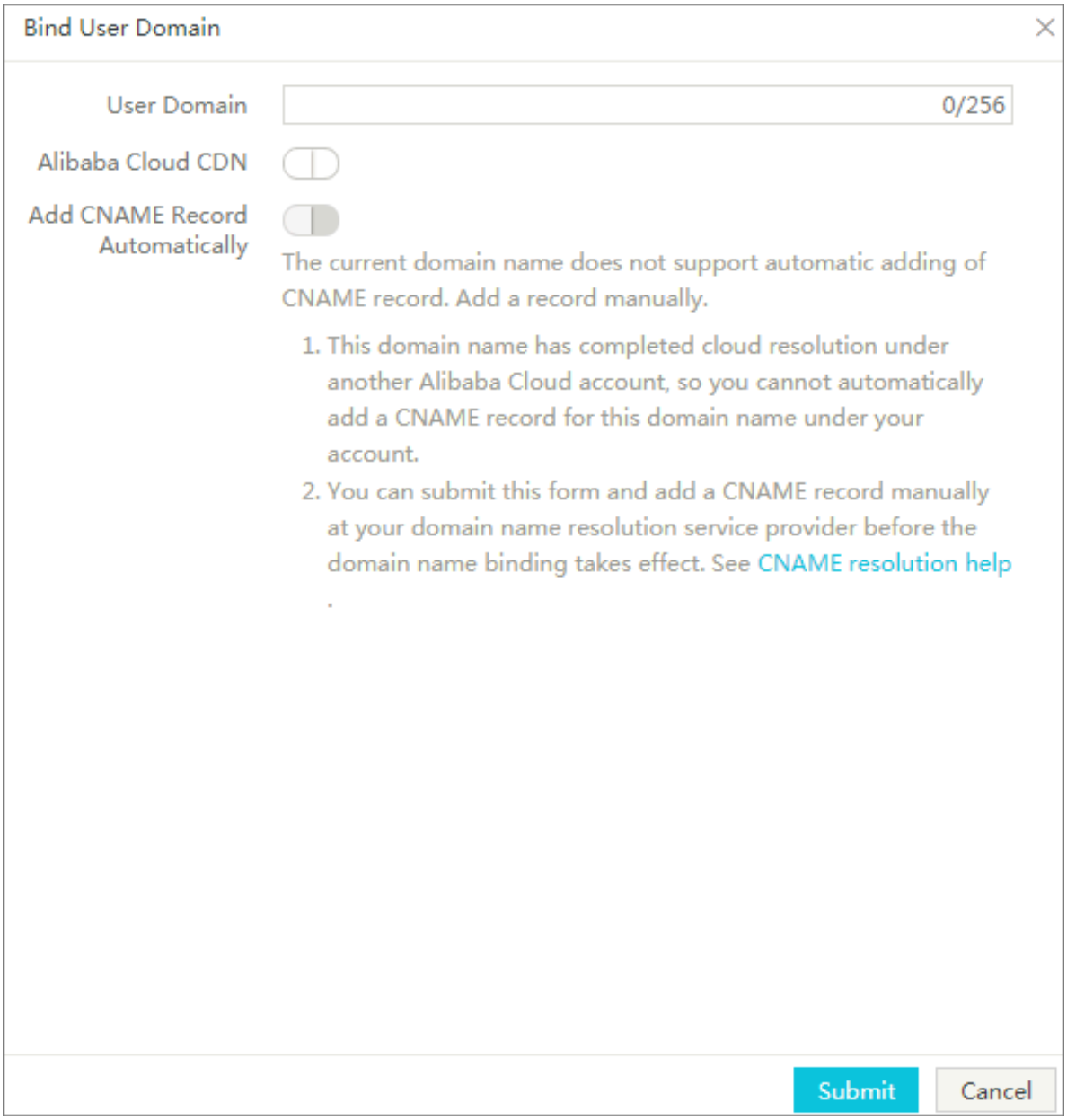
Configure CDN domain name

If the live recordings are stored to OSS, you can configure a CDN domain name to perform CDN acceleration when you view live recordings. CDN delivers videos stored to OSS to nodes in China. Users access the nearest CDN node to read files without accessing the source files in OSS, which does not consume OSS Internet traffic. By using CDN, the access rate and experience of 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.

1. In the page of the bucket you created, click Domain Names > Bind User Domain.



2. In Bind User Domain, configure CDN domain name, and click Submit.



If you just store your live recordings, you are not required to configure a CDN domain name.

> **Note:**
> CDN domain name and the live video domain name must be different. We recommend that you configure the CDN domain name and the live video domain name respectively.

6.1.2 Store live recordings to OSS

ApsaraVideo Live allows you to record source video streams. It supports m3u8 (.ts fragment files), mp4, and flv format, along with recording duration configurations.

Video files are stored in the bucket you specify in OSS. After a streaming ends, a recording index file for the streaming is generated automatically (m3u8, mp4, or flv files). The service also supports the generation of custom recording index files based on your specified recording start time and end time.

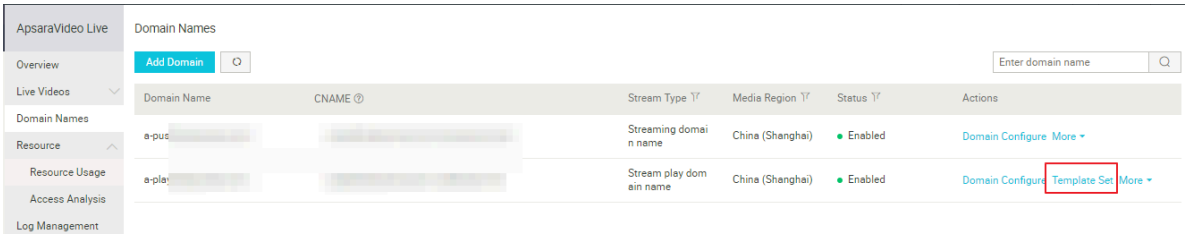
Under a live video CDN domain name, the live recording configurations are differentiated by the AppName and StreamName. That is, streams under the sameAppName and StreamName all perform recording operations following the configurations for this AppName and StreamName.

Introduction

- To facilitate the playback of your recorded content, you can store the live recordings to OSS.
- To store live recordings to OSS, you must first enable OSS service, and provides ApsaraVideo Live service with the access authorization of writing in OSS. Then you can store videos in specific OSS bucket. For more information, see Configure OSS.
- To avoid recorded files abnormally cut off due to network jitter or temporary stream disconnection during live recording, the system disconnects the stream until 180s. That is, if you perform another streaming operation within 180s after stream disconnection, the system judges it as the same stream by default; if the time interval exceeds 180s, the system judges it as two different streams.

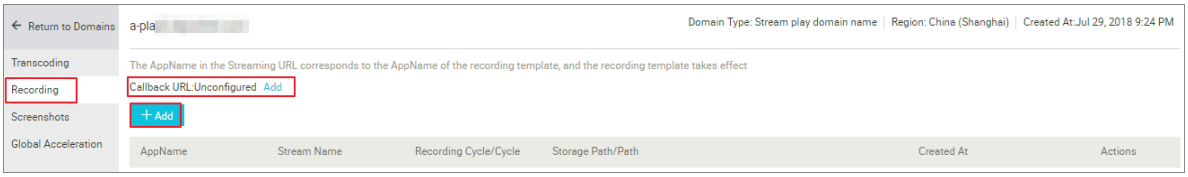
Create live recordings

1. Log on to theApsaraVideo Live console.
2. Click Domain Names..
3. Select the stream play domain name, and click Template Set.



4. In the left-side navigation pane, click Recording.

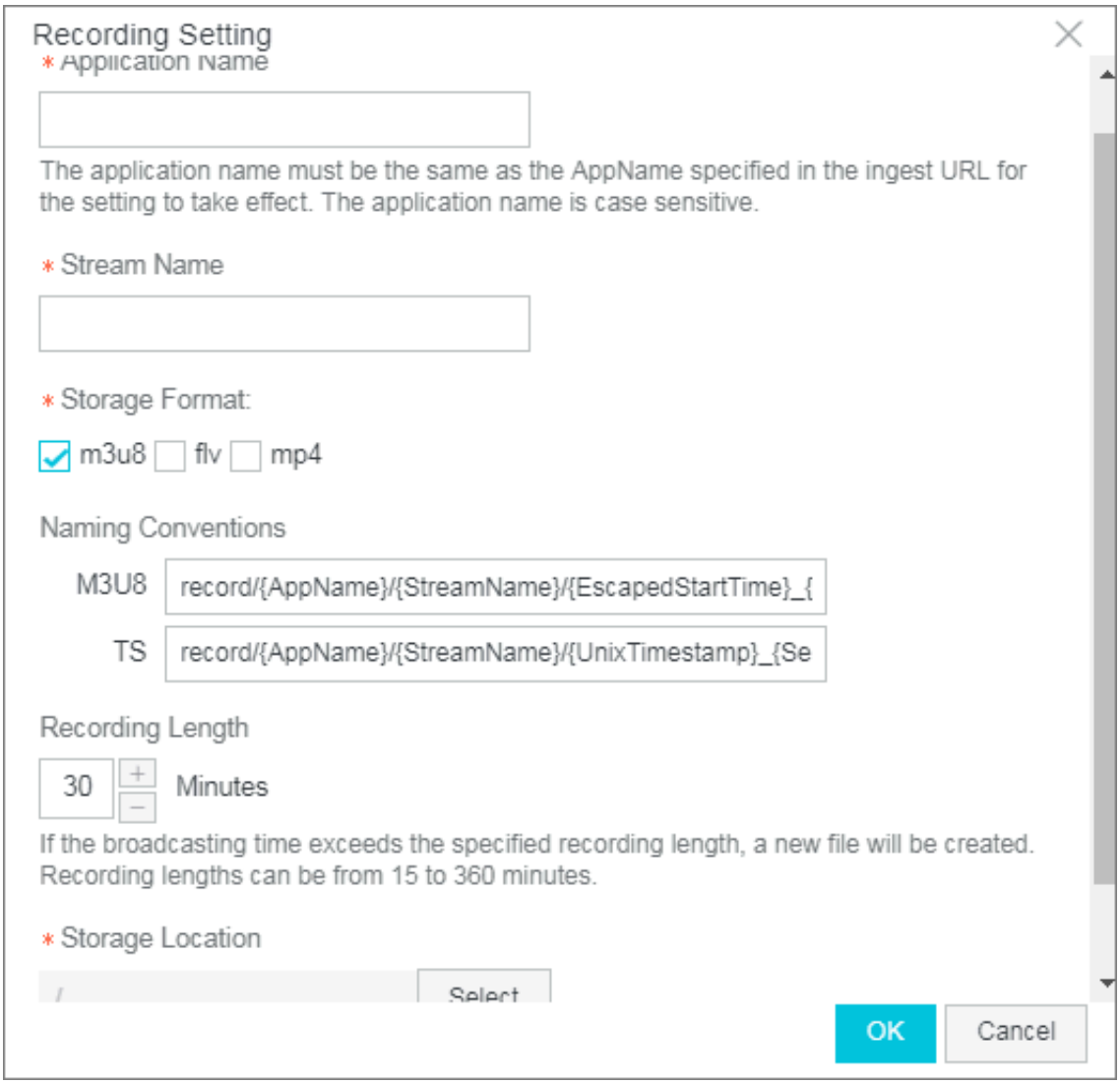
5. Select Store to OSS.



Note:

To store live recordings to OSS, you must provide ApsaraVideo Live service with the access authorization of writing in OSS. Then you can store videos in specific OSS bucket. For more information, see Configure OSS.

6. Add callback URL. For more information, see Recording callback URL.
7. Click Add, and enter recording parameters in Recording Template .



- AppName: The name of the video app. The AppName must be the same with the AppName of the live stream, or the configuration does not take effect. For

example, the AppName in streaming address is `app`, and the AppName of the recording parameter must also be `app`. If you want to configure domain-level recording parameter, enter wildcard (*).

- StreamName: The system supports recording at stream level. You can enter the stream name that you want to record. If you want to record all the streams under the `AppName`, enter wildcard (*).

  Note:
  AppName and StreamName parameters support upper case letters, lower case letters, number, hyphen (-) and underline (_). The length is limited within 255 characters.

- Storage Format/Format: The system supports flv, m3u8, and mp4 formats.
- Naming Conventions: The default storage path for recordings is:

```
m3u8 : record /{ AppName }/{ StreamName }/{ EscapedSta  rtTime  } _
{ EscapedEnd  Time  }

ts : record /{ AppName }/{ StreamName }/{ UnixTimest  amp } _ {
Sequence }

mp4 : record /{ AppName }/{ StreamName }/{ EscapedSta  rtTime  } _
{ EscapedEnd  Time  }

flv : record /{ AppName }/{ StreamName }/{ EscapedSta  rtTime  } _
{ EscapedEnd  Time  }
```

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

```
m3u8 : record / app / stream /{ EscapedSta  rtTime } _ {
EscapedEnd  Time  }

ts : record / app / stream /{ UnixTimest  amp } _ { Sequence }
```

If the default recording file storage path does not meet your requirements, you can modify it by using the API interface.

To maintain compatibility with the streaming process, the recording system judge a live stream 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 (m3u8 files) in the format: `{ AppName }/{ StreamName }/{ Date }. m3u8` .

- Recording Cycle/Cycle: The system supports Recording Cycle/Cycle from 15 to 360 minutes, that is 6 hours recording at most. If a recording time duration exceeds 6 hours, the system generates a new recording file according to the recording naming rule. The default time duration of ts fragments is 30 seconds.
- Storage Path/Path: The storage location of the recording.

> Note:
> The buckets list contains standard buckets and MPS buckets. The standard buckets are OSS buckets, used for storing; the MPS buckets are customized by MPS, and video stored in MPS bucket can perform MPS transcoding tasks. Currently, standard buckets and MPS buckets are not labelled in the buckets list. If you want to convert videos to media files, we recommend that you differentiate the name of the MPS bucket by yourself.

8. Click OK to complete recording configuration.

   All the live streams of which theAppName is `app` , and the StreamName is `stream` under the domain name all perform recording operation according to this configuration. If you want to view recorded files, see View recorded files.

   > Note:
   > The new recording configuration takes effect when you re-perform streaming operation. If you have started the streaming operation before the configuration, you must suspend the current streaming for more than 180s, and then re-configure streaming parameters.

6.1.3 Recording callbacks

You can set recording callback URLs and send requests to these URLs to query the recording status and results.

Restrictions and guidelines

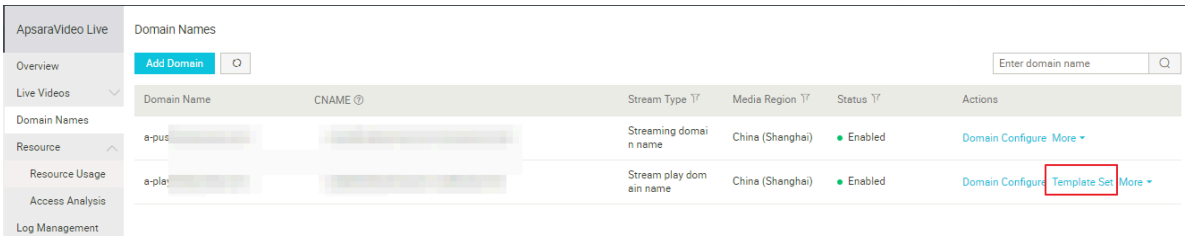
You can only receive recording file generation event, after added a recording callback URL in the ApsaraVideo Live console. If you want recording status events, you should call #unique_67 to set NeedStatusNotify = true first.

Both HTTP and HTTPS URLs are supported. POST requests in JSON format are sent to the user server to inform the user of the recording result and status in real time. The user server then returns a response with status code 200. If an HTTPS callback URL is used, you must make sure that the HTTPS certificate is a CA issued certificate. If the request times out, ApsaraVideo Live will resend the request. ApsaraVideo Live can attempt to resend the request for up to five times. The resending interval is a random number between 100 milliseconds and 10 seconds.

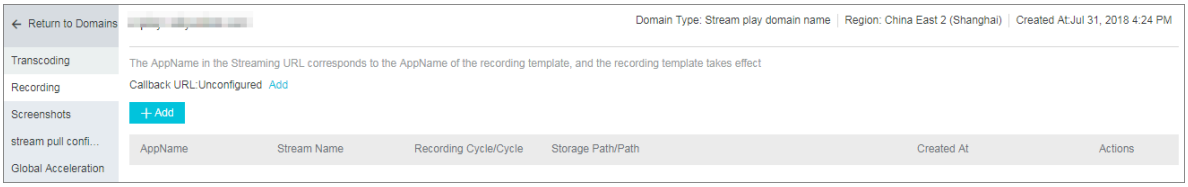
Procedure

You can add a recording callback URL in the ApsaraVideo Live console.

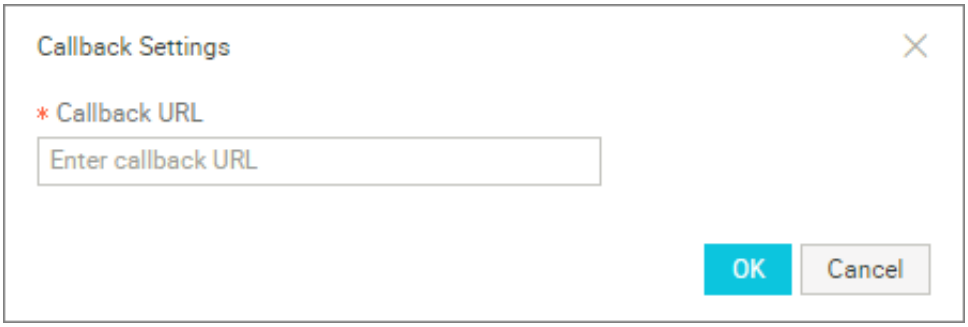
1. Log on to the ApsaraVideo Live console.
2. Click Domain Management.
3. Select the target streaming domain name, and click Stream Settings.



4. In the left-side navigation pane, click Recording Settings.



5. Click Add to the right of Callback URL.
6. In the Configure Callback URL dialog box, enter a callback URL.



Note:
For security, you cannot set internal network addresses as callback URLs. Callback URLs must be valid public network addresses.

Example:

Callback URL: The body of the response returned from `http :// 1 . 1 . 1 . 1 / notify / record` is as follows:

Sample callback for a recording file generation event

This callback indicates that the target recording file has been 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
}
```

The domain, app, and stream parameters indicate the domain name, application name, and stream name, respectively. The URI parameter indicates the path of the OSS bucket that stores the target recording file. The duration, start_time, and stop_time parameters indicate the length of the recording, the recording start time, and the recording end time, respectively.

Sample callback of the recording status (triggered when NeedStatusNotify is set to true)

- Callback indicating that the recording process has started.

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

  The domain, app, and stream parameters indicate the domain name, application name, and stream name, respectively. The event parameter indicates the name of the event, which can be record_started/record_paused/record_resumed.
- Callback indicating that the recording process has been paused.

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

- Callback indicating that a recording error has occurred.

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

}
```

6.1.4 Record indexes

This feature allows you to record live video streams as M3U8 files, store these files in OSS, and edit the stored TS files in real time.

> Note:
> Terms in the console have been updated, and we will update the documentation as soon as possible. We are sorry for any inconvenience caused.

Prerequisites

This feature is available for videos stored in OSS.

Target scenarios

- The start time and end time that need to be adjusted for a video generated after live streaming.
- During the live streaming of major sporting events, video clips need to be edited in real time and broadcast.

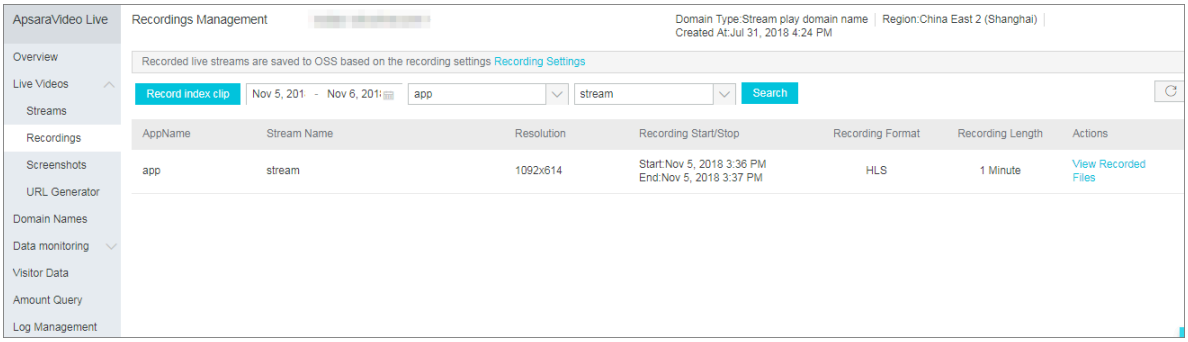
The editing operation reorganizes TS files of different time periods into a new M3U8 file. The TS files are not duplicated.

Procedure

1. Log on to the ApsaraVideo Live console.
2. In the left-side navigation pane, choose Live Videos > Recordings.
3. Click Save to OSS.

> Note:
> You can select specified video streams, application names, and stream names. You can view files that have been recorded within three months.

4. Click Edit Recording Index Files.

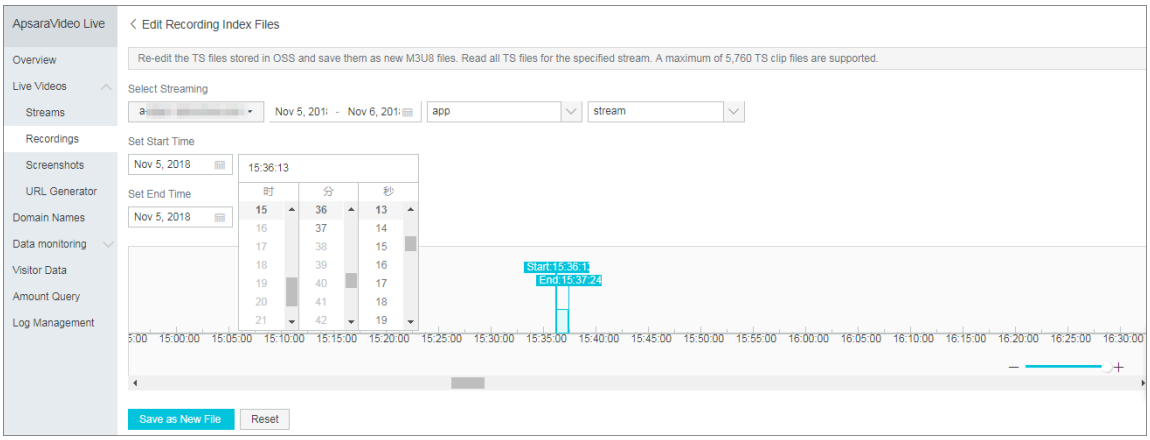


5. On the Edit Recording Index Files page, select the stream, recording time period, application name, and stream name to edit a specified stream.

> **Note:**
> You can only adjust the start time and the end time to remove the beginning or end of a video.

You can perform the following operations on the Edit Recording Index Files page.

- Click an M3U8 file and adjust the start time and end time of the video.
- Click multiple M3U8 files and edit the start time and end time to generate a video clip.
- Click the plus (+) icon to zoom in and the minus (-) icon to zoom out. This allows you to view and edit the file more accurately.



6. Click Save as New File.

   The new M3U8 file is stored in the root directory of the current OSS bucket. You can search for the file in OSS.

7 Screenshots management

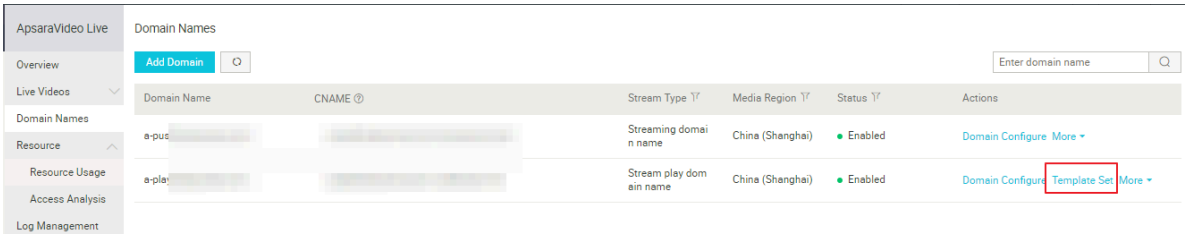
7.1 Configure snapshots

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

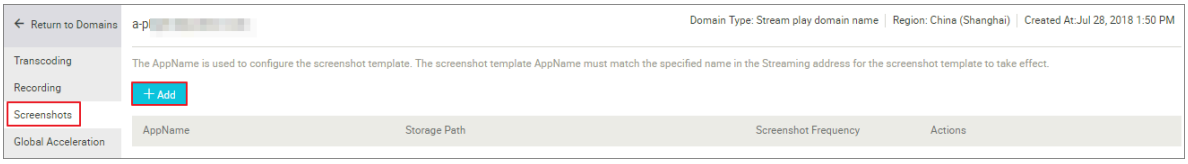
Under an ApsaraVideo Live acceleration domain name, the live snapshot settings are differentiated by the AppName of the live streaming. That is, all the streams under the same AppName perform snapshot operations following the settings of this AppName. The AppName can be set to *, indicating that all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

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

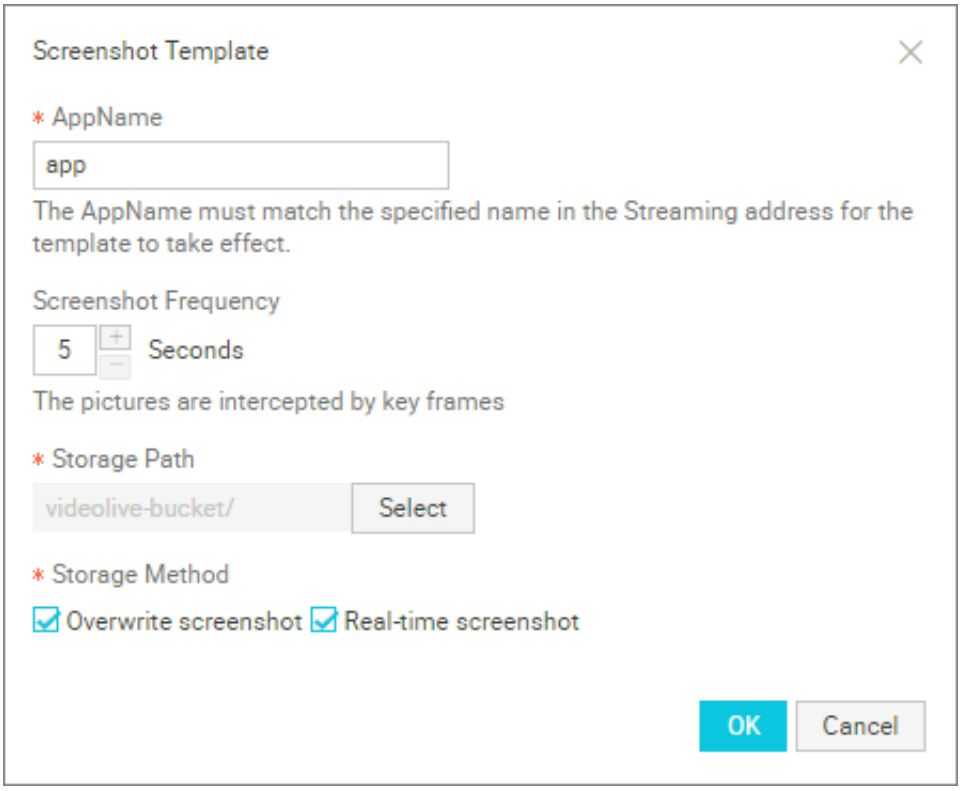
1. Log on to the ApsaraVideo Live console.
2. Click Domain Names.
3. Select the Streaming Domain Name, and click Manage Templates at the right side.



4. Click Snapshots, and click Add.



5. In Snapshot Capture Template, enter the snapshot parameters, and click OK.

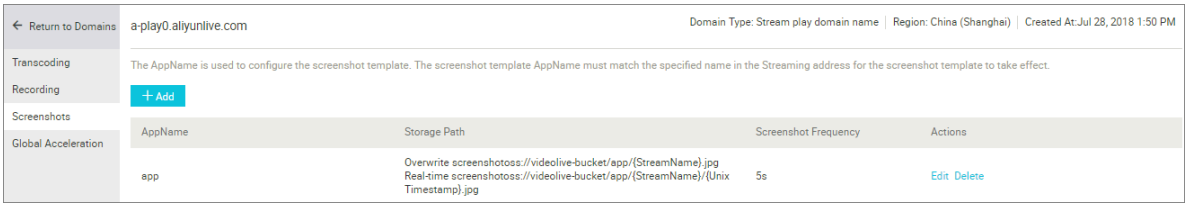


- Enter the AppName that you want to enable snapshots function.
- Enter Snapshot Capture Interval. It can be between 5 and 3,600 seconds.
- Select Storage Location.
- Select Storage Mode, that is Overwrite snapshot or Real-time snapshot. You can also select both.
  - Overwrite: The video snapshots are taken in sequence based on the set interval, and the new snapshot overwrites the previous one.
  - Create New: 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).

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, confirm whether the OSS bucket and the domain name are in the same region.

In Snapshots, all the snapshots configurations are listed under the domain name. For example, all the live streams of which the AppName is app performs the snapshots operation based on this configuration.



Note:

After you modify the snapshots configuration, the new snapshots configuration takes effect for the next push streaming operation.

8 Streams Management

8.1 Ingest Callback URL

Ingest callback URL is mainly used to call back stream status information in real time and promptly notify users about the push 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 you the real-time feedback on whether the video streaming succeeds or fails.

Attentions

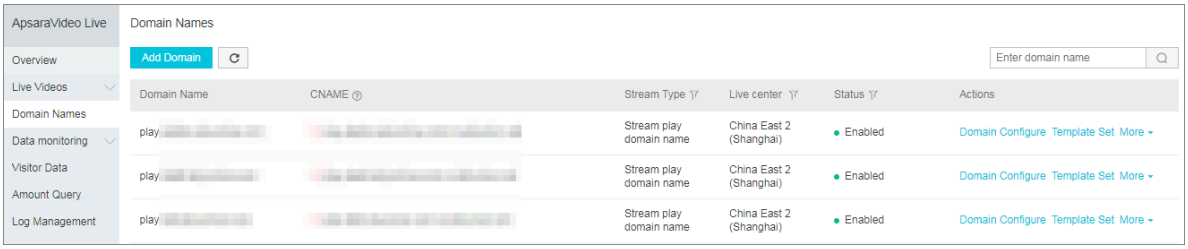
- Principle: The real-time stream status feedback is implemented through GET requests sent to the user’s server through the HTTP interface. The user server returns 200 responses to the interface.

  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.
- If you use an Ingest Domain Name to push a stream, that is, Edge Ingestion, configure the Ingest callback URL on the Ingest Domain Name. If you use a Streaming Domain Name to push the stream, that is the Standard Ingestion, we will generate a standard ingestion URL for you, and push the stream directly to the live center, and you can configure the Ingest callback URL on the Streaming Domain Name. This article takes configuring Ingest callback URL in Edge Ingestion as an example to introduces how to configure Ingest callback URL.

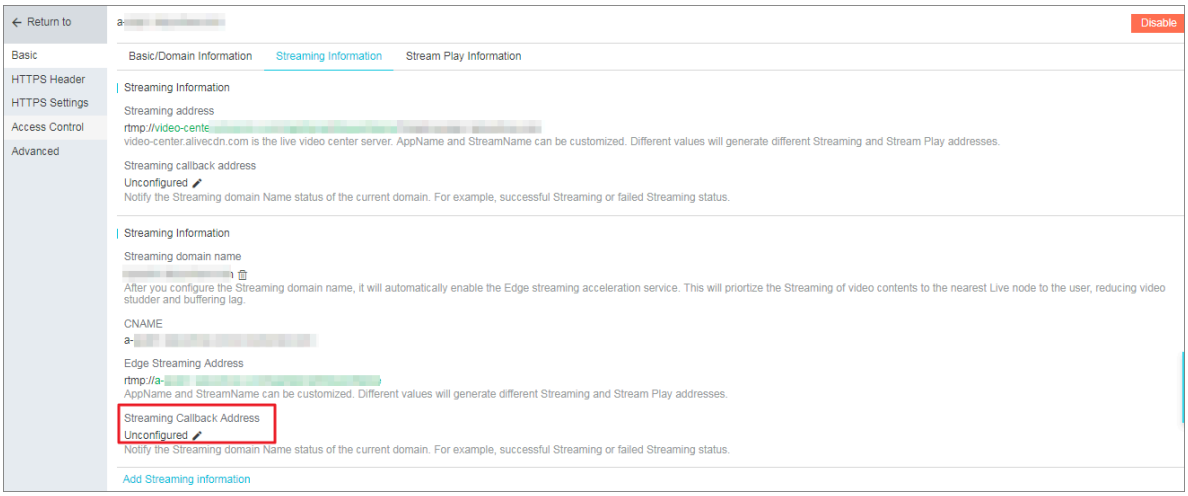
Procedure

1. Log on to the ApsaraVideo Live console.
2. Click Domain Names.

3. Select the Streaming Domain Name and click Configure.



4. In Basic Settings > Stream Pushing Information, select the Ingest Callback URL following ingest URL, and click the edit icon at the right side of Not Configured.



> **Note:**
> If you select Standard Ingestion, select Ingest Callback URL of Streaming Pushing Information for configuration.

5. In Configure Callback URL, enter the callback URL.

Examples

```
https :// live . aliyunlive . com / pub ?  action = publish  &  app
= xc . cdnpe . com  &  appname = test01  &  id = test01  &  ip = 42 .
120 . 74 . 183  &  node = cdnvideoce  nter010207  116011 . cm3
```

Parameters	Value description
time	Unix timestamp

Parameters	Value description
usrargs	User push 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.

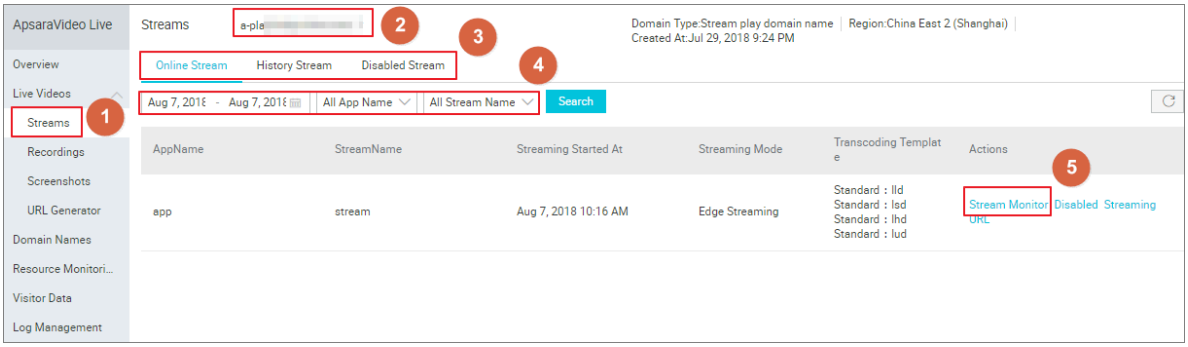
8.2 View frame rate and bit rate

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. You can easily view the uplink transmission status of the live stream to check if there is any problem.

1. Log on to the ApsaraVideo Live console.
2. Click Live Management > Streams.
3. Select the Streaming Domain Name.
4. Select the stream status.
5. Select the time period, the AppName, and the StreamName of the stream that you want to view.

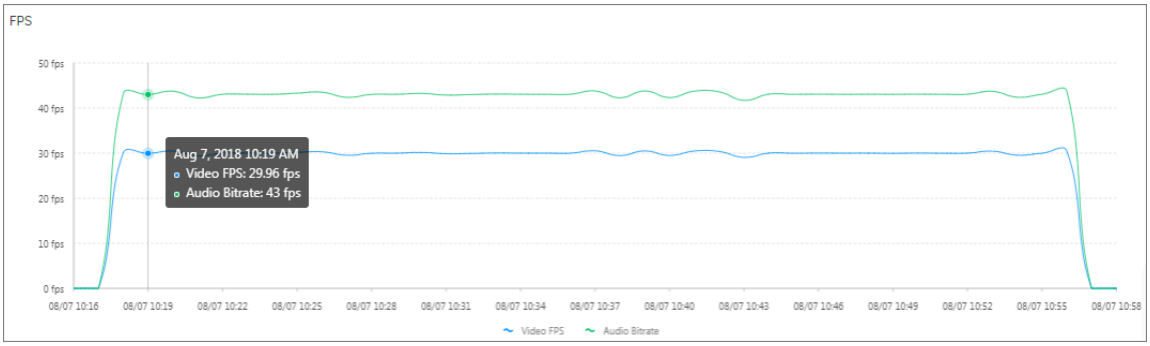
6. Click Stream Monitoring at the right side of the stream that you want to view.



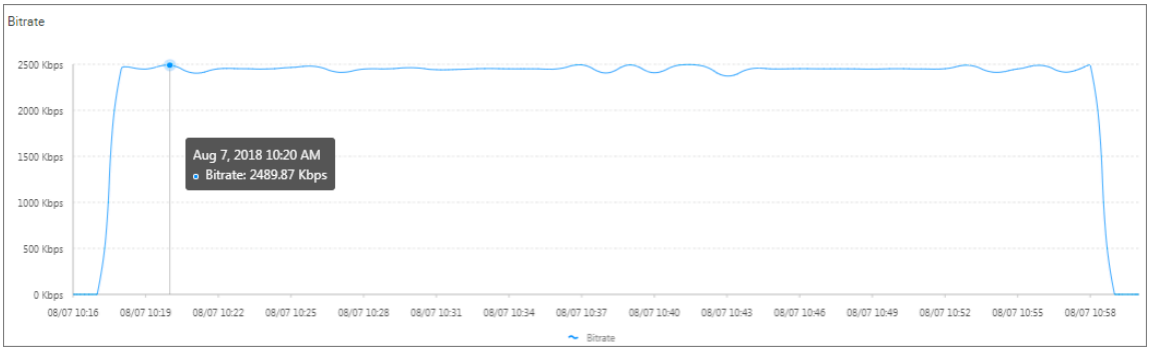
7. View the stream monitoring data.

   In Stream Monitoring, you can see Length, Application Name, Stream Name、Bitrate (Average), and Frame Rate (Average).

   - Video and audio frame rate



   - Bit rate



   On average, the stream monitoring data is updated every minute. You can view the uplink transmission in the Stream Monitoring 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.

Note:
You can get the monitoring data about 5 minutes after push streaming, and the system refreshes the monitoring data every one minute. If the push streaming time is short, you can not see the monitoring data.

Causes of choppy push 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.

  Push streaming consumes CPU resources. During the push 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. Keep the video frame rate higher than 15 frames per second (FPS).

  Although a higher frame rate ensure a smooth video watching process, 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. We recommend that you set appropriate video parameters.

- Network bandwidth.

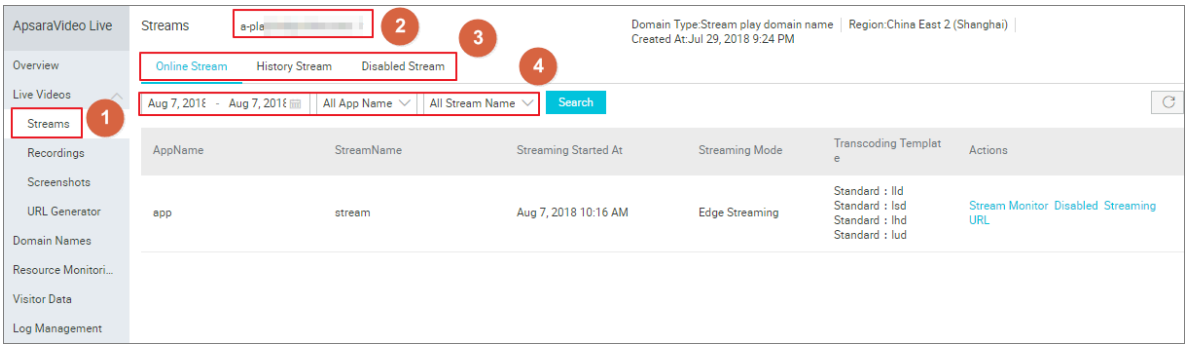
  Common network factors include:

  - 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 delete and terminate any unnecessary programs to save the resources.

8.3 View a live stream

You can perform the following steps to view a live stream.

1. Log on to the ApsaraVideo Live console.
2. Click Live Management > Streams.
3. Select the Streaming Domain Name.
4. In Online Streams, Historical Streams, and Disabled Push Streams, select the stream status you want to view.
5. Select the time period, AppName, and StreamName of the stream that you want to view, and click Search.



You can see the information of the live stream that you want to view.

9 Real-time monitoring

9.1 Push streaming monitoring

Live streaming monitoring includes push streaming monitoring and live streaming monitoring. Most live streaming problems such as lagging are related to push streaming bandwidth. Monitoring streaming bandwidth in real time can help you quickly locate live streaming problems such as lagging and latency. This section describes how to perform push streaming monitoring, monitor the status of streaming during live streaming.

Note:
Terms in the console have been updated, and we will update the documentation as soon as possible. We are sorry for any inconvenience caused.

Monitoring data is returned every second in real time, including received audio and video frame rate from caster to CDN node, audio and video timestamp, received file headers, audio and video bit rate (Kbps), maximum audio and video frame interval (milliseconds), and error code. You can check the status of video stream every second to monitor the streaming stability. This allows you to monitor live streams and helps reduce problems caused by video lagging.

1. Log on to the ApsaraVideo Live console.
2. In the left-side navigation pane, select Data Monitoring > Real-time Monitoring.
3. Select the domain name, time period, application name, and stream name of the stream that is pushed, and click Search.
   - Click Last 10 minutes to obtain monitoring data in real time. The streaming status is returned every second within each minute.
   - Click Last Half Hour, Last Hour, or Custom to query history monitoring data. You can query monitoring data of the last 24 hours.

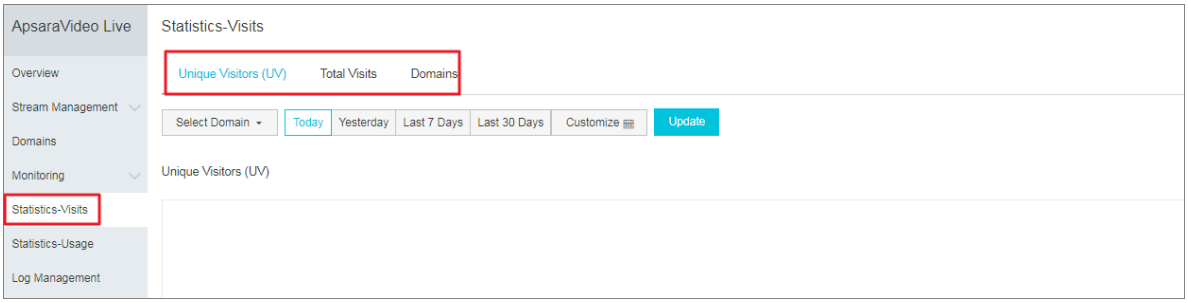
10 Statistics-Visits

Statistics-Visits includes Unique Visitors（UV）, Total Visits and Domains, you can select the Domain Name and Time range that you want to view.

Item	Description
Unique Visitors (UV)	Statistics of the number of visits of unique IP within a specific time range under the current domain name.
Access by Location	The location of users who watch videos.
Domains	Access rankings for each domain name.

Procedure

1. Log on to the ApsaraVideo Live console.
2. ClickStatistics-Visits.
3. Select Unique Visitors, Total Visits, or Domains.
4. Select Domain Name and Time range that you want to view, and clickSearch.



Note:

You can select Mainland China, and HK, Macao, Taiwan, and Overseas to view users location.

11 Set subaccounts to log on to the ApsaraVideo Live console by using 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 information, 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;

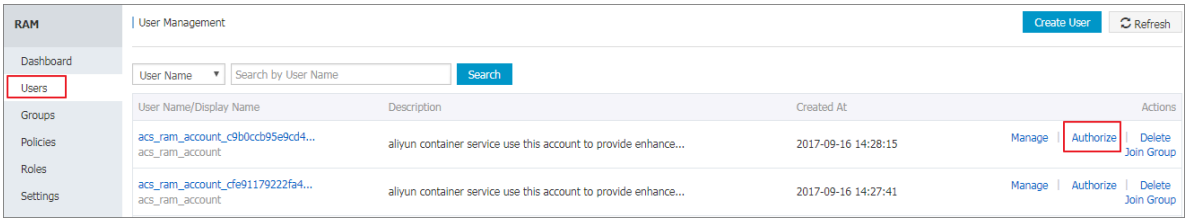
OSS (Required): Grants permission to use the screenshot storage service, which can be customized as needed; For more information, see the following content.

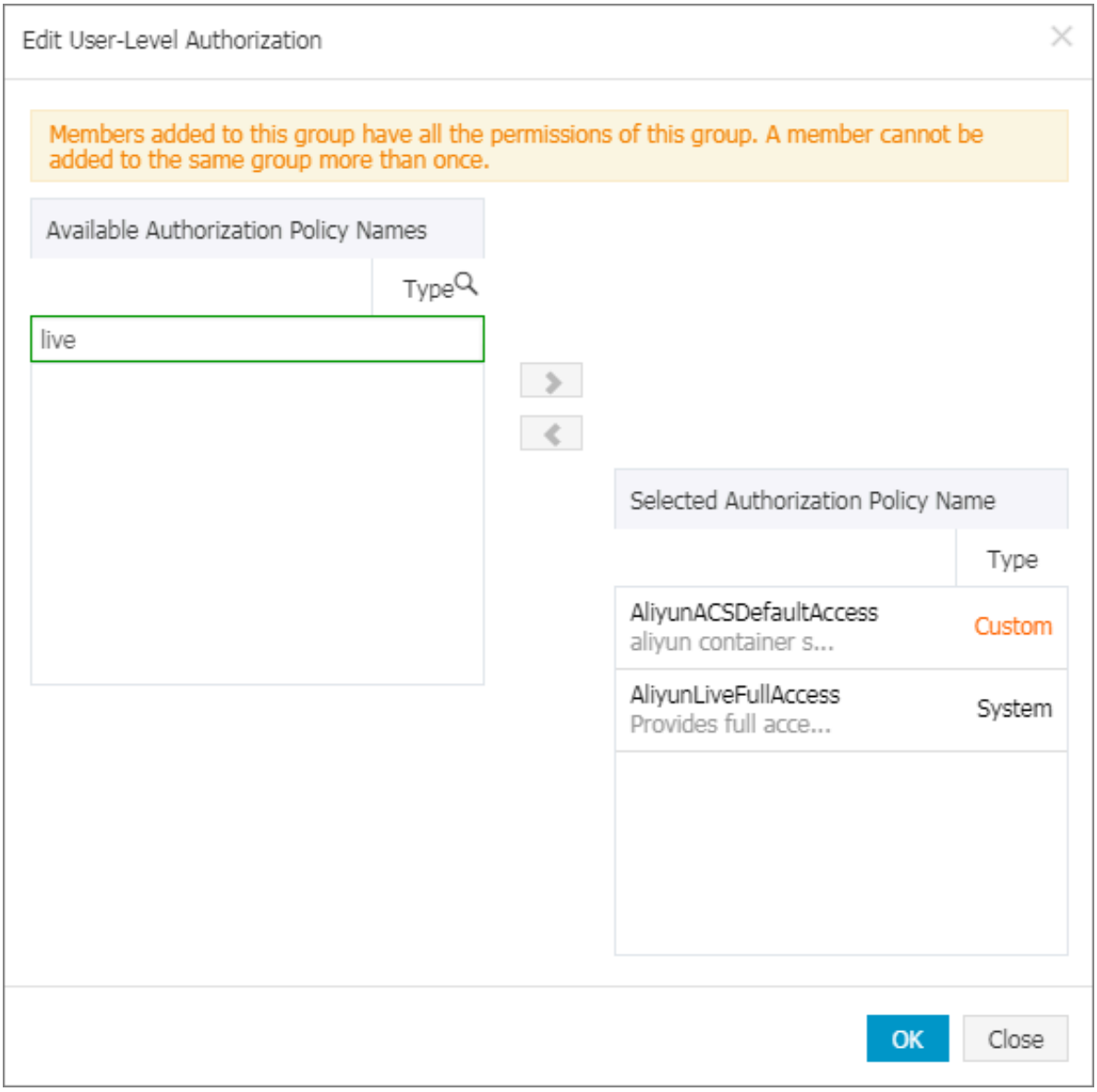
Authorization operations

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-in `AliyunLive FullAccess` authorization policy as follows:

1. Log on to the RAM console.
2. Click Users.
3. Select User Name and click Authorize from the Actions column to grant the `AliyunLive FullAccess` permission to the specified subaccount.

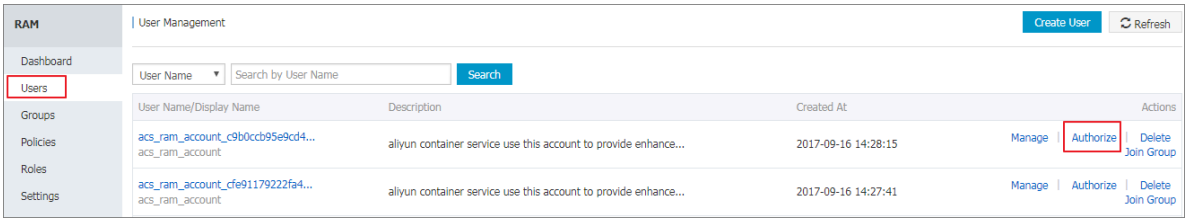




MTS service authorization

If a subaccount is required to use MTS, you must grant the subaccount the permission to use MTS. You can directly use the built-in `AliyunMTSF ullAccess` authorization policy as follows.

1. Log on to the RAM console.
2. Click Users.
3. Select User Name and click Authorize from the Actions column to grant the `AliyunMTSF ullAccess` permission to the specified subaccount.

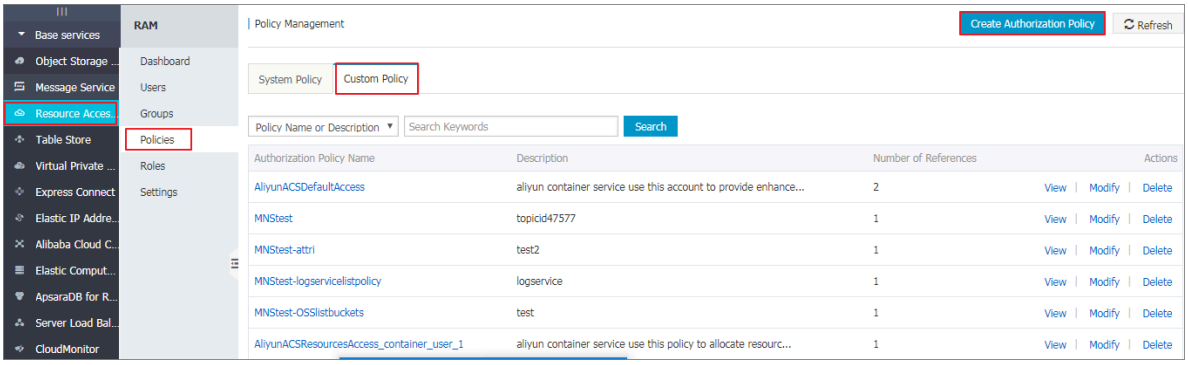


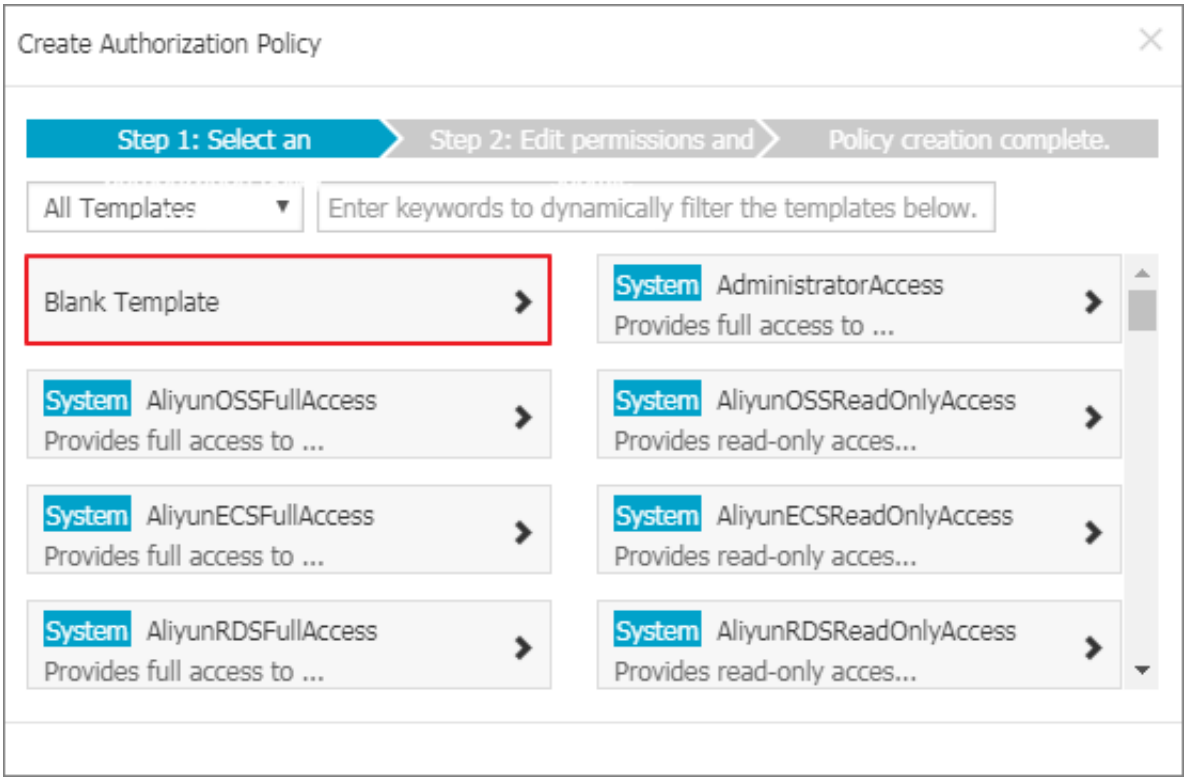
Description of custom authorization policy creation

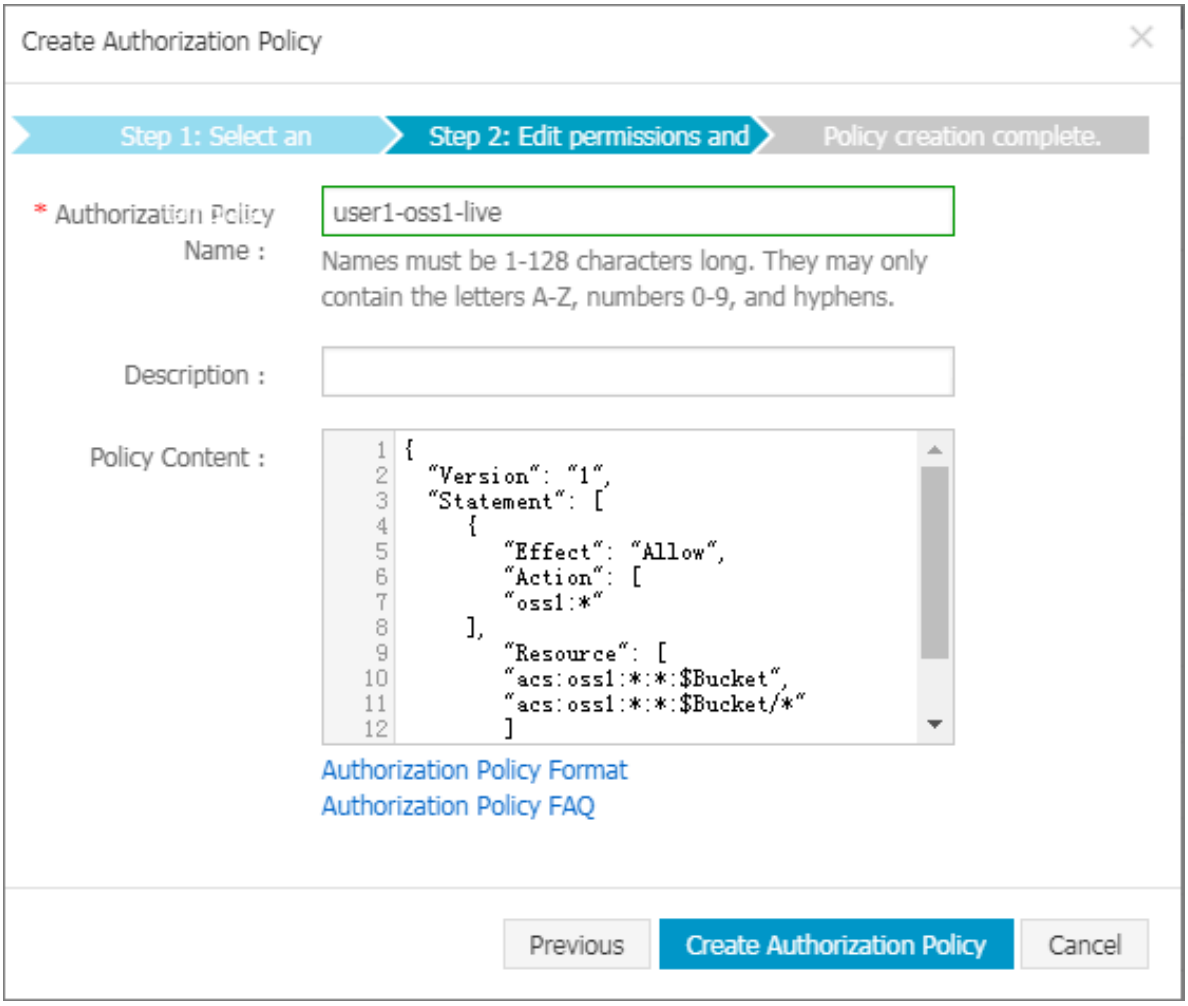
You can customize authorization policies and assign them to specified subaccounts.

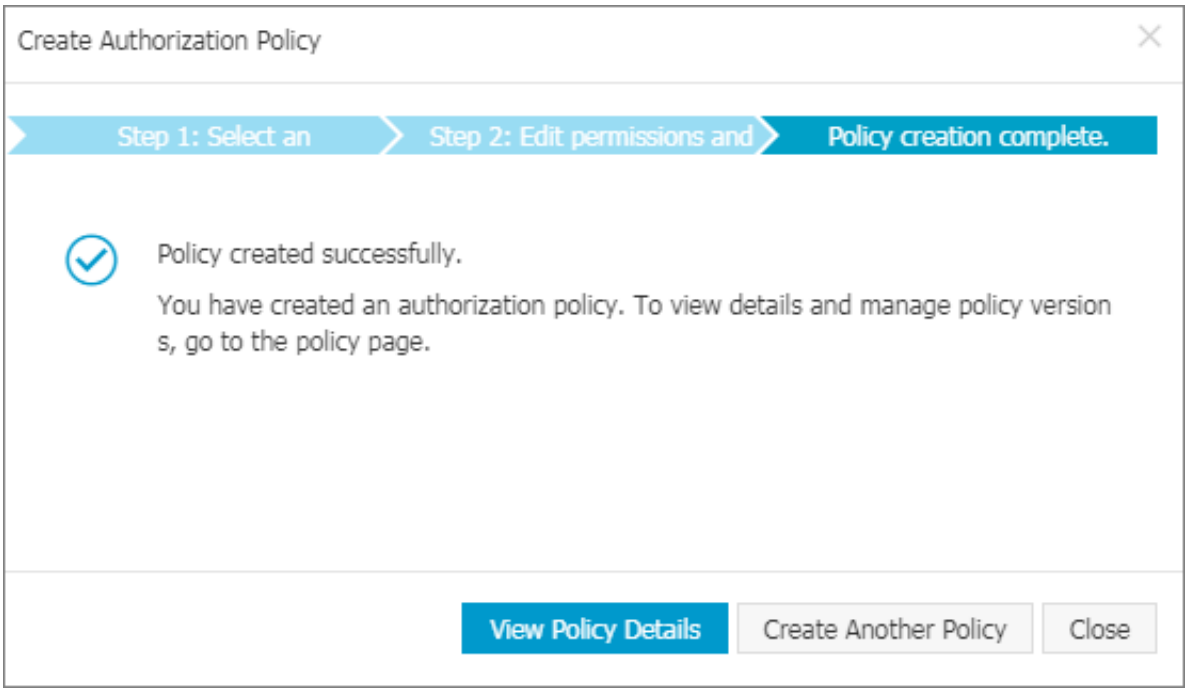
1. Log on to the RAM console.
2. ClickPolicies.
3. Click Custom Policy.

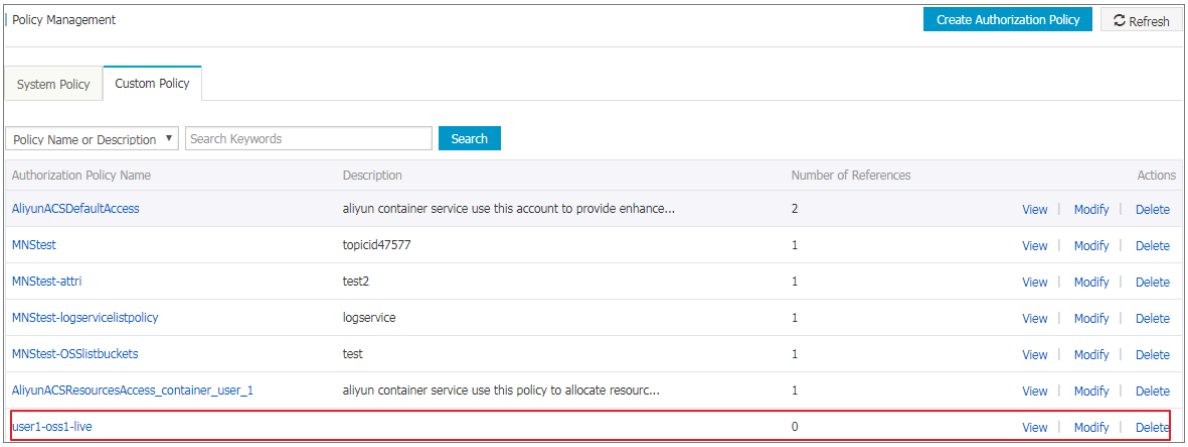
4. Click Create Authorization Policyto create custom authorization policies as the following samples for the specified resource instance and grant the policies to the specified subaccount.






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


Create Authorization Policy
Step 1: Select an
Step 2: Edit permissions and
Policy creation complete.
Policy created successfully.
You have created an authorization policy. To view details and manage policy versions, go to the policy page.
View Policy Details
Create Another Policy
Close



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 : ListBucket  s "
      ],
      " Resource ": "*",
      " Effect ": " Allow "
    }
  ]
}
```

Live authorization policy

Permission description:

- All operation permissions on specified Live CDN domain name;
- Permission to view the Live CDN domain name;

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

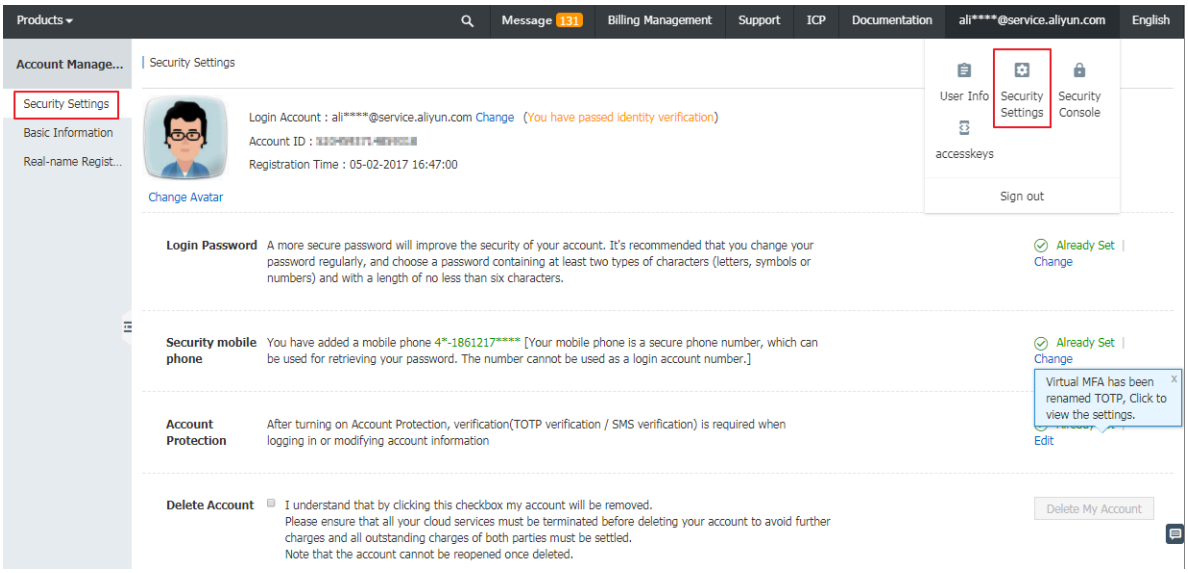
Note:

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.

- **Live**

  $DomainName: Live CDN domain name.