Enterprise Content Delivery Network

Configuration Management

Product Documentation

Tencent Cloud

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

Configuration Management

Configuration Overview

Last updated : 2020-04-28 14:50:49

This document describes how to configure ECDN. You can set ECDN as needed to optimize the acceleration performance.

Basic Configuration

Configuration Name	Document Description
Getting Started	It describes how to activate the service and quickly connect domain names to the service.
Domain Name Connection Configuration	It describes how to connect a domain name to ECDN for acceleration.
CNAME Record Configuration	It describes how to configure a CNAME record.
Domain Name Status Switch	It describes how to enable, disable, and delete domain name acceleration service.
Project Configuration	It describes how to modify a domain name's project and acceleration region.
Origin Server Configuration	It describes how to change the origin server type to origin IP or origin domain.

Advanced Configuration

Configuration Name	Document Description
HTTPS Settings	ECDN supports HTTPS configuration to implement secure acceleration.
HTTP Header Configuration	HTTP header configuration can be added, which will affect the browser's response behaviors.

Configuration Name	Document Description
Cache Rule Configuration	Static cache policies can be configured for domain names with both dynamic and static content.
Alarm Monitoring Configuration	The acceleration service can be monitored and configured with alarms.
Advanced Origin-Pull Configuration	Advanced origin-pull policies based on weight and master/slave architecture are supported.

Basic Configuration

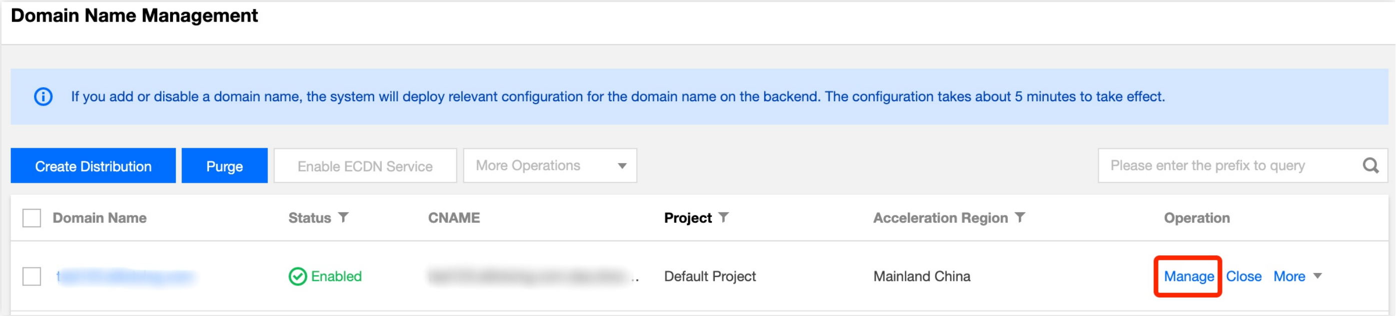
Last updated : 2020-08-28 11:52:45

You can view basic information and origin server information of a domain name in the ECDN Console. You can modify **Project**, **Origin Server Type**, and **Origin Server Address** of the domain name as needed.

- Basic information includes the acceleration domain name, CNAME record, project, and creation time of the acceleration service.
- Origin server information includes origin server type and origin server address.

Domain Name Configuration Page

1. Log in to the ECDN Console and click **Domain Management** on the left sidebar to enter the management page.
2. Select **Manage** on the right of the target configuration domain name to enter the domain name configuration page.

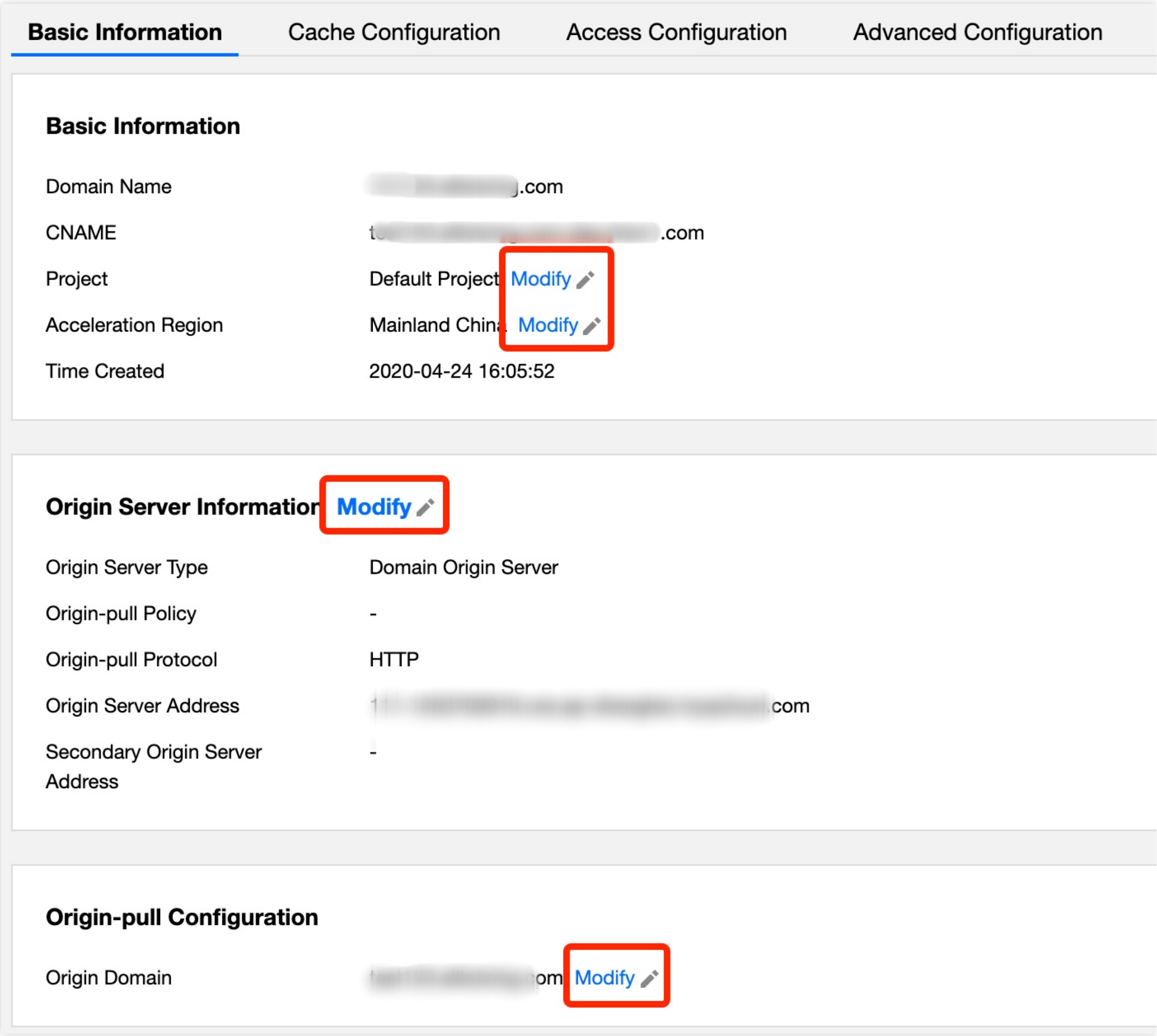


Domain Name Management

If you add or disable a domain name, the system will deploy relevant configuration for the domain name on the backend. The configuration takes about 5 minutes to take effect.

□ Domain Name	Status	CNAME	Project	Acceleration Region	Operation
□ [redacted]	✓ Enabled	[redacted]	Default Project	Mainland China	Manage Close More

3. The **Basic Info** page of the domain name displays its basic configuration information, including the CNAME record, project, acceleration region, origin server information, and origin domain.



Basic Information

Domain Name	[redacted].com
CNAME	t[redacted].com
Project	Default Project
Acceleration Region	Mainland China
Time Created	2020-04-24 16:05:52

Origin Server Information

Origin Server Type	Domain Origin Server
Origin-pull Policy	-
Origin-pull Protocol	HTTP
Origin Server Address	1[redacted].com
Secondary Origin Server Address	-

Origin-pull Configuration

Origin Domain	[redacted]om

Basic Configuration Project

Modifying project of domain name

1. Click **Modify** on the right of the project.
2. In the pop-up window, select the target project name, and click **OK**.

Modifying domain name acceleration region

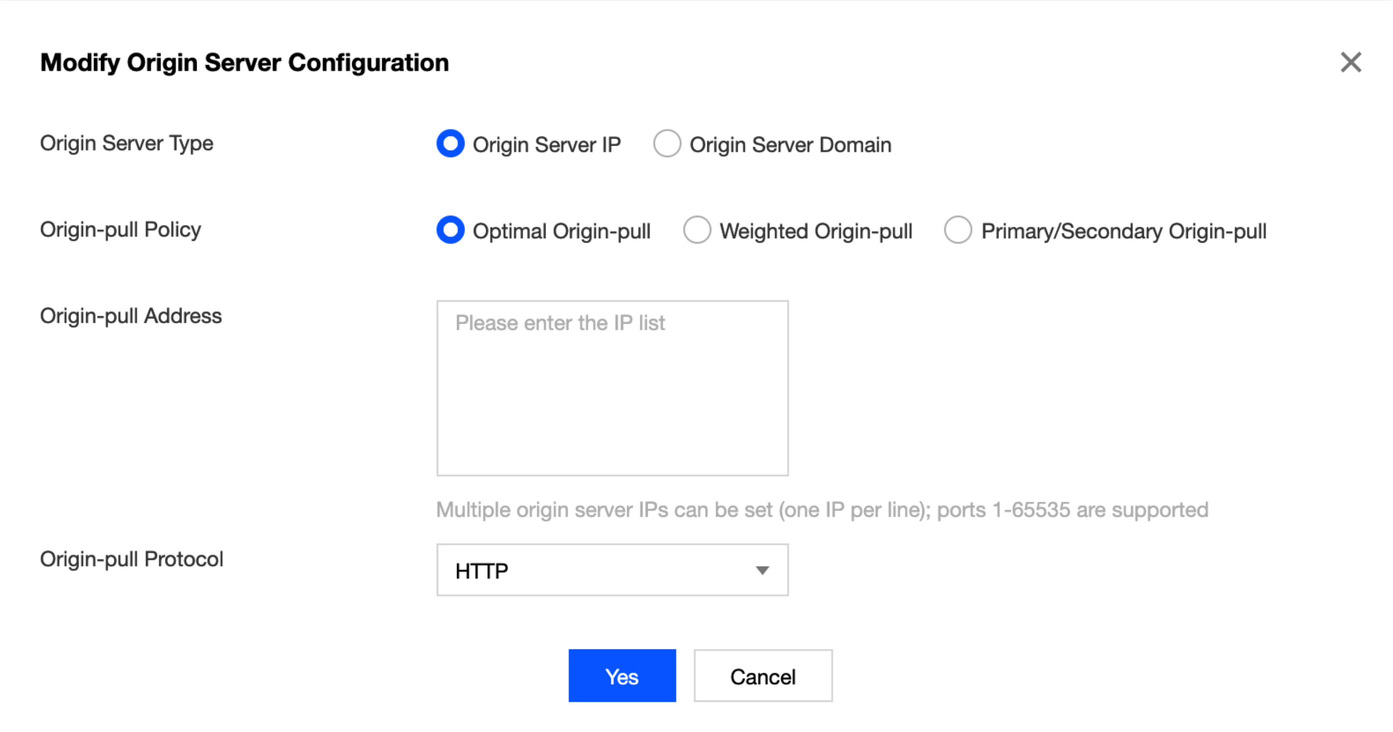
1. Click **Modify** on the right of the acceleration region.

2. Select a domain name acceleration region. Currently, Mainland China, outside Mainland China, or global can be selected.
3. To avoid faulty operations, if you need to delete configuration of an acceleration region, please submit a ticket to apply for modification.

> The acceleration service outside Mainland China is currently in beta test. If your account cannot modify the acceleration region, it indicates that you have not been granted the acceleration permission outside Mainland China. You can submit an application on the ECDN global acceleration eligibility application page, and we will review it in 5 business days and inform you of the result through SMS or internal message.

Modifying origin server configuration

1. Click "Modify" on the right of the origin server configuration to enter the origin server modification page.
2. In the pop-up window, modify your origin server type, origin-pull policy, and origin server address. For more information, please see Advanced Origin-Pull Policies.
3. After the modification is completed, click **OK** to submit the configuration. The system backend will distribute the new origin server modification to the domain name, which will take effect in 3–5 minutes.



Modify Origin Server Configuration

Origin Server Type: ● Origin Server IP ○ Origin Server Domain

Origin-pull Policy: ● Optimal Origin-pull ○ Weighted Origin-pull ○ Primary/Secondary Origin-pull

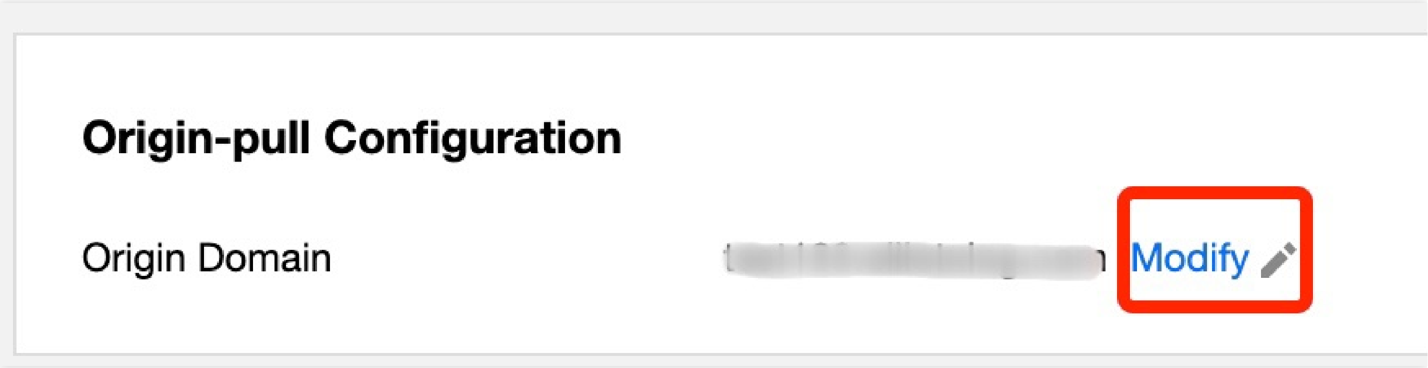
Origin-pull Address: Please enter the IP list

Multiple origin server IPs can be set (one IP per line); ports 1-65535 are supported

Origin-pull Protocol: HTTP

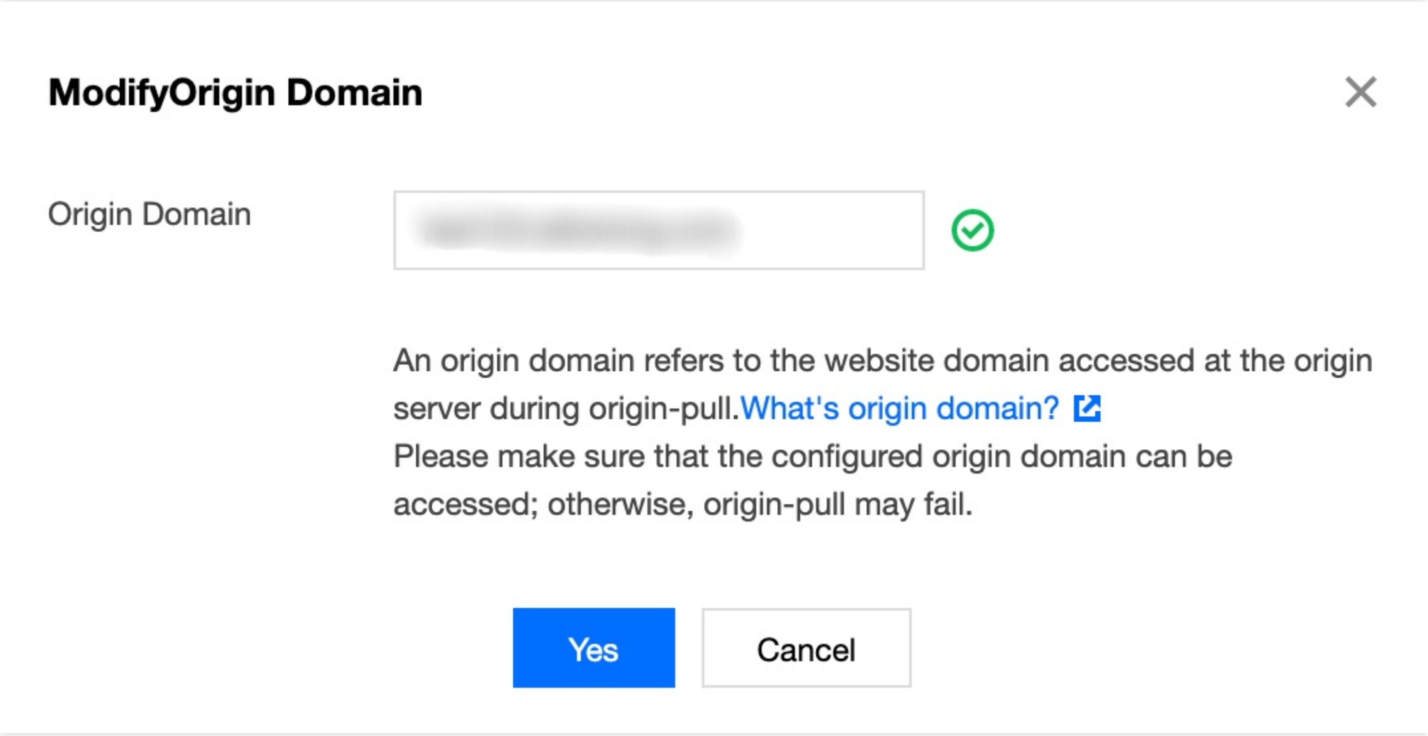
Modifying origin-pull configuration

Click **Edit** next to the origin domain and modify it in the dialog box:



Origin-pull Configuration

Origin Domain [redacted]



ModifyOrigin Domain

Origin Domain [redacted]

An origin domain refers to the website domain accessed at the origin server during origin-pull.What's origin domain?
Please make sure that the configured origin domain can be accessed; otherwise, origin-pull may fail.

Cache Configuration

Last updated : 2020-08-28 12:01:17

Feature Overview

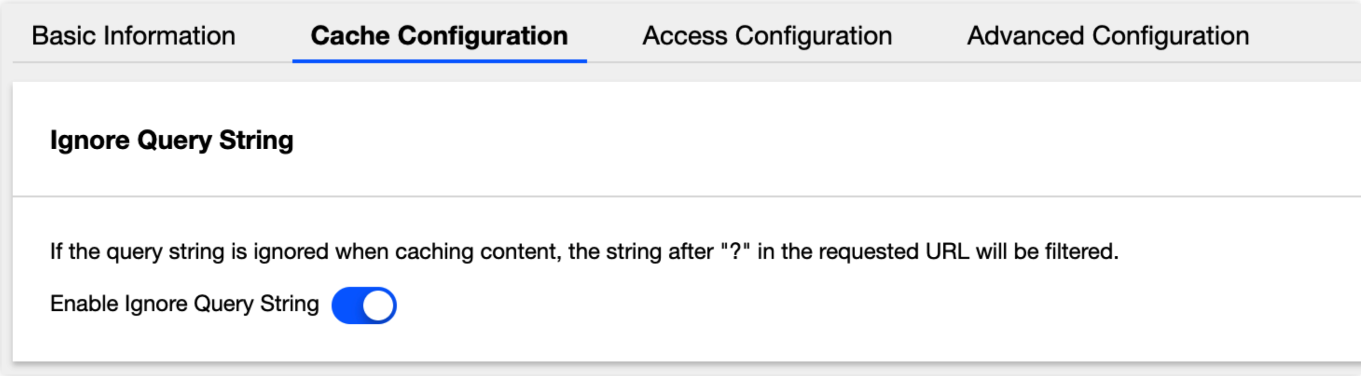
ECDN can automatically detect static/dynamic content access requests based on the configured rules and intelligently choose the most appropriate acceleration scheme, satisfying your needs for accelerating access to sites with static/dynamic hybrid content at one stop.

- For static content requests, the edge servers are preferentially used to cache the content for response, improving access efficiency and reducing origin-pull traffic usage.
- For dynamic content requests, resources are directly pulled from the origin servers through high-quality caching and intelligent routing, reducing the average response latency.

Feature Configuration Guide

1. Log in to the ECDN Console and click **Domain Management** on the left sidebar to enter the management page.
2. In the list, find the domain name to be configured and click **Manage** in the "Operation" column on the right to enter the domain management page.
3. On the "Cache Configuration" page, manage configuration of content caching rules.
   - Ignore Query String cache configuration:
     You can enable Ignore Query String cache to ignore parameters after "?" in the user request URL during caching. For example, when a node caches a resource whose URL is `http://www.example.com/1.jpg?version=1.1` , the corresponding `cache_key` will be `www.example.com/1.jpg` , and parameters after "?" will be ignored. When a user initiates a request, parameters after "?" will also be ignored. The system will use the `cache_key` whose

value is `www.example.com/1.jpg` to search for the resource, which can be hit directly.



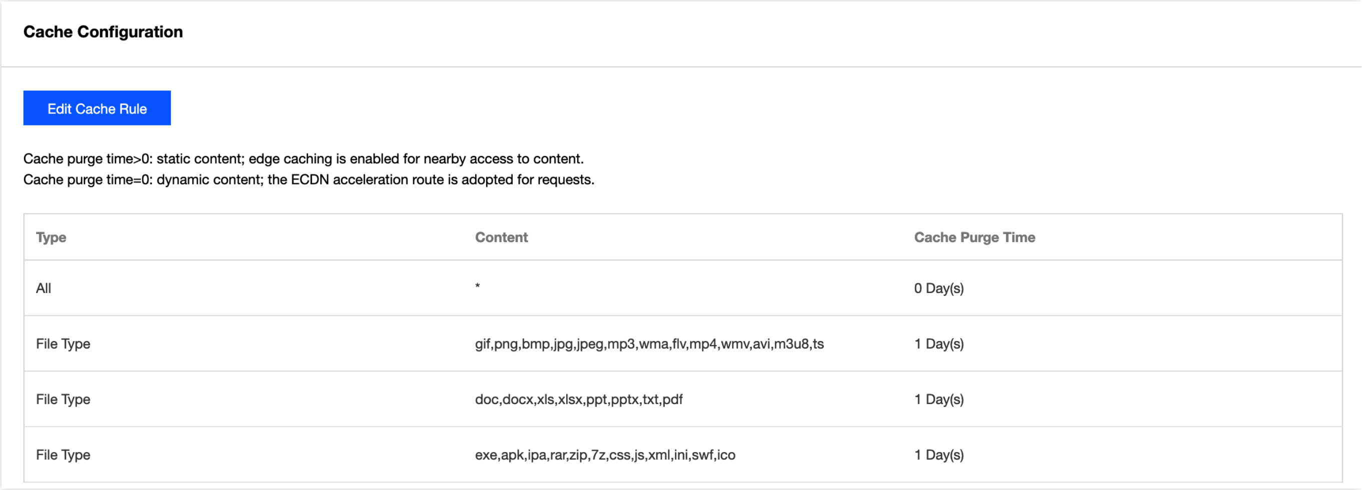
Basic Information | Cache Configuration | Access Configuration | Advanced Configuration

Ignore Query String

If the query string is ignored when caching content, the string after "?" in the requested URL will be filtered.

Enable Ignore Query String

- Content cache configuration:
  Click **Modify Caching Rule** to add a caching rule or modify an existing one and click **Save** for the rule to take effect.



Cache Configuration

Edit Cache Rule

Cache purge time>0: static content; edge caching is enabled for nearby access to content.
Cache purge time=0: dynamic content; the ECDN acceleration route is adopted for requests.

Type	Content	Cache Purge Time
All	*	0 Day(s)
File Type	gif,png,bmp,jpg,jpeg,mp3,wma,flv,mp4,wmv,avi,m3u8,ts	1 Day(s)
File Type	doc,docx,xls,xlsx,ppt,pptx,txt,pdf	1 Day(s)
File Type	exe,apk,ipa,rar,zip,7z,css,js,xml,ini,swf,ico	1 Day(s)

Caching rule types

Cache Type	Description	Example	Remarks

File Type	Sets the caching time based on file extension	.jpg;
		.png;
		.jsp
			1. The content is case-sensitive and must be a file extension starting with `.`.
			2. Different file types should be separated with `;`.

Folder	Sets the caching time based on folder	/access; /pic	1. The content is case-sensitive, and different paths should be separated with `;`. 2. It must be a folder starting with `/`. 3. It cannot end with `/`.

Full-path file	Sets the caching time for a specified file	/a.jpg; /b.png	1. The content is case-sensitive, and files at different paths should be separated with `;`. 2. `*` can be used to match a type of files by regex, such as `/test/abc/*.jpg`. 3. It must be a folder starting with `/`.
Homepage	Sets the caching time for the homepage	/	The homepage content to be cached is "/" by default and does not need to be modified.

Cache purge time

Cache purge time description

- Cache purge time can be set by second, minute, hour, and day (up to 30 days).
- If the cache purge time is 0, it indicates dynamic content, all requests will be directly passed through to the origin server, and the response content will not be cached.
- If the cache purge time is greater than 0, it indicates static resource, and the edge caching feature will be enabled:
  - If the content accessed by the user has been cached on the edge server, and the cache has not expired, then the request does not need to be forwarded to the origin server, and the cached content will be directly returned, so that the user can enjoy nearby access to the content.
  - If the content accessed by the user has not been cached on the edge server, or the cache has expired, then the request needs to be forwarded to the origin server to get the content, which will be returned to the user and cached on the edge server.
- When a domain name is connected, the cache purge time of all files is 0 seconds by default, indicating that the dynamic acceleration service is not used by default.

Suggestions on setting cache purge time

File Type	Scenario Example	Recommended Caching Time
Basically unchanged static content	Images and audio/video files	Set the cache purge time to 30 days.
Static content that needs to be frequently updated	Files in formats such as .js and .css	Set the caching time generally at the day or hour level based on the update frequency.
Dynamic content that is frequently	Weather queries and region-specific portal content	Set the caching time at the minute or second

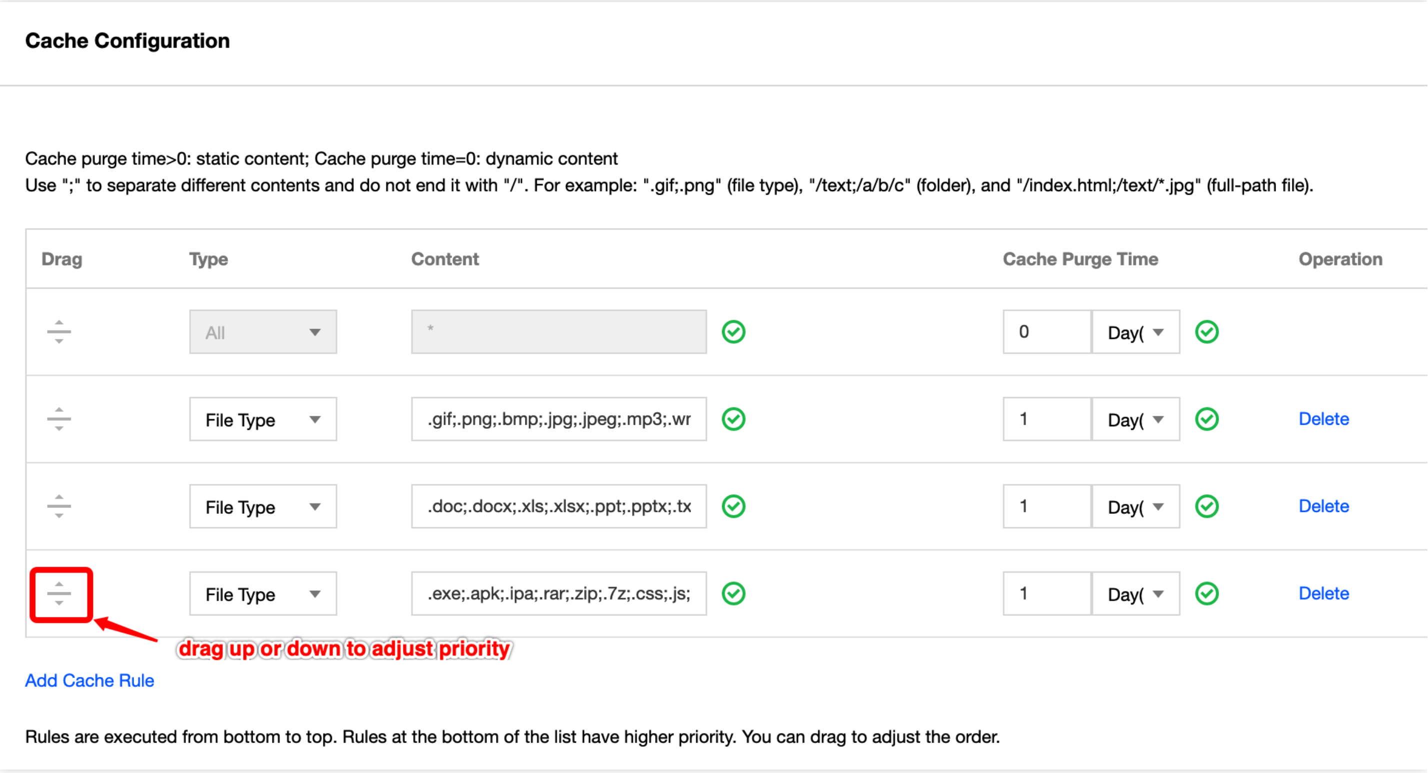
updated and shared by users		level.
Content that is dynamically generated or cannot be accessed twice by the same user	User registration and login APIs	Set the caching time to 0 to disable caching.

Caching rule priority

If multiple caching policies are set, there may be overlapping rules, and a request may hit multiple rules. Therefore, there is priority order for caching rules.

- The rule at the bottom of the configuration list has higher priority than that on the top, and a new caching rule has the highest priority by default.
- A user request will be matched with caching rules by rule priority from high to low. The first hit rule determines the cache purge time of the request.
- You can adjust the priority of rules.

Click **Edit Caching Rule**. You can **drag the icon** to adjust the rule priority.



Cache Configuration

Cache purge time>0: static content; Cache purge time=0: dynamic content
Use ";" to separate different contents and do not end it with "/". For example: ".gif;.png" (file type), "/text;/a/b/c" (folder), and "/index.html;/text/*.jpg" (full-path file).

Drag	Type	Content	Cache Purge Time	Operation
	All	* ✓	0 Day(✓	
	File Type	.gif;.png;.bmp;.jpg;.jpeg;.mp3;.wr ✓	1 Day(✓	Delete
	File Type	.doc;.docx;.xls;.xlsx;.ppt;.pptx;.tx ✓	1 Day(✓	Delete
	File Type	.exe;.apk;.ipa;.rar;.zip;.7z;.css;.js; ✓	1 Day(✓	Delete

drag up or down to adjust priority

Add Cache Rule

Rules are executed from bottom to top. Rules at the bottom of the list have higher priority. You can drag to adjust the order.

Cache Inheritance

- When you configure edge caching for static content, the ECDN system will use the caching rules configured on the platform to process static user requests by default. The `Cache-Control` field in the response header from the origin server will not be inherited by the node for processing by default.

Access Control

IP Access Limit Configuration

Last updated : 2020-07-29 14:16:47

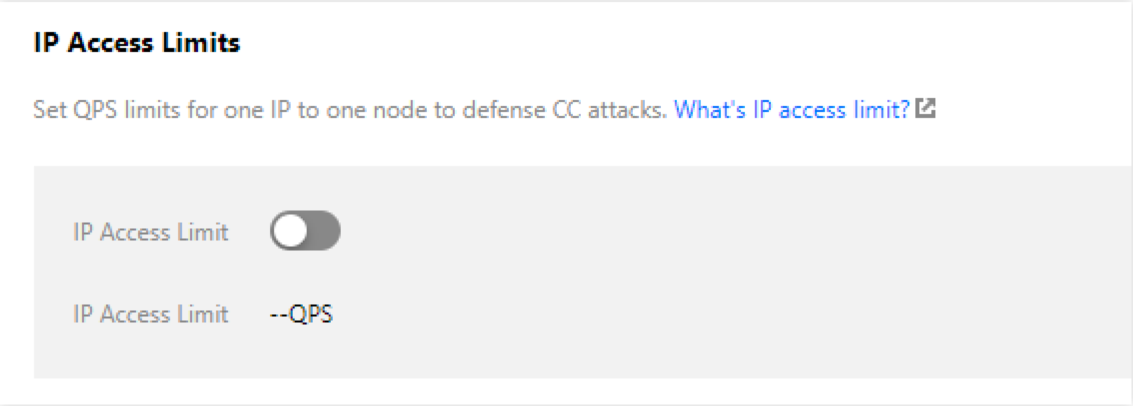
Configuration Scenario

To control the source of access to your business resources, you can use the IP access limit feature in ECDN. By limiting the number of access requests to a node per second from a client IP, you can defend against high-frequency CC attacks and prevent hotlinking by malicious users.

Configuration Guide

Viewing configuration

Log in to the ECDN Console, select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. You will find the IP access frequency limit configuration in **Access Configuration**. It is disabled by default:



IP Access Limits

Set QPS limits for one IP to one node to defense CC attacks. What's IP access limit?

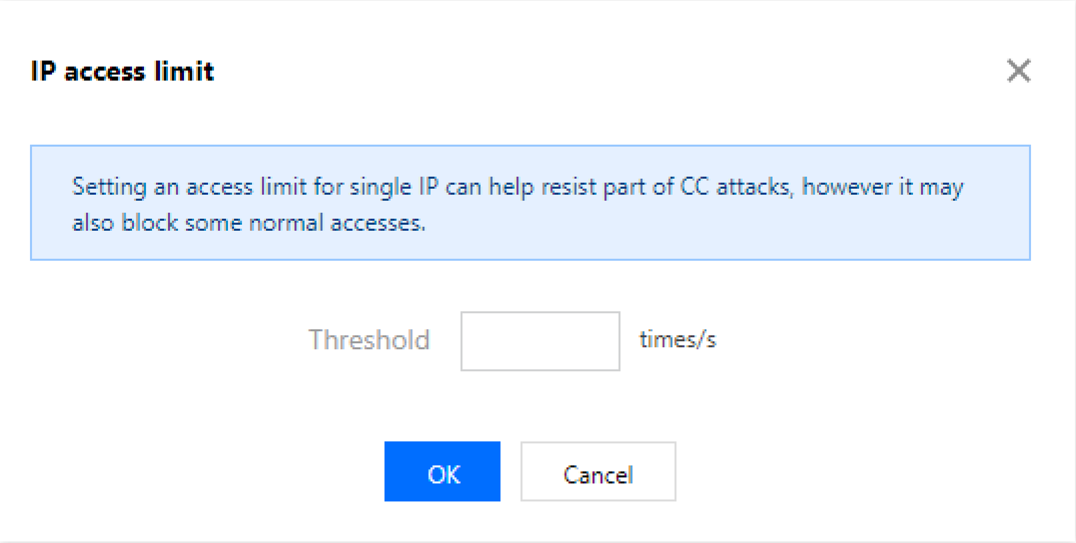
IP Access Limit ○

IP Access Limit --QPS

Modifying configuration

1. Modify the configuration

Enter the frequency threshold and click **OK** to enable IP access limit.



IP access limit

Setting an access limit for single IP can help resist part of CC attacks, however it may also block some normal accesses.

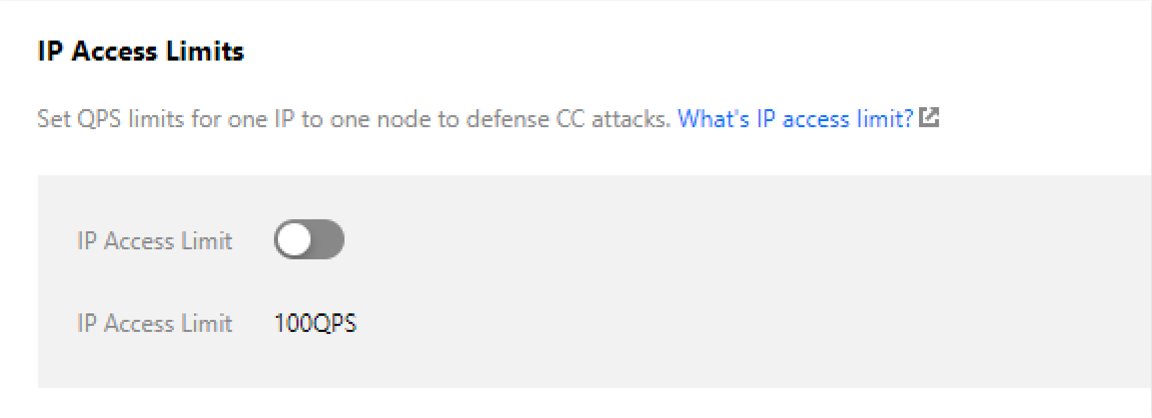
Threshold ______ times/s

Configuration description

- After the configuration is enabled, a 514 error will be returned for requests that exceed the QPS limit. A low access frequency limit may impact the normal use of your business by high-frequency users. Configure the proper threshold according to your actual business conditions and use cases.
- IP access limit is effective for attacks from a single IP to a single node. If a malicious user uses a high number of IPs to attack nodes on your entire network, this feature is no longer applicable.

2. Disable the configuration

You can switch to disable this feature. When the switch is off, this feature does not take effect in the production environment even if there is an existing configuration. When the switch is on, this configuration will take effect across the entire network:



IP Access Limits

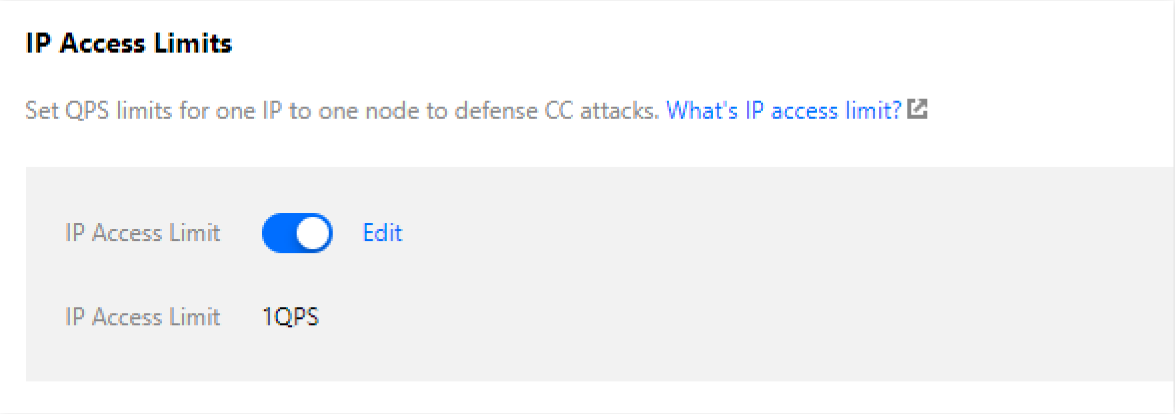
Set QPS limits for one IP to one node to defense CC attacks. What's IP access limit?

IP Access Limit

IP Access Limit 100QPS

Configuration Sample

Suppose the IP access limit for the acceleration domain name `www.test.com` is as follows:



IP Access Limits

Set QPS limits for one IP to one node to defense CC attacks. What's IP access limit?

IP Access Limit Edit

IP Access Limit 1QPS

The actual access status will be as follows:

1. If a user with client IP `1.1.1.1` requests the resource `http://www.test.com/1.jpg` for 10 times in one second, and all access requests are made to one server on ECDN cache node A, then 10 access logs will be generated on this server, 9 of which exceed the QPS limit, and the status code "514" will be returned.
2. If a user with client IP `2.2.2.2` requests the resource `http://www.test.com/1.jpg` twice in one second, and the access requests may be distributed to two ECDN cache nodes for processing due to network conditions, then each node will return the content normally.

IP Blocklist/Allowlist Configuration

Last updated : 2020-07-29 14:16:47

Configuration Scenario

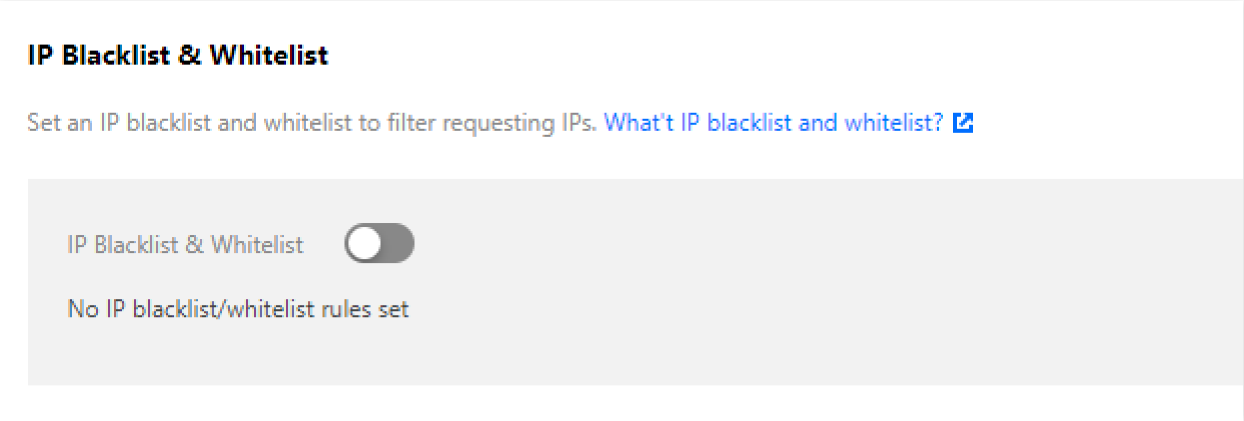
To control the source of access to your business resources, you can use the IP blocklist/allowlist feature in Tencent Cloud ECDN.

By configuring an access control policy on IPs of user requests, you can effectively control the source of access to prevent hotlinking by malicious IPs, attacks, etc.

Configuration Guide

Viewing configuration

Log in to the ECDN Console, select **Domain Management** on the left sidebar, and click **Manage** on the right of a domain name to enter its configuration page. You will find the IP blocklist/allowlist configuration in **Access Configuration**.



IP Blacklist & Whitelist

Set an IP blacklist and whitelist to filter requesting IPs. What't IP blacklist and whitelist?

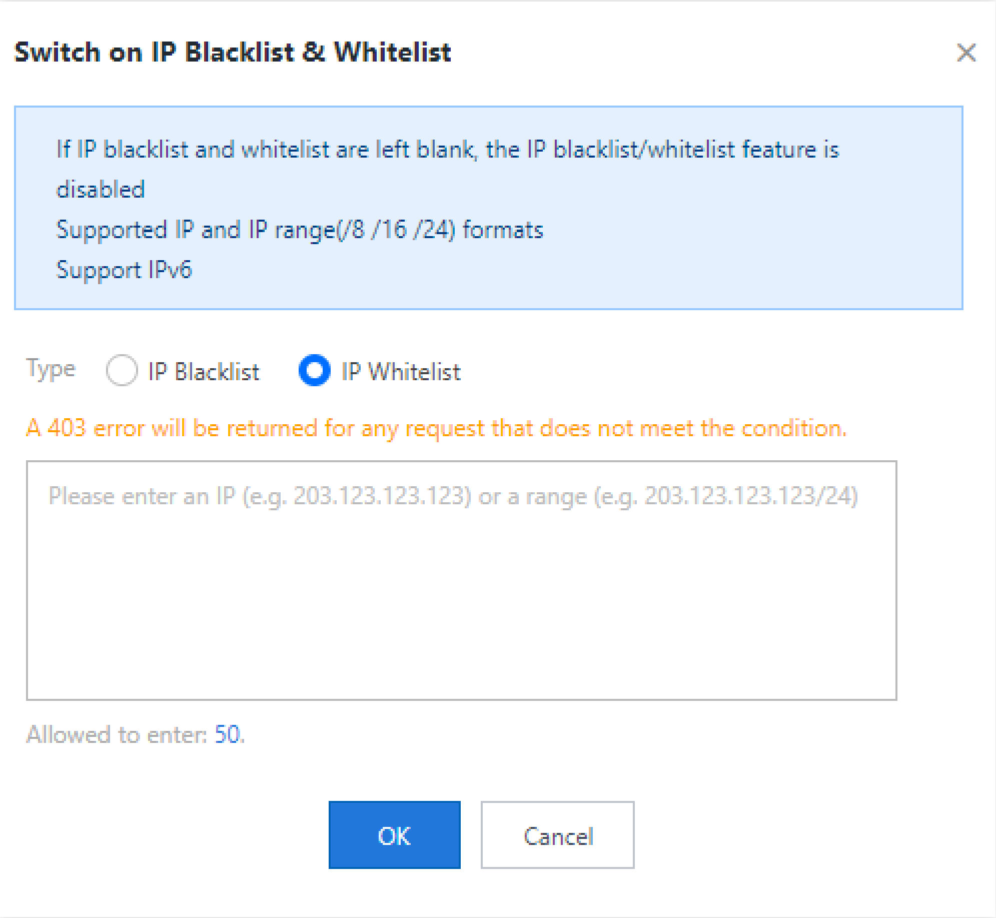
IP Blacklist & Whitelist ○

No IP blacklist/whitelist rules set

Modifying configuration

1. Modify the configuration

Click **Edit** to select "IP Blocklist" or "IP Allowlist", enter the list of IPs or IP ranges, and click **OK** to enable IP blocklist/allowlist configuration:



Switch on IP Blacklist & Whitelist

If IP blacklist and whitelist are left blank, the IP blacklist/whitelist feature is disabled
Supported IP and IP range(/8 /16 /24) formats
Support IPv6

Type ○ IP Blacklist ● IP Whitelist

A 403 error will be returned for any request that does not meet the condition.

Please enter an IP (e.g. 203.123.123.123) or a range (e.g. 203.123.123.123/24)

Allowed to enter: 50.

IP blocklist

If a client IP matches an IP or IP range in the blocklist, the accessed ECDN node will directly return a 403 status code.

IP allowlist

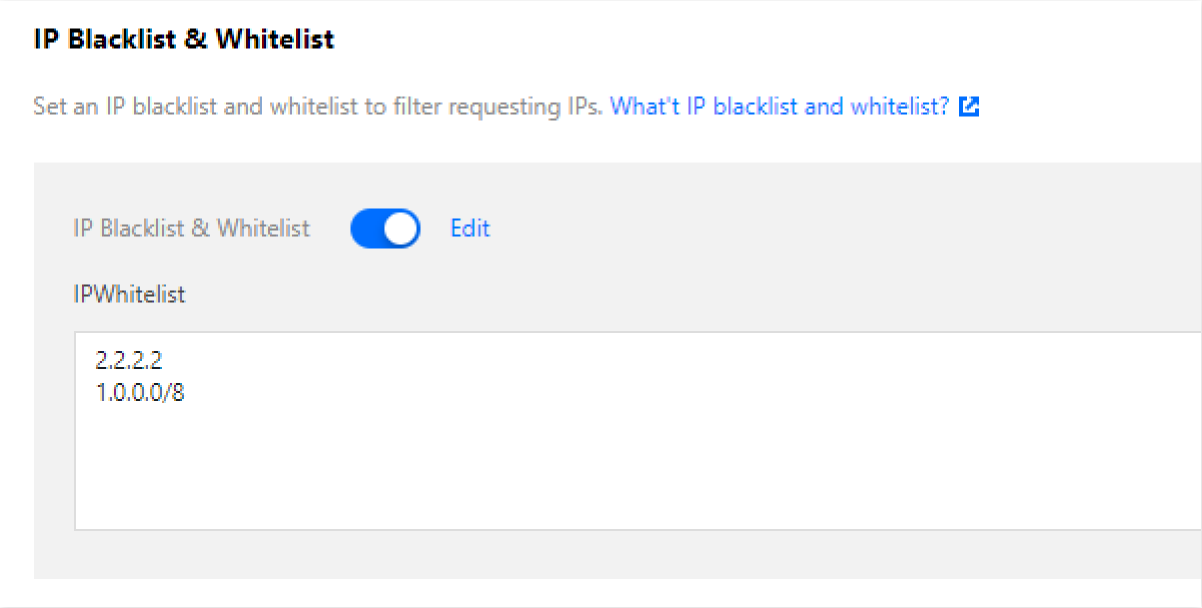
If a client IP does not match any IP or IP range in the allowlist, the accessed ECDN node will directly return a 403 status code.

Blocklist/Allowlist rules

- The IP blocklist and allowlist are mutually exclusive and cannot be configured at the same time.
- Only IP ranges `/8` , `/16` , `¥24` , and `/32` are supported.
- The blocklist/allowlist does not support entries in `IP:port` format and can contain up to 50 entries.

Configuration Sample

Suppose the IP blocklist/allowlist of the acceleration domain name `www.test.com` is as follows:



IP Blacklist & Whitelist

Set an IP blacklist and whitelist to filter requesting IPs. What't IP blacklist and whitelist?

IP Blacklist & Whitelist ● Edit

IPWhitelist

2.2.2.2
1.0.0.0/8

The actual access status will be as follows:

1. When a user with client IP `1.1.1.1` accesses the resource `http://www.test.com/test.txt` , as the IP matches an IP in the allowlist, the requested content will be returned.
2. When a user with client IP `2.1.1.1` accesses the resource `http://www.test.com/test.txt` , as the IP does not match any IP in the allowlist, a 403 status code will be returned.

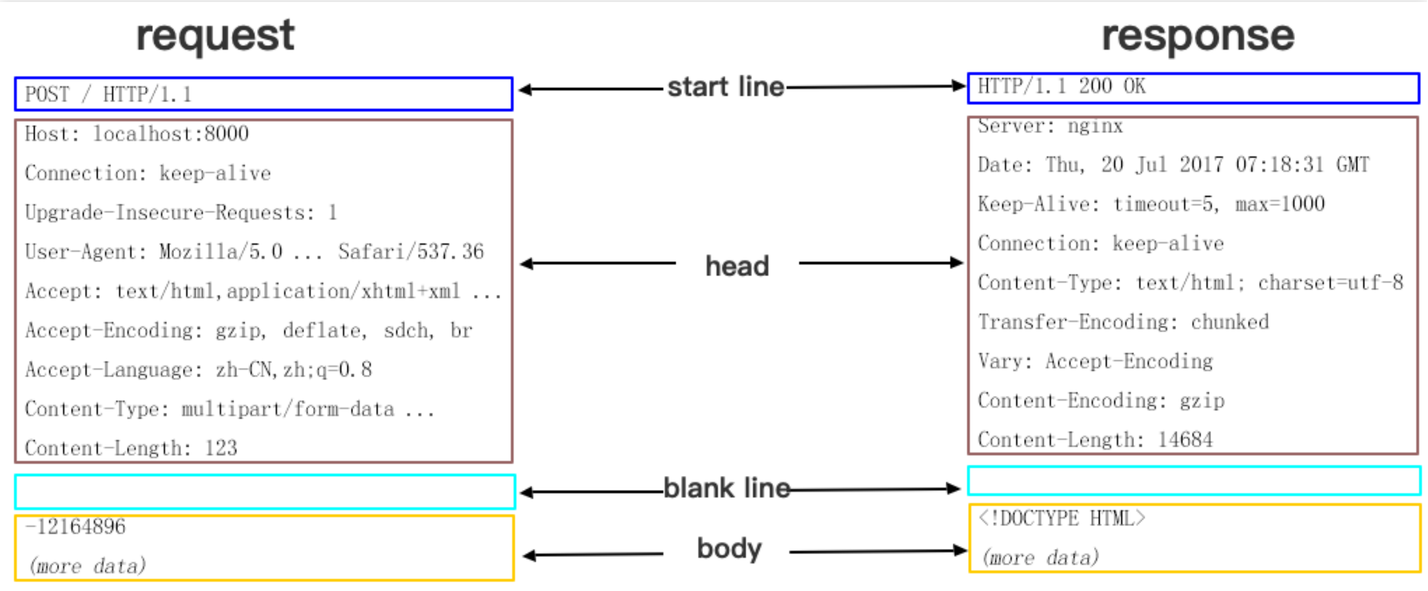
Advanced Configuration
Configure HTTP Header

Last updated : 2020-04-28 14:50:51

An HTTP message generally contains:

- Request message sent from client to server.
- Response message sent from server to client.

These messages all consist of a beginning line, one or multiple headers, a blank line indicating the end of headers, and an optional message body.



```
POST / HTTP/1.1
Host: localhost:8000
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 ... Safari/537.36
Accept: text/html,application/xhtml+xml ...
Accept-Encoding: gzip, deflate, sdch, br
Accept-Language: zh-CN,zh;q=0.8
Content-Type: multipart/form-data ...
Content-Length: 123

-12164896
(more data)
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 20 Jul 2017 07:18:31 GMT
Keep-Alive: timeout=5, max=1000
Connection: keep-alive
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 14684

<!DOCTYPE HTML>
(more data)
```

HTTP headers divide into common header, request header, response header, and entity header. Each header consists of a domain name, colon (":"), and domain value, such as `Connection:keep-alive` .
If you use the HTTP header configuration feature provided by ECDN, when an end user requests a business resource, you can add a custom header in the returned **response message** to implement cross-origin access.

- As the HTTP header configuration is for a specified domain name, once the configuration takes effect, the configured header will be added to the response messages of user requests for any resource under this domain name.
- HTTP header configuration affects only response of the client (such as browser) rather than ECDN node's caching behaviors.

Configuration Description

ECDN allows you to configure the following headers:

- Content-Disposition: it activates download in the browser and sets the default filename of the downloaded file.
- Content-Language: it specifies the language used in the client (such as browser) response for the resource.
- Access-Control-Allow-Origin: it specifies the sources of cross-origin requests allowed to access the resource.
- Access-Control-Allow-Methods: it specifies the allowed methods of cross-origin requests.
- Access-Control-Max-Age: it specifies the validity period for caching the returned result of preflight request for a particular resource when a cross-origin request is initiated.
- Access-Control-Expose-Headers: it specifies the headers visible to the client when a cross-origin request is initiated.

General configuration

Content-Disposition

`Content-Disposition` is used to activate download in the browser and set the default filename of the downloaded resource. When the server sends a file to the client browser, if it is in a type supported by the browser, such as .txt or .jpg, it will be directly opened in the browser by default. If you want to ask the user to save the file, you can configure the `Content-Disposition` field to override the browser's default behavior. The common configuration is `Content-Disposition:attachment;filename=FileName.txt`

Content-Language

`Content-Language` specifies the code of the language used by the webpage. Common configurations are as follows:

- `Content-Language: zh-CN`
- `Content-Language: en-US`

Cross-Origin access configuration

Cross-origin access refers to a scenario where a resource under a domain name, such as `www.abc.com` , initiates a request to another resource under another domain name, such as `www.def.com` . As the resource domain names are different, **cross-origin access** will occur. Using different protocols or ports can cause cross-origin access. You need to add configuration related to cross-origin access in the response header to make the first resource get the desired data.

Access-Control-Allow-Origin

`Access-Control-Allow-Origin` is used to solve the problem of cross-origin permissions of resources. Its value specifies the origins that can access the resource. You can also set the wildcard `¥*` to allow all origins to access the resource. Common configurations are as follows:

- `Access-Control-Allow-Origin: *`
- `Access-Control-Allow-Origin: http://www.test.com`

Pay attention to the following limits when configuring `Access-Control-Allow-Origin` :

- Do not use wildcard domain names, e.g., `*.qq.com` .
- Only configure it as `¥*` or specify a URI.
- When configuring a specified domain name, add the "http://" or "https://" prefix.

Access-Control-Allow-Methods

`Access-Control-Allow-Methods` is used to specify the HTTP request methods allowed for cross-origin access. Multiple methods can be set as follows:
`Access-Control-Allow-Methods: POST, GET, OPTIONS`

Access-Control-Max-Age

`Access-Control-Max-Age` specifies the validity period of a preflight request.
For a non-simple cross-origin request, before the formal communication, an HTTP query request called "preflight request" needs to be made to check whether the cross-origin request is secure and acceptable. The following requests are considered as non-simple cross-origin requests:

- The request is initiated in a method other than `GET` , `HEAD` , and `POST` or is initiated by using `POST` with a data type other than `application/x-www-form-urlencoded` , `multipart/form-data` , and `text/plain` , such as `application/xml` or `text/xml` .
- A custom request header is used.

`Access-Control-Max-Age` is measured in seconds. Here, the configuration sample `Access-Control-Max-Age: 1728000` indicates that no more preflight requests will be sent for the cross-domain access to this resource within 1,728,000 seconds (20 days).

Access-Control-Expose-Headers

`Access-Control-Expose-Headers` specifies which headers can be accessed when a cross-region request is initiated. By default, the following six types of headers can be exposed to the client:

- Cache-Control
- Content-Language
- Content-Type

- Expires
- Last-Modified
- Pragma

If you want the client to access other header information, you can set as follows (separate multiple headers with `;`):
`Access-Control-Expose-Headers: Content-Length, QCloud-DSA-MyCustom-HeaderY`

Then, the server will allow requests to contain the `Content-Length` and `QCloud-DSA-MyCustom-HeaderY` fields.

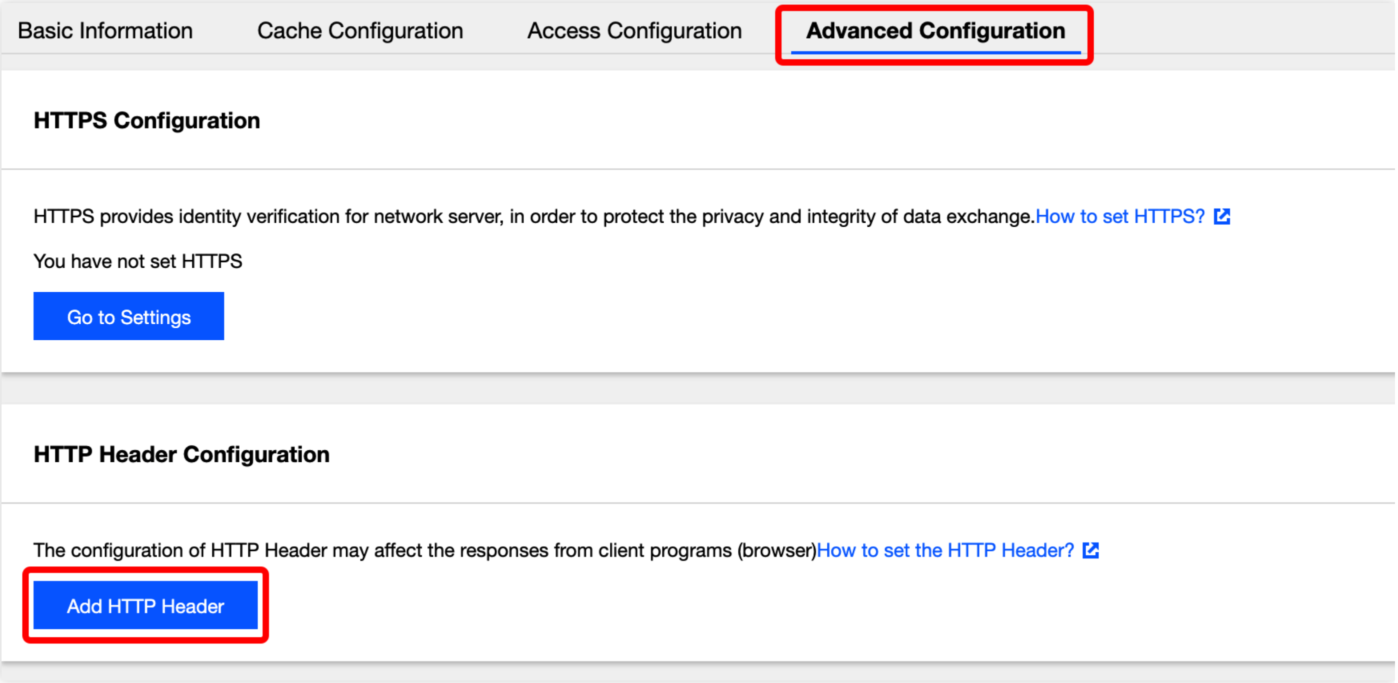
Custom header

ECDN allows you to add custom headers as needed.
The following fields cannot be added currently:

```
Date
Expires
Content-Type
Content-Encoding
Content-Length
Transfer-Encoding
Cache-Control
If-Modified-Since
Last-Modified
Connection
Content-Range
ETag
Accept-Ranges
Age
Authentication-Info
Proxy-Authenticate
Retry-After
Set-Cookie
Vary
WWW-Authenticate
Content-Location
Content-MD5
Content-Range
Meter
Allow
Error
```

Configuration process

1. Log in to the ECDN Console and click **Domain Management** on the left sidebar. On the management page, click **Manage** on the right of the target domain name to enter the domain management page.
2. Click **Advanced Configuration** and click **Add HTTP Header** in the **HTTP Header Configuration** module.



Basic Information | Cache Configuration | Access Configuration | Advanced Configuration

HTTPS Configuration

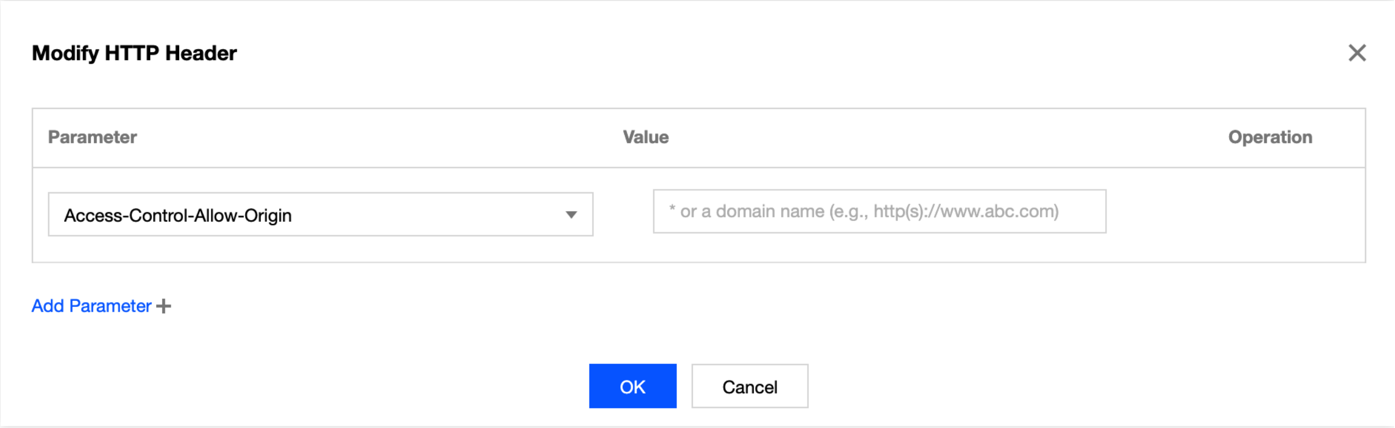
HTTPS provides identity verification for network server, in order to protect the privacy and integrity of data exchange.How to set HTTPS?

You have not set HTTPS

HTTP Header Configuration

The configuration of HTTP Header may affect the responses from client programs (browser)How to set the HTTP Header?

3. In the pop-up window, select the HTTP header to be added and enter the corresponding value. You can click **Add Parameter** to add more header fields. Click **OK** to submit the settings.

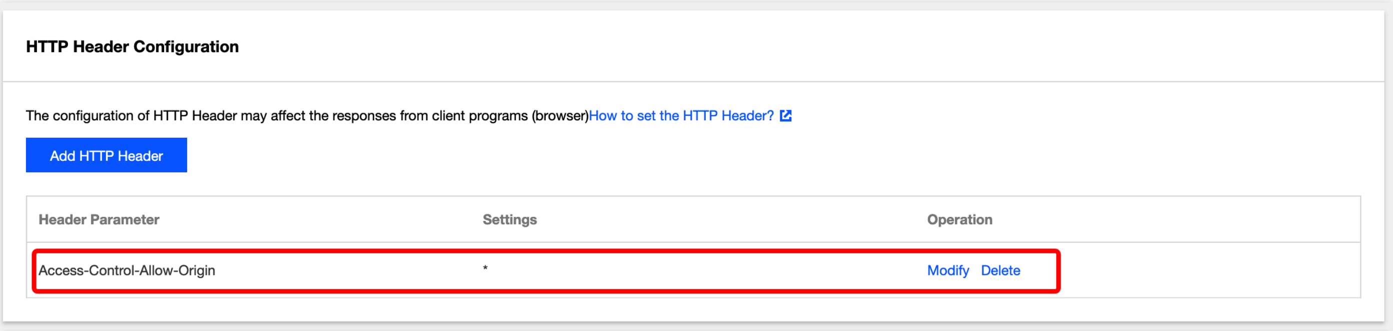


Modify HTTP Header

Parameter	Value	Operation
Access-Control-Allow-Origin	* or a domain name (e.g., http(s)://www.abc.com)	

4. The configuration will take effect in about 5 minutes. In the table at the bottom, you can view the added HTTP headers. You can click **Modify** or **Delete** on the right of a header to perform the

corresponding operation as needed.



HTTP Header Configuration

The configuration of HTTP Header may affect the responses from client programs (browser)How to set the HTTP Header?

Header Parameter	Settings	Operation
Access-Control-Allow-Origin	*	Modify Delete

5. You can click **Add HTTP Header** to add more HTTP headers, each of which can be added only once.

HTTPS Configuration

Last updated : 2020-04-30 09:44:54

Configuration Description

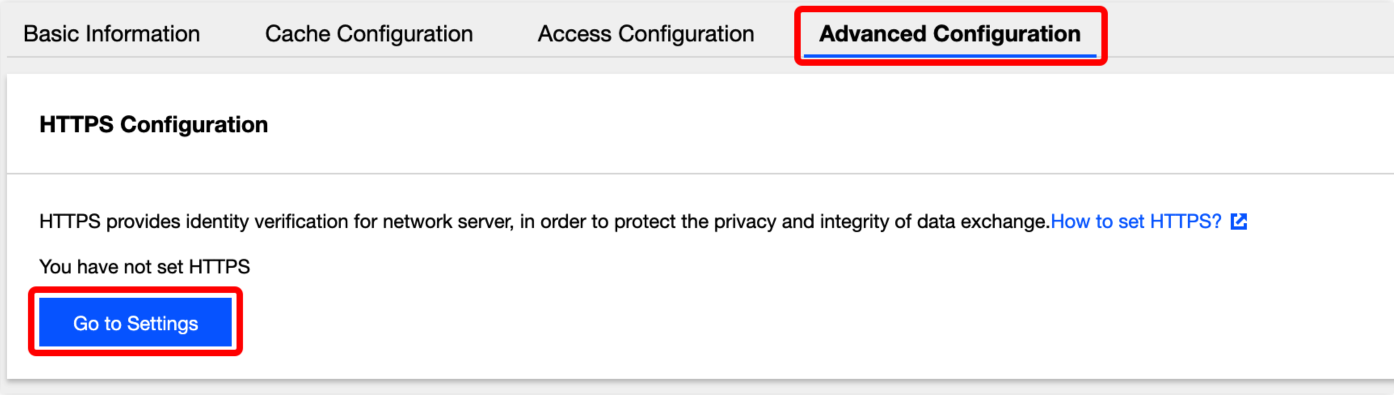
HTTPS refers to Hypertext Transfer Protocol Secure, which is a security protocol that encrypts and transfers data based on the HTTP protocol to ensure the security of data transfer. When configuring HTTPS, you need to provide a certificate for the domain name and deploy it on all ECDN nodes to implement encrypted data transfer across the network.

> The configured HTTPS domain name should already have been connected to ECDN, and the domain name status should be **activated**.

Adding Configuration

Selecting domain name

1. Log in to the ECDN Console and click **Domain Management** on the left sidebar to enter the management page.
2. In the list, find the domain name to be configured, click **Manage** to enter the details page, and select **Advanced Configuration**.
3. Deploy a domain name certificate before enabling HTTPS. Click **Configure** to enter the domain name certificate management page.



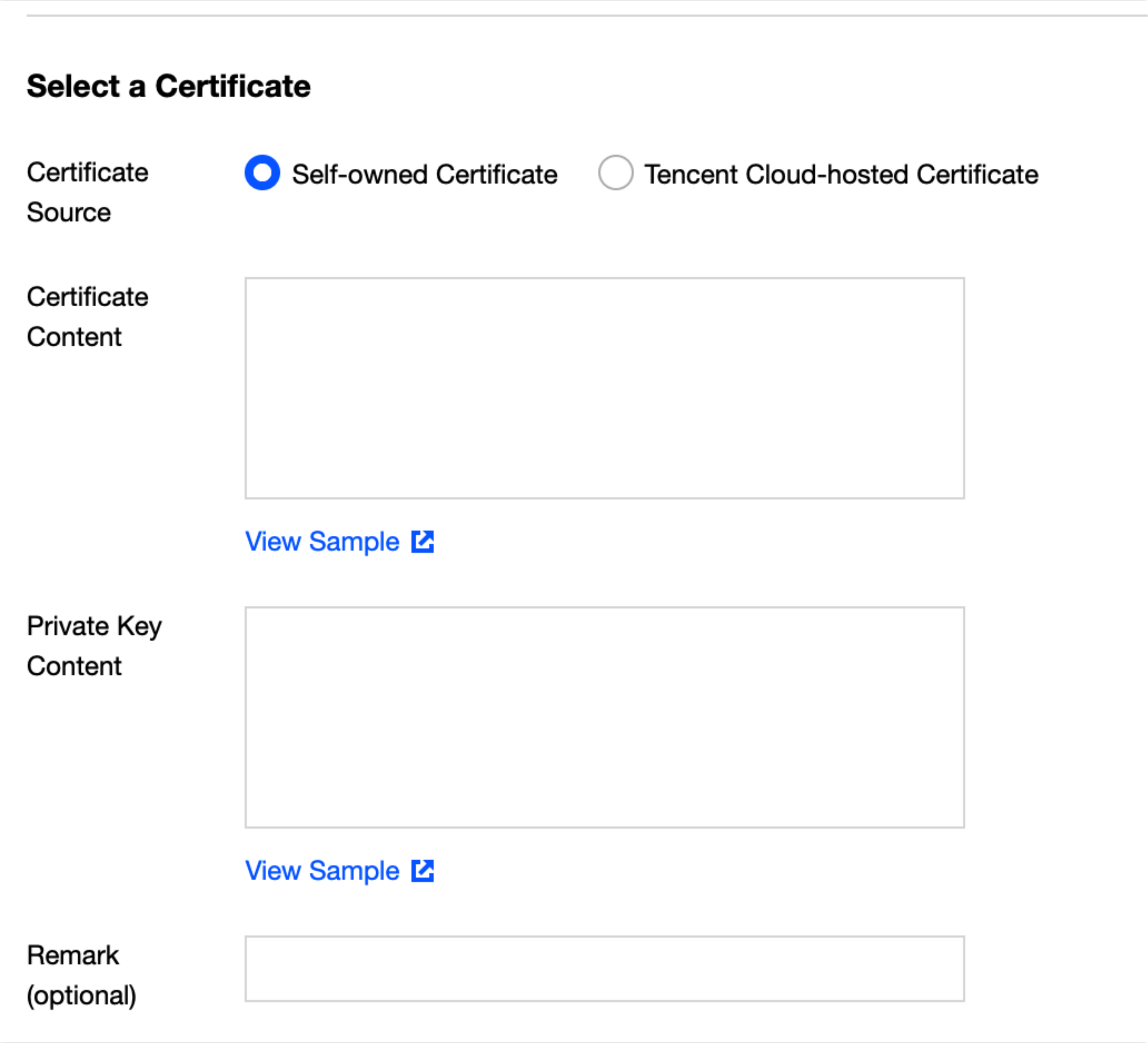
HTTPS Configuration

HTTPS provides identity verification for network server, in order to protect the privacy and integrity of data exchange.How to set HTTPS?

You have not set HTTPS

Configuring certificate

On the certificate configuration page, you can configure private certificates or Tencent Cloud-hosted certificates for the domain name. For detailed directions, please see Certificate Management.



Select a Certificate

Certificate Source ● Self-owned Certificate ○ Tencent Cloud-hosted Certificate

Certificate Content

View Sample

Private Key Content

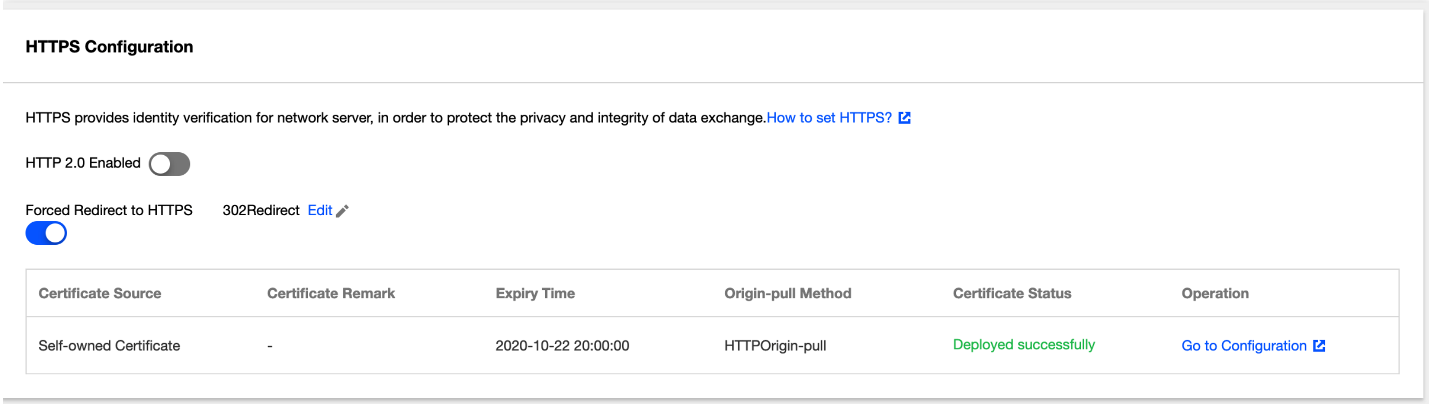
View Sample

Remark (optional)

Modifying Configuration

- **Enable HTTP2.0**
  If a domain names has been configured with a certificate, you can enable HTTP2.0 on the advanced configuration page.

- **Enable forced HTTPS redirection**
  If a domain names has been configured with a certificate, you can enable forced HTTPS redirection. Then, all HTTP requests will be forcibly redirected to HTTPS.
  After enabling forced HTTPS redirection, you can specify whether to use the 301 or 302 status code for redirection, and 302 is used by default.
- **Modify the certificate**
  If a domain name has been configured with a certificate, you can click **Configure** to enter the certificate management page to modify the certificate content.



HTTPS Configuration

HTTPS provides identity verification for network server, in order to protect the privacy and integrity of data exchange.How to set HTTPS?

HTTP 2.0 Enabled ○

Forced Redirect to HTTPS ● 302Redirect Edit

Certificate Source	Certificate Remark	Expiry Time	Origin-pull Method	Certificate Status	Operation
Self-owned Certificate	-	2020-10-22 20:00:00	HTTPOrigin-pull	Deployed successfully	Go to Configuration

Alarm Monitoring Configuration

Last updated : 2020-08-27 11:26:02

Description of Connecting ECDN to Cloud Monitor

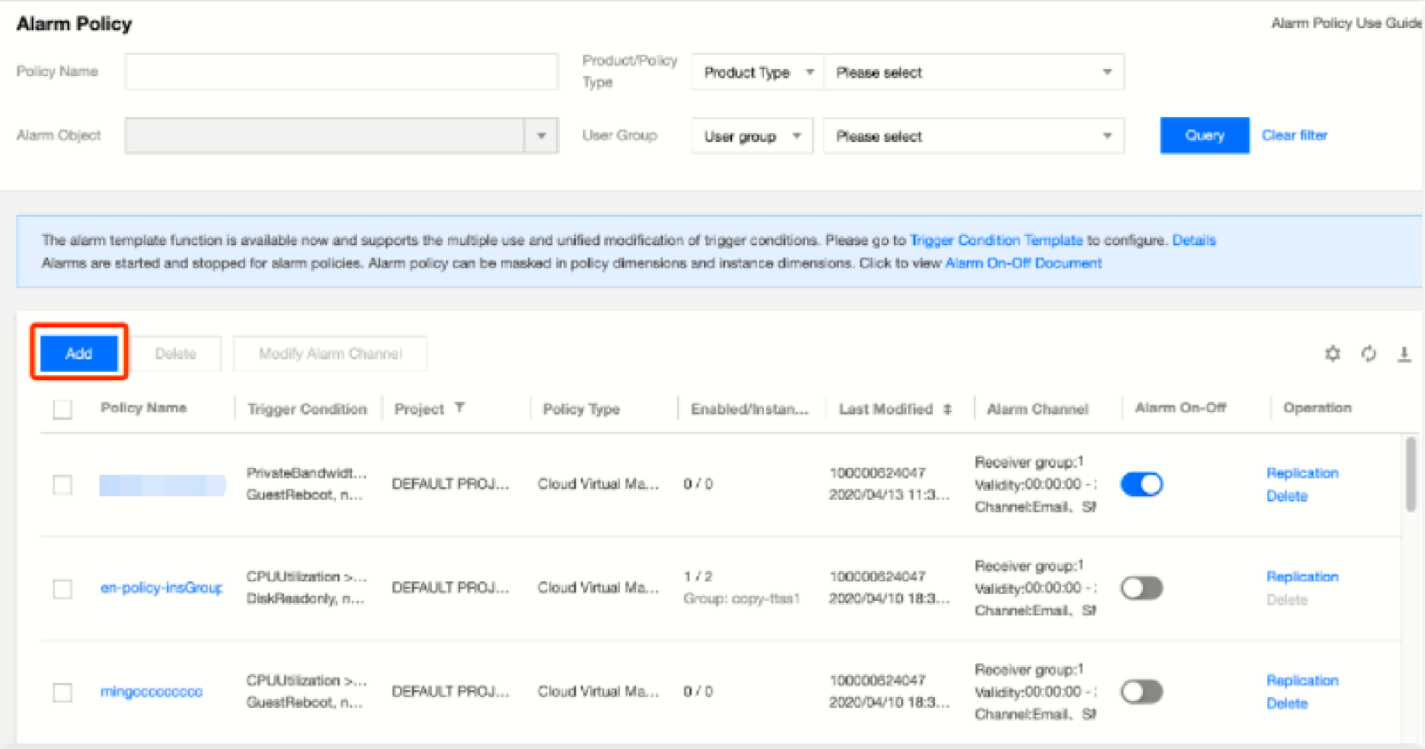
ECDN has been connected to Tencent Cloud Monitor. The following alarming metrics are supported in the current version:

Category	Metric	1-Minute Alarming Granularity Supported	5-Minute Alarming Granularity Supported
Access traffic metrics	Total number of requests	Yes	Yes
	Access bandwidth	Yes	Yes
	Access traffic (upstream)	Yes	Yes
	Access traffic (downstream)	Yes	Yes
Origin-pull traffic metrics	Total number of origin-pulls	Yes	Yes
	Number of failed origin-pull	Yes	Yes
	Origin-pull failure rate	Yes	Yes
	Origin-pull bandwidth	Yes	Yes
Access performance metrics	Average response time	Yes	Yes
Status code metrics	Number of 200, 206, 2XX, etc. status code occurrences and their ratio	Yes	Yes
	Number of 302, 304, 3XX, etc. status code occurrences and their ratio	Yes	Yes
	Number of 401, 403, 404, 416, 4XX, etc. status code occurrences and their ratio	Yes	Yes
	Number of 500, 502, 5XX, etc. status code occurrences and their ratio	Yes	Yes

- You can activate and use Cloud Monitor free of charge.
- The system sends alarm messages through email, WeChat, and callback APIs free of charge, and you can enjoy a free tier of SMS alarm messages every month.
- If the monthly free tier of SMS alarm messages is exceeded, you need to purchase a higher tier for receiving more alarm messages through SMS.
- Alarm data is collected and reported in real time and may have certain deviation, as the data is delayed for about 5 minutes.
- Alarm data monitoring can be used only to assist in operation and cannot be used as the basis for billing or SLA.

Monitoring Configuration Entry

Log in to the Cloud Monitor Console and click **Alarm Policy** on the left sidebar to enter the management page.



Alarm Policy

Policy Name:

Product/Policy Type: Product Type | Please select

Alarm Object:

User Group: User group | Please select

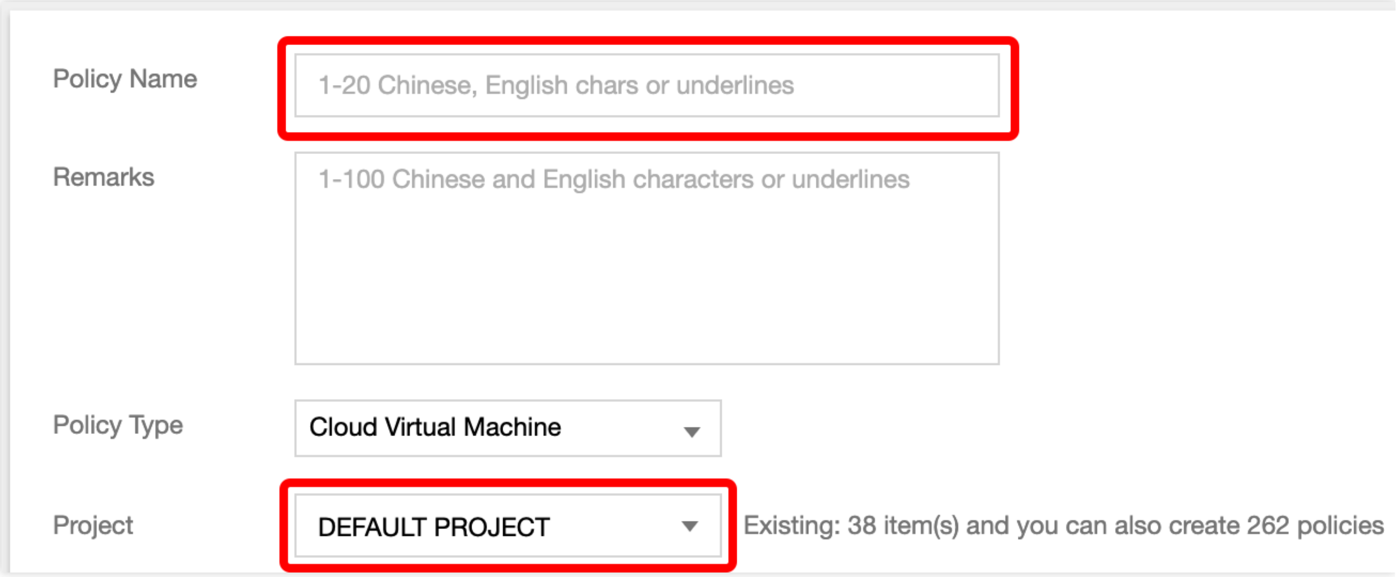
The alarm template function is available now and supports the multiple use and unified modification of trigger conditions. Please go to Trigger Condition Template to configure. Details
Alarms are started and stopped for alarm policies. Alarm policy can be masked in policy dimensions and instance dimensions. Click to view Alarm On-Off Document

□	Policy Name	Trigger Condition	Project	Policy Type	Enabled/Instan...	Last Modified	Alarm Channel	Alarm On-Off	Operation
□	[redacted]	PrivateBandwidt... GuestReboot, n...	DEFAULT PROJ...	Cloud Virtual Ma...	0 / 0	100000624047 2020/04/13 11:3...	Receiver group:1 Validity:00:00:00 - : Channel:Email, SI	●	Replication Delete
□	en-policy-insGroup	CPUUtilization >... DiskReadonly, n...	DEFAULT PROJ...	Cloud Virtual Ma...	1 / 2 Group: copy-ttss1	100000624047 2020/04/10 18:3...	Receiver group:1 Validity:00:00:00 - : Channel:Email, SI	○	Replication Delete
□	mingoccccccco	CPUUtilization >... GuestReboot, n...	DEFAULT PROJ...	Cloud Virtual Ma...	0 / 0	100000624047 2020/04/10 18:3...	Receiver group:1 Validity:00:00:00 - : Channel:Email, SI	○	Replication Delete

Adding Alarm

The steps for adding an alarm policy are as follows:

1. Enter the policy name and remarks and select the ECDN alarm policy type.



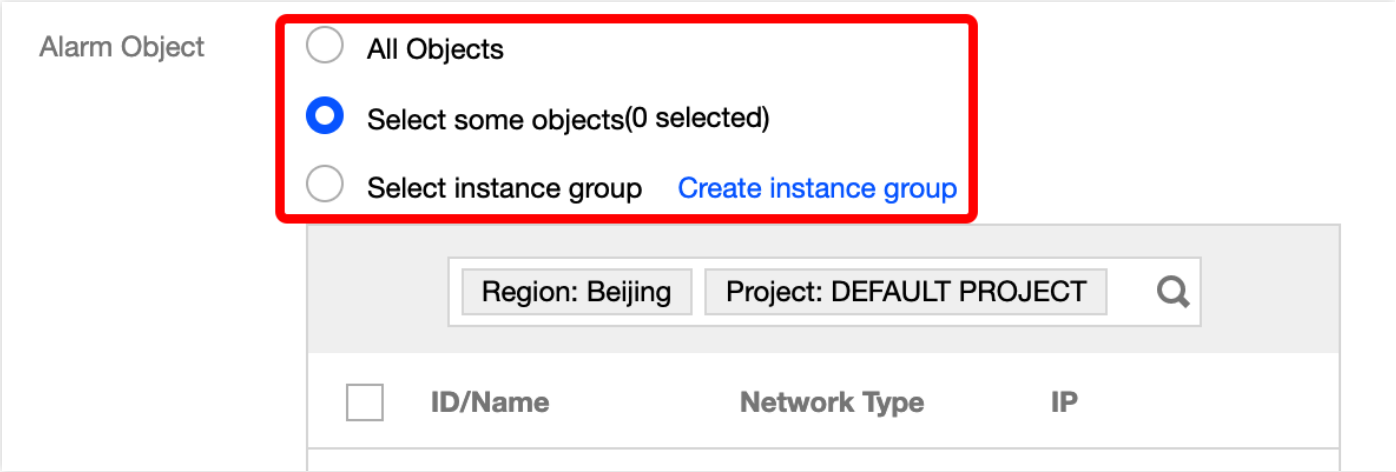
Policy Name: 1-20 Chinese, English chars or underlines

Remarks: 1-100 Chinese and English characters or underlines

Policy Type: Cloud Virtual Machine

Project: DEFAULT PROJECT Existing: 38 item(s) and you can also create 262 policies

2. Select the alarm object.



Alarm Object

○ All Objects

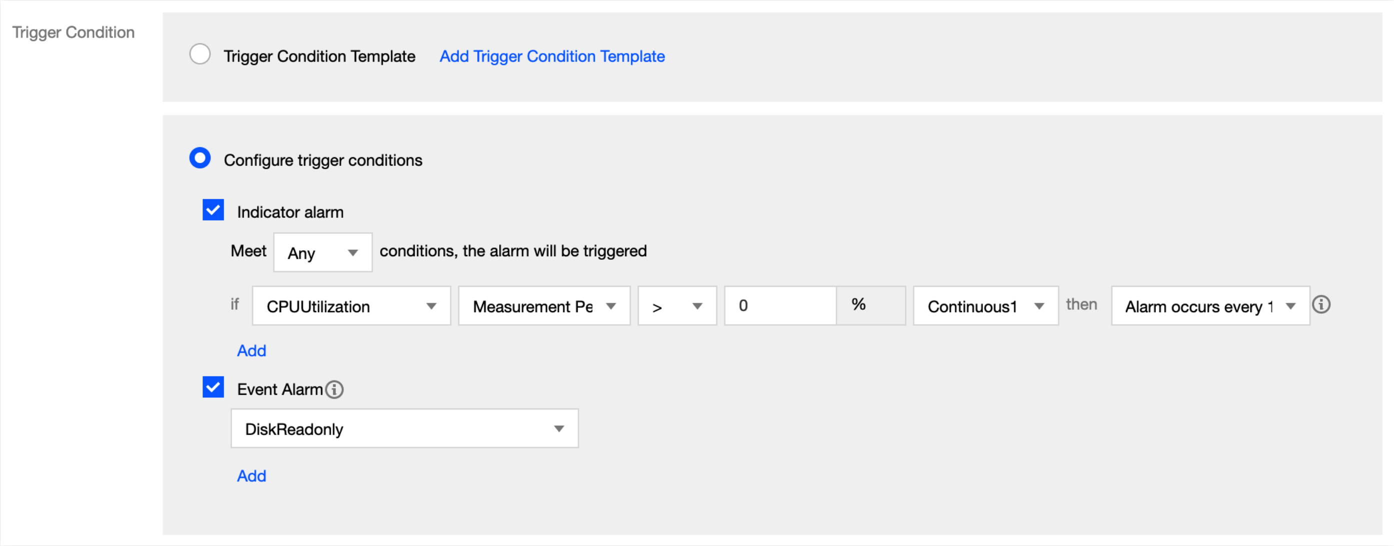
● Select some objects(0 selected)

○ Select instance group Create instance group

Region: Beijing Project: DEFAULT PROJECT

□	ID/Name	Network Type	IP

3. Set the alarm trigger condition. Multiple conditions can be set at a time.



Trigger Condition

○ Trigger Condition Template Add Trigger Condition Template

● Configure trigger conditions

☑ Indicator alarm

Meet Any conditions, the alarm will be triggered

if CPUUtilization | Measurement Pe | > | 0 | % | Continuous1 | then | Alarm occurs every 1

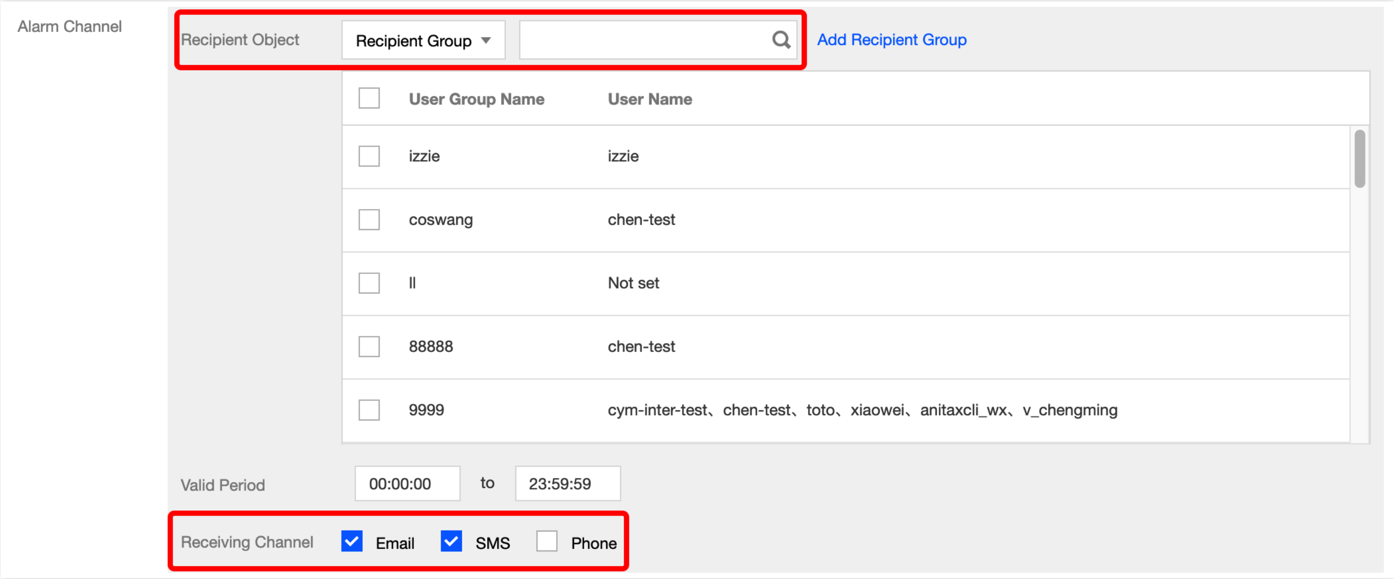
Add

☑ Event Alarm

DiskReadonly

Add

4. Set the alarm recipient, alarm time period, and alarm method.



Alarm Channel

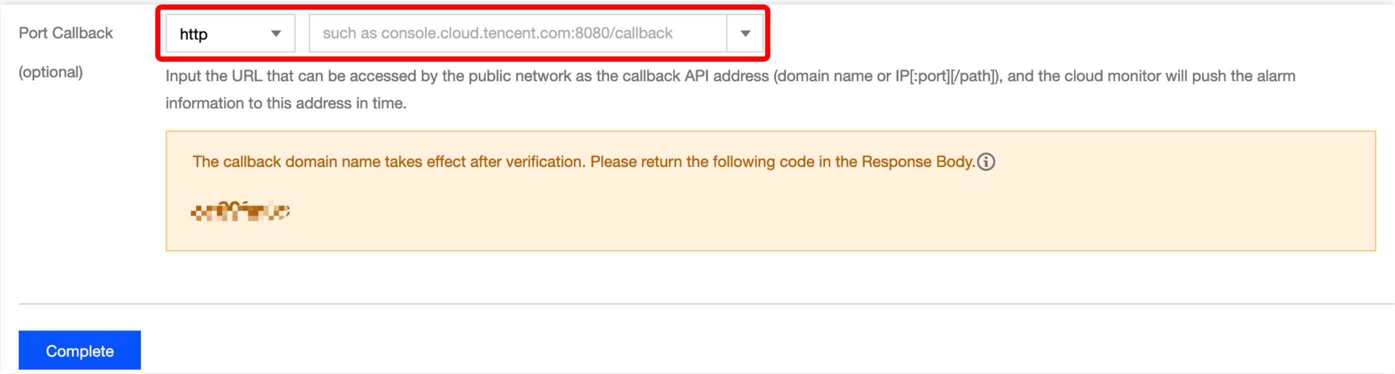
Recipient Object: Recipient Group Add Recipient Group

□	User Group Name	User Name
□	izzie	izzie
□	coswang	chen-test
□	ll	Not set
□	88888	chen-test
□	9999	cym-inter-test、chen-test、toto、xiaowei、anitaxcli_wx、v_chengming

Valid Period 00:00:00 to 23:59:59

Receiving Channel ☑ Email ☑ SMS □ Phone

5. Set the alarm callback API.



Port Callback (optional)

http ▾ | such as console.cloud.tencent.com:8080/callback ▾

Input the URL that can be accessed by the public network as the callback API address (domain name or IP[:port][/path]), and the cloud monitor will push the alarm information to this address in time.

The callback domain name takes effect after verification. Please return the following code in the Response Body. ⓘ

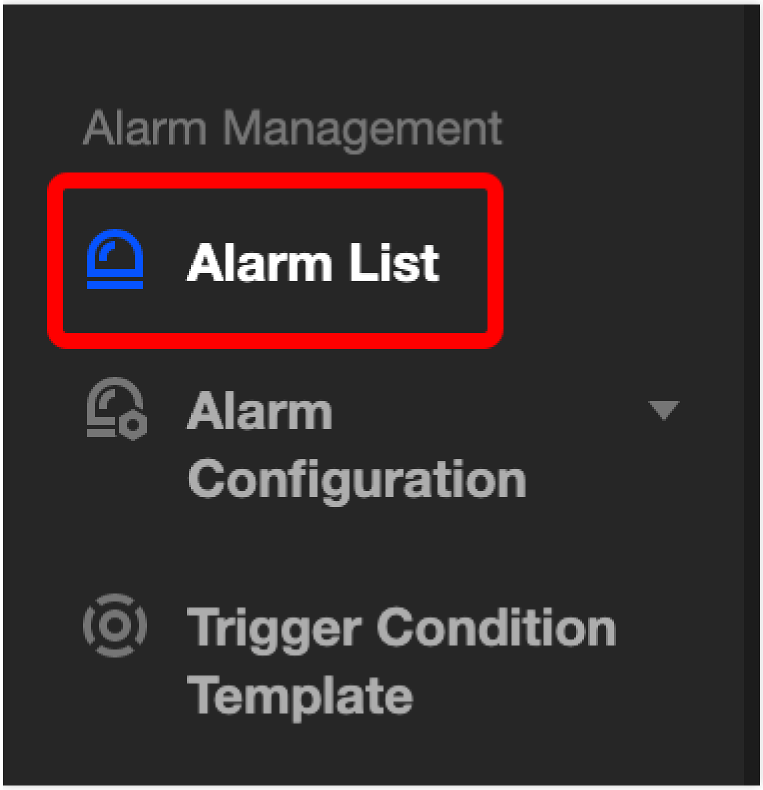
[redacted]

Complete

6. Click **Complete** to submit the settings.

Viewing Alarm

On the historical alarm page in Cloud Monitor, you can view the list of alarm details.



Other Alarm Policies

For more information on how to configure alarm policies, please see Creating Alarm Policies.