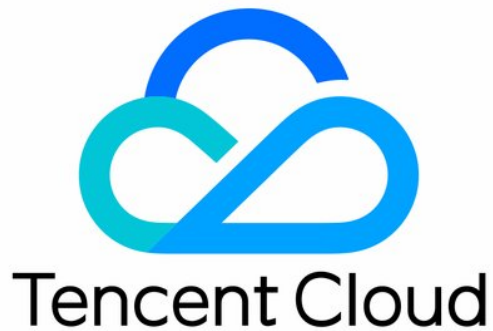


StreamLink

Console Guide

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

 Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Console Guide

- Managing Events

- Flow Management

 - Managing Flows

 - Adding Inputs and Outputs

 - Configuring IP security group

 - Starting and Stopping a Flow

 - Viewing Addresses, Log, and Health Info

- Usage Statistics

Console Guide

Managing Events

Last updated : 2023-12-23 17:15:52

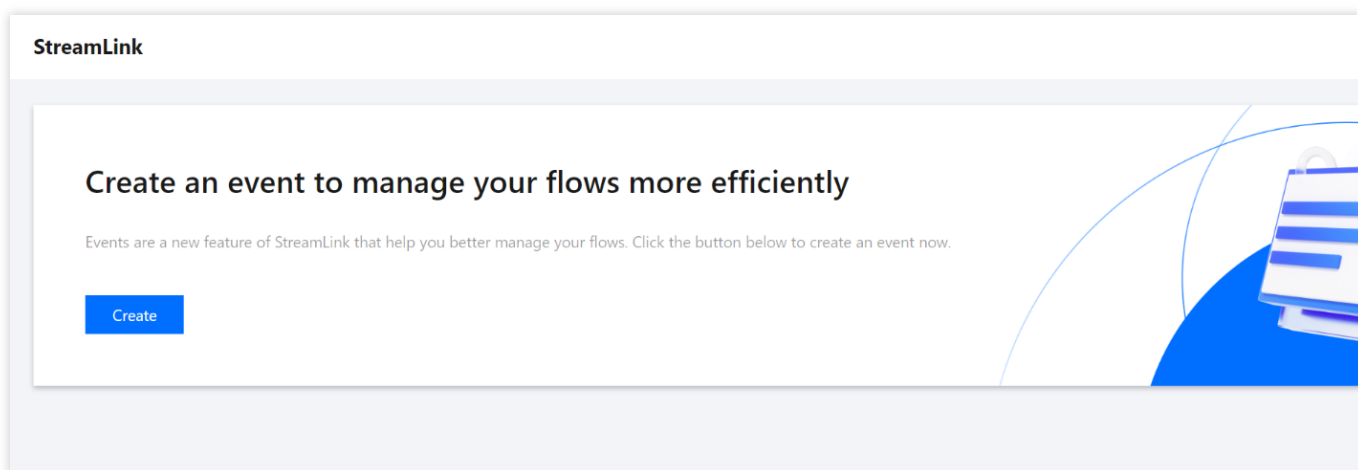
Overview

StreamLink offers reliable and secure real-time transport capabilities to help you transmit media quickly, stably, and with low latency. In the StreamLink console, transport resources are managed as events and flows. You can create an event in the console for an esports competition, a sports event, a concert, a product launch, or other activities or projects. An event is a collection of flows, and each flow is a transfer linkage. With StreamLink, you can not only transport videos quickly and stably, but also monitor the transmission process in a comprehensive way.

Managing Events

In StreamLink, flows are managed at the event level. An event can have multiple interrelated flows. Usually, an event is an activity or a project, such as an esports competition, a sports event, a concert, and a product launch. After creating an event in the console, you can create flows for it.

1. In the StreamLink console, click **Create** and enter the information required.



Create event ✕

Event name *

Event description

[Create](#) [Cancel](#)

2. The event overview page shows all the events you created. You can start or stop all flows of an event on this page, or click **Flow management** to manage the details of a flow.

StreamLink

[Create event](#)

<p>Not started test ✎ ⋮</p> <p>test</p> <p>Event ID <input type="text"/></p> <p>Creation time 2023-01-30 18:58:47</p> <p>Flow count 1</p> <p>Start all Flow Management</p>	<p>Not started <input type="text"/> ✎ ⋮</p> <p><input type="text"/> event hold in Shanghai.</p> <p>Event ID <input type="text"/></p> <p>Creation time 2023-01-29 15:55:47</p> <p>Flow count 1</p> <p>Start all Flow Management</p>	<p>Running <input type="text"/> ✎ ⋮</p> <p>yulong</p> <p>Event ID <input type="text"/></p> <p>Creation time 2023-01-17 18:18</p> <p>Flow count 5</p> <p>Start all Flow Manage</p>
<p>Not started <input type="text"/> ✎ ⋮</p> <p>This is default event, flow will be saved here if you create flow...</p> <p>Event ID <input type="text"/></p> <p>Creation time 2023-01-11 18:14:06</p> <p>Flow count 26</p> <p>Start all Flow Management</p>	<p>Not started <input type="text"/> ✎ ⋮</p> <p><input type="text"/></p> <p>Event ID <input type="text"/></p> <p>Creation time 2023-01-06 11:12:02</p> <p>Flow count 7</p> <p>Start all Flow Management</p>	<p>Not started <input type="text"/> ✎ ⋮</p> <p>-</p> <p>Event ID <input type="text"/></p> <p>Creation time 2022-12-28 19:17</p> <p>Flow count 4</p> <p>Start all Flow Manage</p>

Flow Management

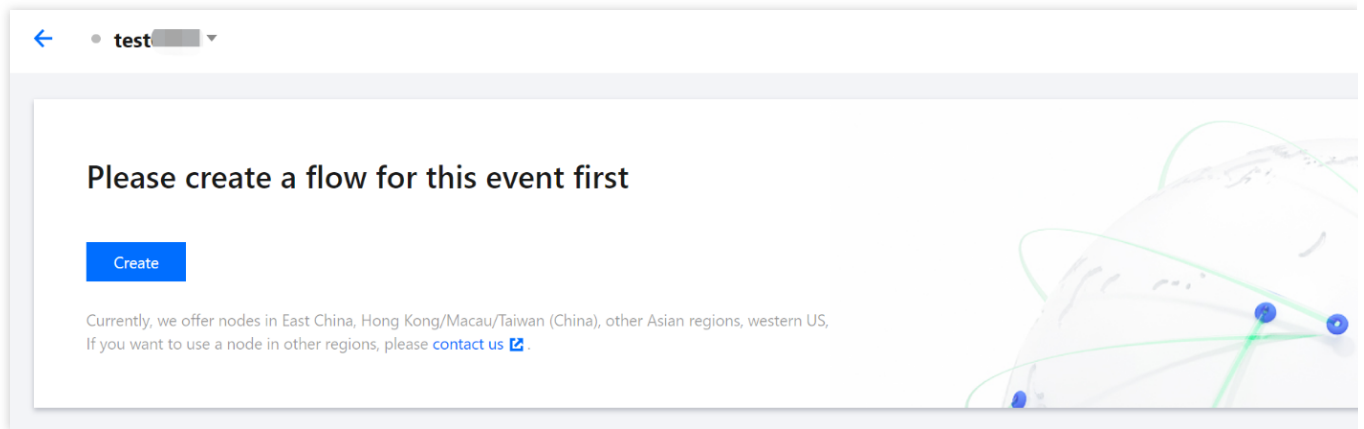
Managing Flows

Last updated : 2023-12-23 17:16:44

After creating an event, click the event on the event overview page. You will enter the flow management page, where you can manage the event's flows. Each flow is a transfer linkage.

Creating a Flow

1. In the **StreamLink console**, select the event you created, click **Flow management**, and then click **Create**.



2. Enter the following information:

Flow name: Enter a name that can help you easily distinguish the flow from others.

Max bandwidth: Select the maximum bandwidth for your flow. The system will assign network resources based on your configuration.

Region: Select the region of your flow.

Create Flow ✕

Flow name *

Max bandwidth *

Region *

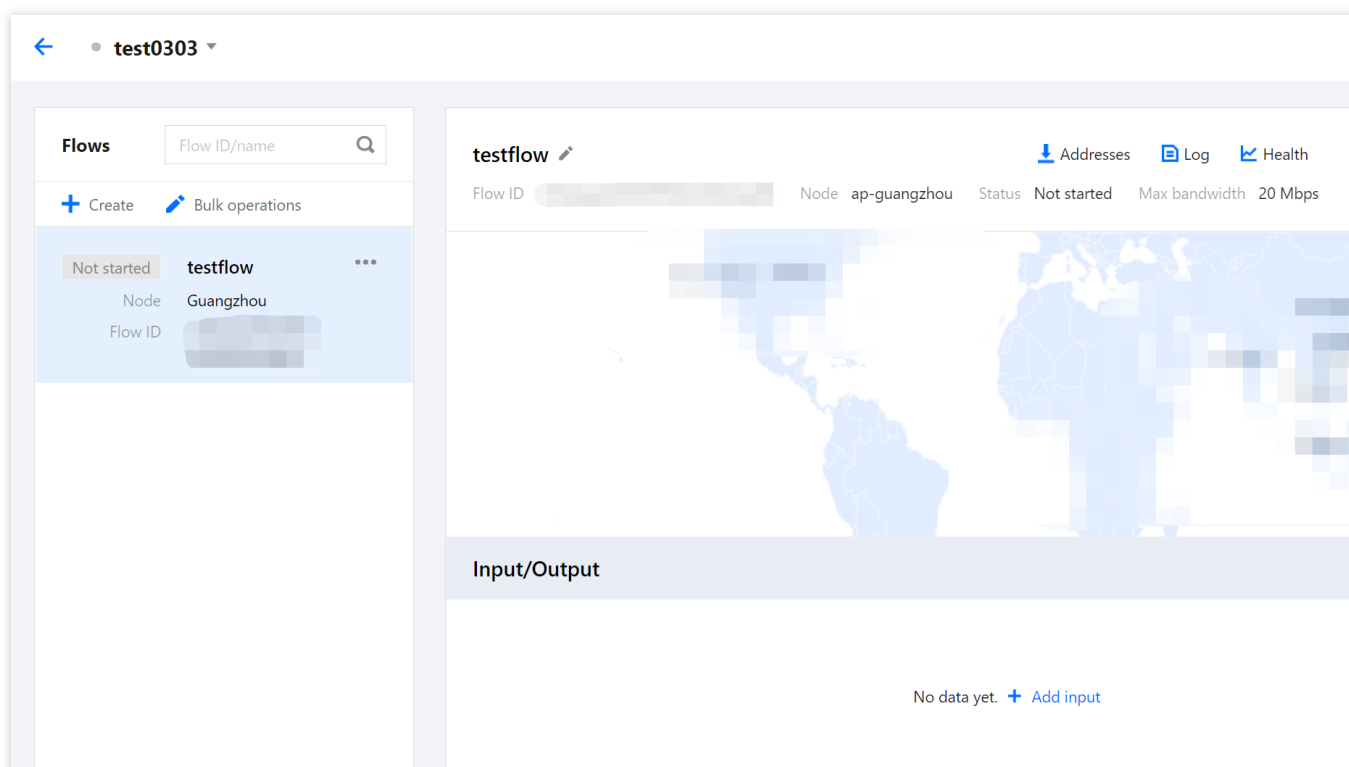
[Create](#) [Cancel](#)

3. After creating a flow, it will appear on the flow management page, where you can start, stop, and delete a flow (bulk operation supported), as well as export the addresses of a flow.

The screenshot shows the 'Flow Management' page in the Tencent Cloud StreamLink console. On the left, a sidebar lists flows. One flow named 'test' is highlighted, with a status of 'Not started' and a node of 'Shanghai'. A context menu is open over this flow, showing 'Start' and 'Delete' options. The main content area shows the details for the selected 'test' flow, including its Flow ID, Node (ap-shanghai), Status (Not started), and Max bandwidth (20 Mbps). Below the details is a world map and an 'Input/Output' section showing an active RTMP connection.

Adding Inputs and Outputs

Last updated : 2023-12-23 17:17:10



On the [Flow management](#) page, select a flow in the flow list to add [inputs](#) and [outputs](#).

Adding an Input

Click **Add input** and enter the following information:

Input name: Enter a name that can help you easily distinguish the input from others.

Input region: Select the input region.

Protocol type: Select the input protocol. The protocols supported include RTMP, RTMP_PULL, SRT, and RTP. The other input settings vary with the input protocol you select.

Latency setting: Set the server-side latency. Currently, only the SRT protocol supports latency configuration.

Mode: If the input protocol is SRT, you choose either the listener or caller mode.

Create input

Input name *	<input type="text" value="Enter an input name"/>	Protocol type *	SRT
Input Region	Guangzhou	Mode *	Please select
Latency Setting ⓘ *	120	Decryption Settings ⓘ	<input checked="" type="checkbox"/>
Failover ⓘ	<input type="checkbox"/>		
CIDR IP allowlist ⓘ	Please enter an allowlist of IPs in CIDR format, e.g. 192.168.0.1/24, and separate multiple IPs with semicolons, e.g. 192.168.0.1/24;192.168.1.1/25.		
Input source description	Add input source description to distinguish it from other input sources.		

1. RTMP

If you select RTMP as the input protocol, you need to push the stream to an address generated by StreamLink.

Failover: If you enable failover, StreamLink will generate two input addresses. You can push streams to both addresses. The stream that arrives first will be used as the primary source. If the primary source is down, StreamLink will automatically switch to the backup stream.

CIDR IP allowlist: The IP allowlist, which specifies the IP addresses (example: `203.3.3.3/28`) that are allowed to push streams. This makes for improved security. Separate multiple addresses with semicolons, as in

`203.3.3.3/28;202.3.3.3/28` .

Input name *	<input type="text" value="Enter an input name"/>	Protocol type *	RTMP
Input Region	Guangzhou	Failover	<input type="checkbox"/>
CIDR IP allowlist ⓘ	Please enter an allowlist of IPs in CIDR format, e.g. 192.168.0.1/24, and separate multiple IPs with semicolons, e.g. 192.168.0.1/24;192.168.1.1/25.		
Input source description	<input type="text" value="Add input source description to distinguish it from other input sources."/>		

2. RTMP_PULL

If you select RTMP_PULL as the input protocol, StreamLink will pull streams from the address you specify.

Source address: The RTMP URL, such as `rtmp://example.com/live`.

Flow key: The RTMP stream key, such as `e18c3c4dd05aef020946e6afb9e04ef`.

Failover: Currently, failover is not yet supported for this protocol type. It will be made available in the future.

Create input			
Input name *	<input type="text" value="Enter an input name"/>	Protocol type *	RTMP_PULL
Input Region	Guangzhou	Source Address *	<input type="text" value="Enter the source URL"/>
Stream key *	<input type="text" value="Enter the stream key"/>	Failover	<input type="checkbox"/>
Input source description	<input type="text" value="Add input source description to distinguish it from other input sources."/>		

3. SRT Listener

If you use this as the input protocol:

Mode: Select **Listener**. In this mode, you need to use the SRT caller mode to request to send your stream to the StreamLink input address. You can view the input address in the flow list.

Latency setting: The server-side SRT latency. If the push end is in the same country as your StreamLink AZ, we recommend you set this to 120 ms. If the push end is not in the same country as your StreamLink AZ, we recommend you set this to 200 ms. If the push end is not in the same continent as your StreamLink AZ, we recommend you set this to 1,000 ms. You can determine the value of this parameter based on the IP address assigned.

Decryption settings: You can toggle this on to use the encryption feature of SRT for improved security. Enter the key and key length. You need to configure the same parameters at the push end, or you will fail to push the stream.

- **Decryption key:** The encryption/decryption key. You need to configure the same key at the push end.

- **Key length:** The key length. You need to specify the same key length at the push end.

Failover: Currently, failover is not yet supported for this protocol type. It will be made available in the future.

CIDR IP allowlist: The IP allowlist, which specifies the IP addresses (example: `203.3.3.3/28`) that are allowed to push streams. This makes for improved security. Separate multiple addresses with semicolons, as in

`203.3.3.3/28;202.3.3.3/28` .

Input name *	<input type="text" value="Enter an input name"/>	Protocol type *	<input type="text" value="SRT"/>
Input Region	<input type="text" value="Guangzhou"/>	Mode *	<input type="text" value="Listener"/>
Latency Setting ⓘ *	<input type="text" value="120"/>	Decryption Settings ⓘ	<input checked="" type="checkbox"/>
Failover ⓘ	<input type="checkbox"/>		
CIDR IP allowlist ⓘ	Please enter an allowlist of IPs in CIDR format, e.g. 192.168.0.1/24, and separate multiple IPs with semicolon e.g. 192.168.0.1/24;192.168.1.1/25.		
Input source description	<input type="text" value="Add input source description to distinguish it from other input sources."/>		

4. SRT Caller

If you use this as the input protocol:

Mode: Select **Caller**. In this mode, StreamLink will request the source stream from the address you provide using the caller mode.

Input IP address: The IP address of the source stream. You can also enter a domain.

Source port: The port number of the source stream.

Latency setting: The server-side SRT latency. If the source address is in the same country as your StreamLink AZ, we recommend you set this to 120 ms. If the source address is not in the same country as your StreamLink AZ, we recommend you set this to 200 ms. If the source address is not in the same continent as your StreamLink AZ, we recommend you set this to 1,000 ms. You can determine the value of this parameter based on the IP address assigned.

Decryption settings: If encryption is enabled for the source stream, you need to toggle this on and enter the decryption key and key length; otherwise, StreamLink will fail to pull the stream.

Decryption key: The decryption key. This is required if encryption is enabled for the source stream.

Key length: The key length, which must be the same as that configured for the source stream.

Failover: Currently, failover is not yet supported for this protocol type. It will be made available in the future.

Input name *	<input type="text" value="Enter an input name"/>	Protocol type *	SRT
Input Region	Guangzhou ▼	Mode *	Caller
Input IP address *	<input type="text" value="Enter the input IP address"/>	Source Port *	<input type="text" value="Enter the input port"/>
Latency Setting ⓘ *	120	Decryption Settings ⓘ	<input checked="" type="checkbox"/>
Failover ⓘ	<input type="checkbox"/>		
Input source description	<input type="text" value="Add input source description to distinguish it from other input sources."/>		

5. RTP

If you select RTP as the input protocol, you need to push the stream to an address generated by StreamLink.

Failover: Currently, failover is not yet supported for this protocol type. It will be made available in the future.

CIDR IP allowlist: The IP allowlist, which specifies the IP addresses (example: `203.3.3.3/28`) that are allowed to push streams. This makes for improved security. Separate multiple addresses with semicolons, as in

`203.3.3.3/28;202.3.3.3/28` .

Input name *	<input type="text" value="Enter an input name"/>	Protocol type *	RTP
Input Region	Guangzhou ▼	Failover ⓘ	<input type="checkbox"/>
CIDR IP allowlist ⓘ	<input type="text" value="Please enter an allowlist of IPs in CIDR format, e.g. 192.168.0.1/24, and separate multiple IPs with semi e.g. 192.168.0.1/24;192.168.1.1/25."/>		
Input source description	<input type="text" value="Add input source description to distinguish it from other input sources."/>		

Adding an Output

Click **Add output** and enter the following information:

Output name: Enter a name that can help you easily distinguish the output from others.

Output region: Select the region to push your stream to.

Protocol type: Select the output protocol type. The other output settings vary with the protocol you choose.

Input Protocols	Supported Output Protocols
RTMP, RTMP_PULL	RTMP, RTMP_PUSH, RTMP_PULL, SRT
SRT	SRT, RTMP_PUSH
RTP	RTP
RTSP	RTSP

1. RTMP_PUSH

If you select this protocol, the stream will be relayed to the address you specify.

Destination URL: The RTMP URL, such as `rtmp://example.com/live` .

Flow key: The RTMP stream key, such as `e18c3c4dd05aef020946e6afb9e04ef` .

Create Output

Output Name *

Output Region *

Stream key *

Output Description

Protocol type *

Destination URL *

2. RTMP_PULL

If you need to play your stream from an output, select this protocol. After creating an RTMP_PULL output, you can view the playback URL in the output list.

CIDR IP allowlist: The IP allowlist, which specifies the IP addresses (example: `203.3.3.3/28`) that are allowed to push streams. This makes for improved security. Separate multiple addresses with semicolons, as in

```
203.3.3.3/28;202.3.3.3/28 .
```

Output Name *	<input type="text" value="Enter an output name"/>	Protocol type *	RTMP_PULL ▼
Output Region *	<input type="text" value="Please select"/>		
CIDR IP allowlist ⓘ	<input type="text" value="Please enter an allowlist of IPs in CIDR format, e.g. 192.168.0.1/24, and separate multiple IPs with semicolons, e.g. 192.168.0.1/24;192.168.1.1/25."/>		
Output Description	<input type="text" value="Add output description to distinguish it from other outputs."/>		

3. SRT Listener

If you use this as the input protocol:

Mode: Select **Listener**. In this mode, you need to use the SRT caller mode at the receiving end to request the stream from StreamLink. You can view the playback URL in the output list.

Latency setting: The server-side SRT latency. If the push end is in the same country as your StreamLink AZ, we recommend you set this to 120 ms. If the push end is not in the same country as your StreamLink AZ, we recommend you set this to 200 ms. If the push end is not in the same continent as your StreamLink AZ, we recommend you set this to 1,000 ms. You can determine the value of this parameter based on the IP address assigned.

Enable encryption: If you enable encryption for the output, you need to do the same at the receiving end and configure the key and key length; otherwise, you will fail to pull the stream from StreamLink.

Encryption key: The encryption key.

Key length: The key length.

CIDR IP allowlist: The IP allowlist, which specifies the IP addresses (example: `203.3.3.3/28`) that are allowed to push streams. This makes for improved security. Separate multiple addresses with semicolons, as in

```
203.3.3.3/28;202.3.3.3/28 .
```

Output Name *	<input type="text" value="Enter an output name"/>	Protocol type *	<input type="text" value="SRT"/>
Output Region *	<input type="text" value="Please select"/>	Mode *	<input type="text" value="Listener"/>
Latency Setting ⓘ *	<input type="text" value="120"/>	Enable Encryption ⓘ	<input checked="" type="checkbox"/>
CIDR IP allowlist ⓘ	<input type="text" value="Please enter an allowlist of IPs in CIDR format, e.g. 192.168.0.1/24, and separate multiple IPs with semicolon e.g. 192.168.0.1/24;192.168.1.1/25."/>		
Output Description	<input type="text" value="Add output description to distinguish it from other outputs."/>		

4. SRT Caller

If you use this as the input protocol:

Mode: Select **Caller**. In this mode, StreamLink will use the SRT caller mode to send the stream to the address you specify.

Output IP address: The IP address that receives the SRT stream. You can also enter a domain.

Port: The port that receives the SRT stream.

Latency setting: The server-side SRT latency. If the source address is in the same country as your StreamLink AZ, we recommend you set this to 120 ms. If the source address is not in the same country as your StreamLink AZ, we recommend you set this to 200 ms. If the source address is not in the same continent as your StreamLink AZ, we recommend you set this to 1,000 ms. You can determine the value of this parameter based on the IP address assigned.

Enable encryption: If you enable encryption at the receiving end, you need to toggle this on and specify the encryption key and key length. Otherwise, you will fail to push the stream.

Encryption key: The encryption key.

Key length: The key length, which must be the same as that configured at the receiving end.

Output Name *	<input type="text" value="Enter an output name"/>	Protocol type *	<input type="text" value="SRT"/>
Output Region *	<input type="text" value="Please select"/>	Mode *	<input type="text" value="Caller"/>
Output IP address *	<input type="text" value="Enter the output IP address"/>	Port *	<input type="text" value="Please enter the port"/>
Latency Setting ⓘ *	<input type="text" value="120"/>	Enable Encryption ⓘ	<input checked="" type="checkbox"/>
Output Description	<input type="text" value="Add output description to distinguish it from other outputs."/>		

5. RTP

If you select this protocol, StreamLink will push the stream to the address you specify.

Output IP address: The IP address StreamLink will push the stream to.

Port: The port StreamLink will push the RTP stream to.

Output Name *	<input type="text" value="Enter an output name"/>	Protocol type *	<input type="text" value="RTP"/>
Output Region *	<input type="text" value="Please select"/>	Output IP address *	<input type="text" value="Enter the output IP address"/>
Port *	<input type="text" value="Please enter the port"/>		
Output Description	<input type="text" value="Add output description to distinguish it from other outputs."/>		

Configuring IP security group

Last updated : 2023-12-23 17:17:37

Overview

Upon completion of creating [events](#) and [flows](#) in [StreamLink](#), when [adding inputs and outputs](#), for input protocols such as SRT Listener, RTMP, and RTP, and output protocols like SRT Listener, RTMP_PULL, and RTSP_PULL, security group can be bound to input/output nodes to perform security verification on corresponding IP addresses. On the security group management page, accessible by clicking on **Security group**, users can add, edit, and delete security group.

The screenshot displays the StreamLink management interface. On the left, a sidebar titled 'demo' contains a 'Flows' section with a search bar and buttons for '+ Create' and 'Bulk operations'. Three flows are listed: 'srt_demo', 'rtmp_demo', and 'test', each with 'Node: Guangzhou' and 'Flow ID' fields. The main area shows the 'srt_demo' flow details, including 'Node: ap-guangzhou', 'Status: Not started', and 'Max bandwidth: 20 Mbps'. A world map is displayed with a blue line connecting 'Frankfurt' in Europe to 'Guangzhou' in Asia. Other cities marked on the map include Silicon Valley, Ashburn, Beijing, Seoul, Tokyo, Chengde, Shanghai, Guangzhou, Hong Kong, Mumbai, Bangkok, and Singapore. At the bottom, an 'Input/Output' section shows two nodes: 'guangzhou (SRT_LISTENER)' and 'frankfurt (SRT_LISTENER)'. A '+ Add' button is visible in the bottom right corner of the Input/Output section.

Security group				
+ Add security group				
Name	Status	ID	Operation	
IPGroup2	None	6565B93E000013D1D3FE	Edit	Delete
IPGroup1	Assigned	6565B31000008CEAFCA4	Edit	Delete

Add security group

Click **Add security group**:

[←](#) **Add security group**

Security group *

IP allowlist ⓘ

Security group: It can be custom-defined, with 1-32 characters, which can be a combination of digits, letters, or underscores "_".

IP allowlist: Enter IP addresses (separate them with semicolons, commas, or line breaks). CIDR format is also supported, for example, "192.168.0.1/24;192.168.1.1/25".

Delete security group

Security group with a status of **None** can be **Delete**. Security group that are Assigned cannot be **Delete**.

Security group				
+ Add security group				
Name	Status	ID	Operation	
IPGroup2	None	6565B93E000013D1D3FE	Edit	Delete
IPGroup1	Assigned	6565B31000008CEAFCA4	Edit	Delete

Binding a security group

For the input protocols: SRT Listener, RTMP, RTP, and output protocols: SRT Listener, RTMP_PULL, RTSP_PULL, you can bind a **Security group** to the input/output nodes in the detailed information. For example: For SRT Listener input, if IPGroup1 is bound in the **Security group**, then only the IPs listed in this allowlist can push streams to this input node.

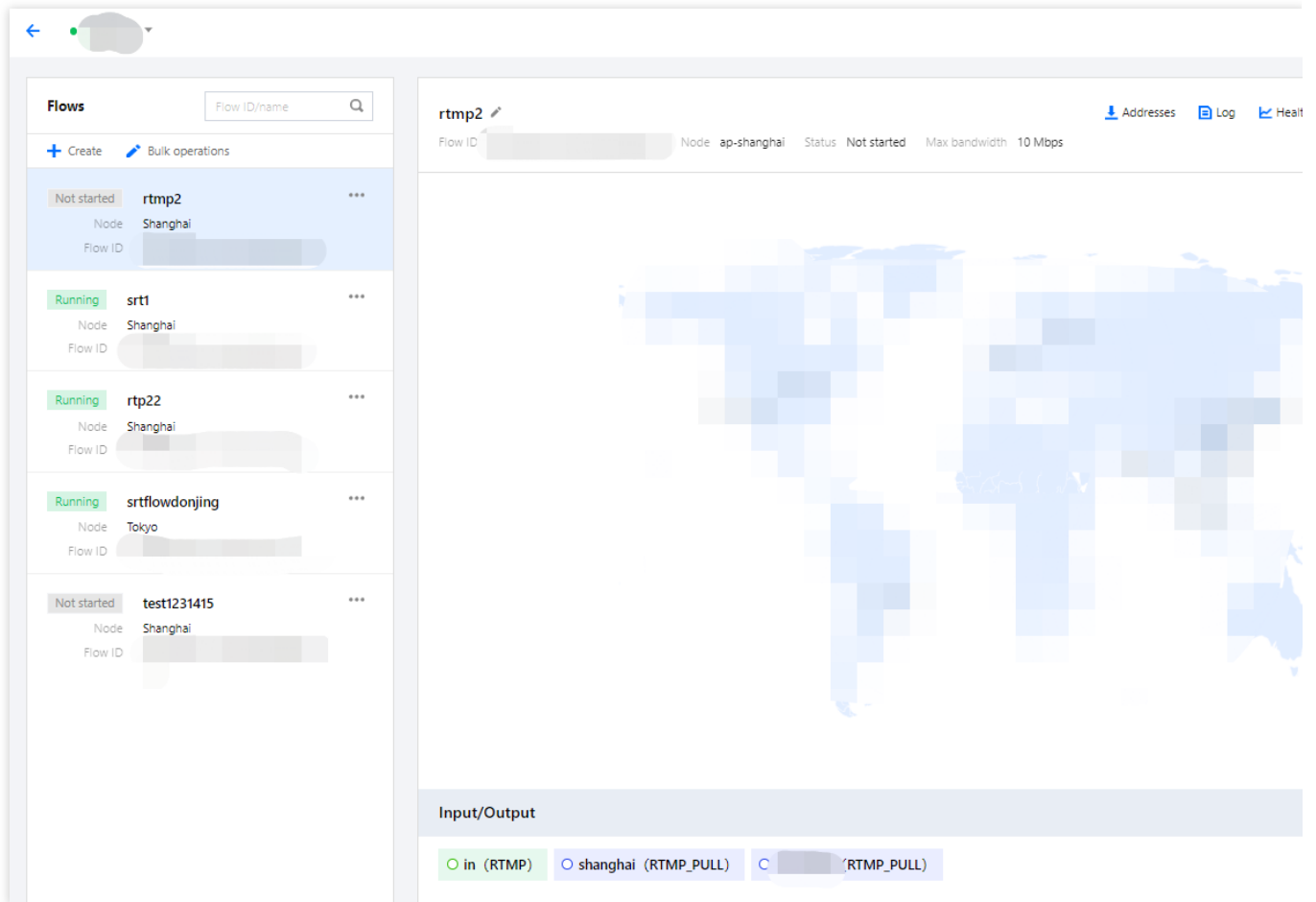
guangzhou

Input name *	<input type="text" value="guangzhou"/>	Protocol type *	<input type="text" value="SRT"/>
Input region	<input type="text" value="Guangzhou"/>	Mode *	<input type="text" value="Listener"/>
Latency setting ⓘ *	<input type="text" value="100"/>	Decryption settings ⓘ	<input type="checkbox"/>
Failover ⓘ	<input type="checkbox"/>		
Security group	<input type="text" value="IPGroup1"/>		
Input source description	<input type="text" value="Add input source description to distinguish it from other input sources."/>		

Starting and Stopping a Flow

Last updated : 2023-12-23 17:18:04

After you [add an input/output](#), it will appear in the **Input/Output** area. You can **Start** or **Stop** the flow in the top right corner.



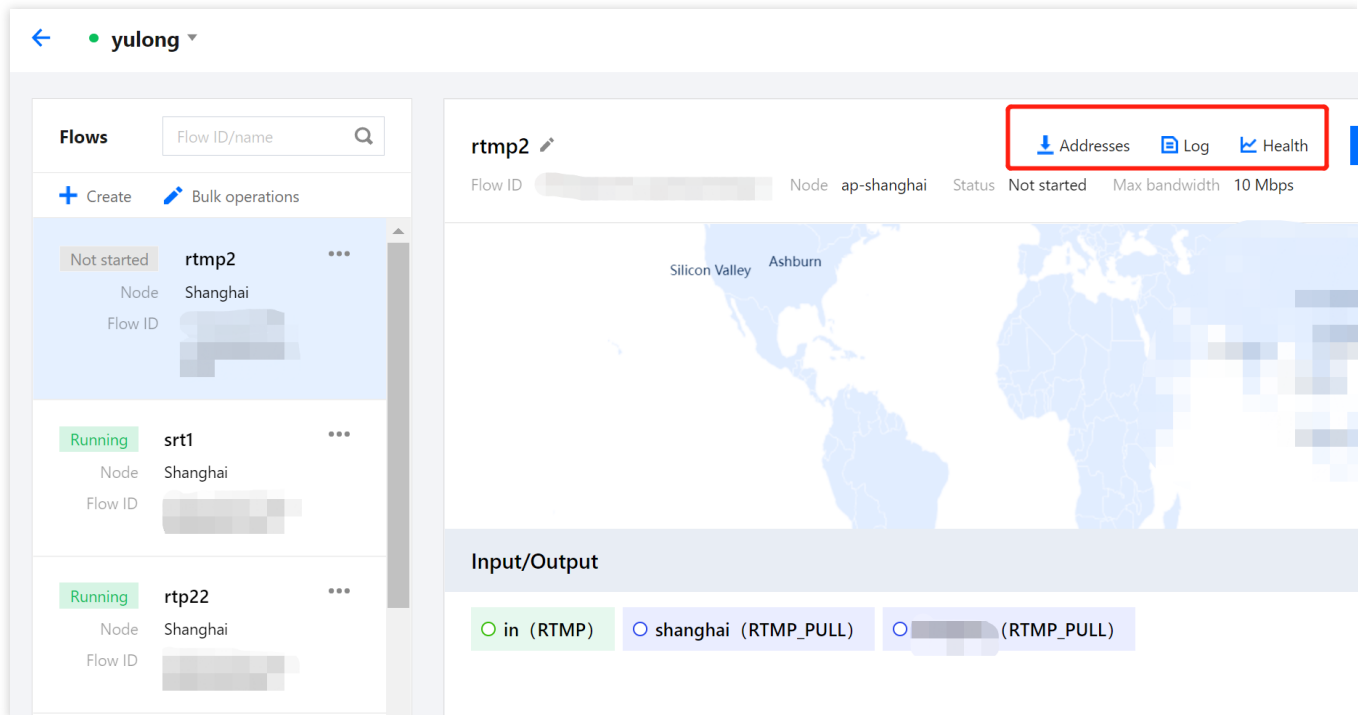
In the **Input/Output** area, you can click an input/output to view its details.

The screenshot displays the Tencent Cloud StreamLink console interface. On the left, a 'Flows' list shows several configurations: 'rtmp2' (Not started, Shanghai), 'srt1' (Running, Shanghai), 'rtp22' (Running, Shanghai), 'srtflowdonjng' (Running, Tokyo), and 'test1231415' (Not started, Shanghai). The main area shows the configuration for the 'rtmp2' flow, which is currently 'Not started'. The 'Input/Output' section at the bottom of the configuration panel shows an input named 'in (RTMP)' and two outputs: 'PULL' and 'TMP_PULL'. A red box highlights the 'in (RTMP)' input in the 'Input/Output' section, and a red arrow points from this box to the 'in' input name field in the configuration details above. The configuration details include fields for 'Input name' (set to 'in'), 'Input Region' (set to 'Shanghai'), and 'Protocol type' (set to 'R'). There are also fields for 'CIDR IP allowlist' and 'Input source description'.

Viewing Addresses, Log, and Health Info

Last updated : 2023-12-23 17:18:39

In the **StreamLink console**, on the details page of a flow, you can click the buttons in the top right to view the addresses, log, and health information of the flow.



Click **Addresses** to view the input/output name and addresses. You can copy the addresses and export the information.

Details ✕

Addresses Log Health

[Export](#)

Name	Type	Input/Output ID	Protocol	Addresses
	Input		RTMP	Address 1: Address 2:
	Output		RTMP_PULL	
	Output		RTMP_PULL	

Click **Log** to view the events that occurred while a flow is running, such as stream pushed, stream interrupted, and IP address blocked.

Details ✕

Addresses **Log** Health

Time Zone: UTC+8 2023-03-03 18:49:49 ~ 2023-03-03 19:49:49 [Confirm](#)

Time ↕	Type ▼	Input/Output Name	Information
No data yet			

Total items: 0 10 / page 1 / 1 page

Click **Health** to view statistics including the frame rate and bitrate of a flow's inputs and outputs.

Details

Addresses Log **Health**

Input Output

Time Zone UTC+8 2023-03-03 18:50:15 ~ 2023-03-03 19:50:15 A B **Confirm**

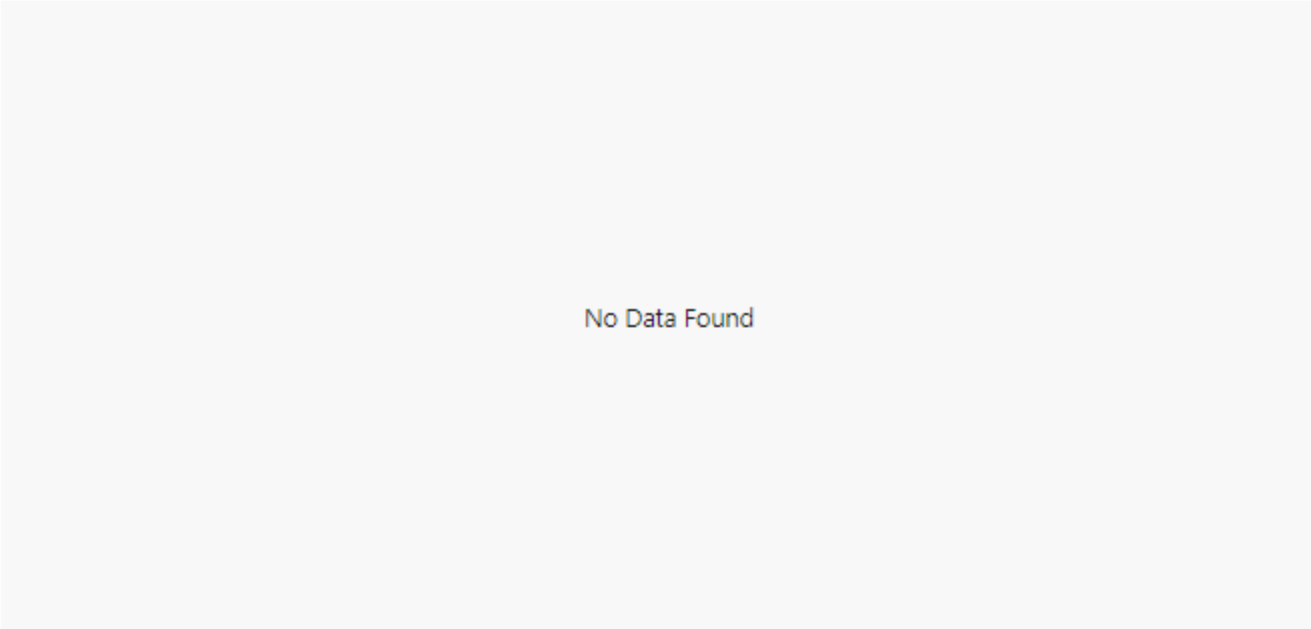
View Data in Last Hour

Select a time range of up to 24 hours in the last 5 days.

Bandwidth

Bandwidth

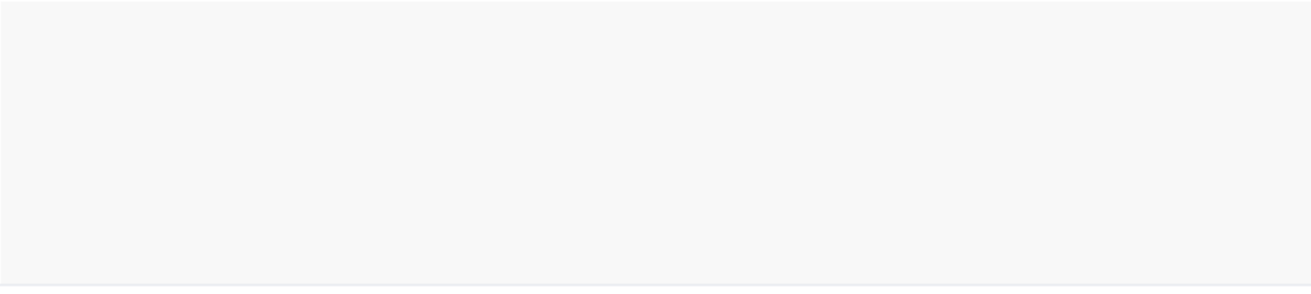
(Kbps)



Video

Bitrate Frame Rate Please select

(Kbps)

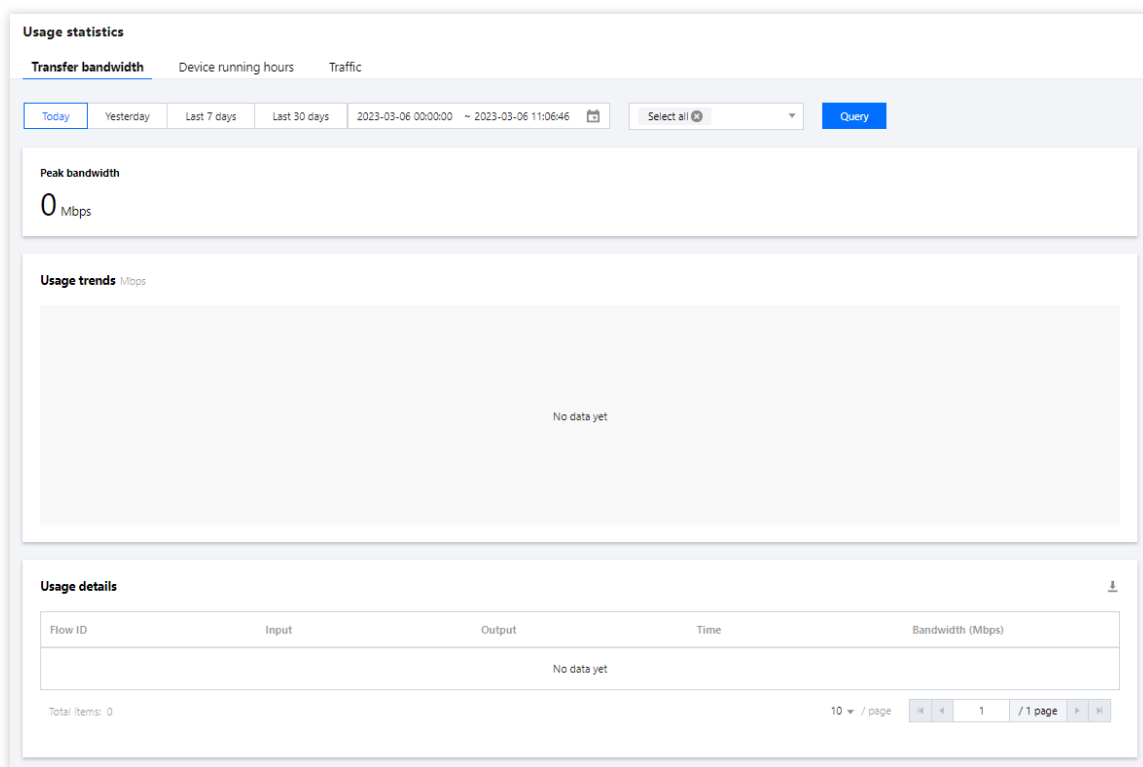


Usage Statistics

Last updated : 2023-12-23 17:19:10

Transfer Bandwidth

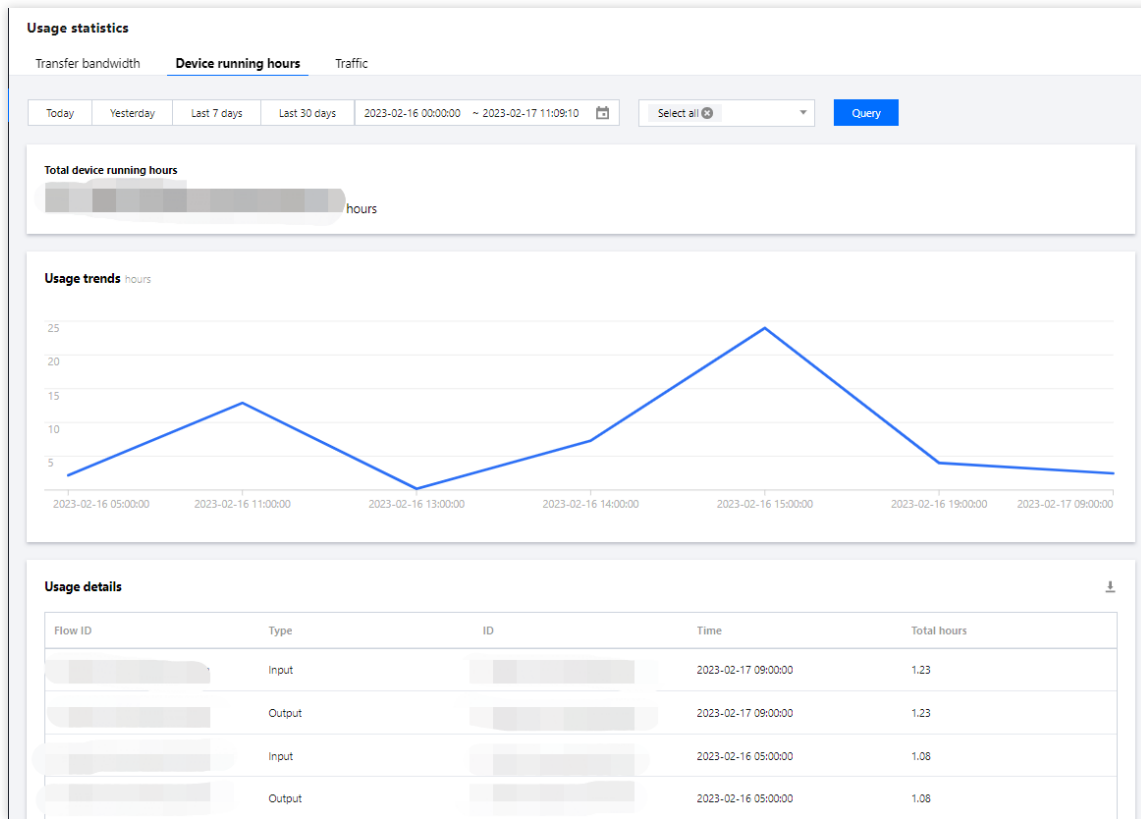
On the usage statistics page, you can view the bandwidth usage of a specific flow in a specific time period. Please note that the line chart shows your total bandwidth usage at different time points, but your daily transfer cost is based on the sum of the peak bandwidth of each flow in a day. In addition to viewing the statistics in the console, you can also export your usage details.



Device Running Hours

Device running costs are based on the running hours of each input/output. For example, if a flow has one input and three outputs, its device running cost will quadruple.

You can view the running hours of a specific flow in a specific time period. In addition to viewing the statistics in the console, you can also export your usage details.



Outbound Traffic

Outbound traffic costs vary with region.

You can view the traffic consumption of a specific flow in a specific time period in different regions. In addition to viewing the statistics in the console, you can also export your usage details.

Usage statistics

Transfer bandwidth Device running hours **Traffic**

Today Yesterday Last 7 days Last 30 days 2023-03-06 00:00:00 ~ 2023-03-06 11:10:24 Select all Query

Total traffic

5110.22 MB

Usage trends MB

Ashburn Silicon Valley Singapore

Usage details

Flow ID	Output node	Output ID	Time	Traffic (MB)
[blurred]	Ashburn	[blurred]	2023-03-06 00:00:00	26.180336999999998
[blurred]	Ashburn	[blurred]	2023-03-06 00:05:00	31.152869
[blurred]	Ashburn	[blurred]	2023-03-06 00:10:00	33.059384
[blurred]	Ashburn	[blurred]	2023-03-06 00:15:00	32.164814
[blurred]	Ashburn	[blurred]	2023-03-06 00:20:00	32.961186000000005