

Tencent Cloud EdgeOne

Site and Billing Management

Product Documentation



Copyright Notice

©2013–2025 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



All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. 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

Site and Billing Management

Billing Management

- Usage Cap Policy

- Billing Usage

- Tag-based Cost Allocation

- Change Plan

- Plan Destruction Guide

Site Management

- Quickly Importing and Exporting Site Configuration

General Policy

- Custom Response Page

- IP Groups

- Content Identifier

Site and Billing Management

Billing Management

Usage Cap Policy

Last updated: 2025-07-28 14:25:31

Feature Overview

Once you've exhausted the [Plan Fees](#) and the [Extra Package Description \(Prepaid\)](#), you'll transition to EdgeOne's [Fees for Out-of-plan Resource Usage \(Pay-as-You-Go\)](#). If you're concerned about potentially high costs due to abnormal traffic in your operations, a usage cap policy can be implemented to control the traffic and requests for your service.

EdgeOne periodically calculates business traffic, bandwidth and request numbers. You can independently configure the thresholds for business traffic, bandwidth and request numbers. When the usage consumption generated within the statistical period reaches the alarm threshold you configured, EdgeOne will push a notification to inform you and immediately disable EdgeOne secure acceleration services to avoid incurring more abnormal charges.

Note:

1. The usage cap configuration takes effect with some delay (approximately 10 minutes), and during this period, the incurred consumption will be billed normally.
2. Usage cap policies are calculated based on the subdomain dimension. When the effective scope is set to a site or all subdomains, it means that all subdomains under the site share a single usage cap policy.
3. When both traffic, bandwidth and request policies exist for the same domain, triggering the threshold for either one will result in the deactivation of the domain's service.
4. Currently, only L7 (application layer) traffic, L7 (application layer) bandwidth and HTTP/HTTPS request configuration support usage capping policies. The data comes from the real-time monitoring data of Data Analysis – Metric Analysis, rather than the billing usage data.

Directions

1. Log in to the [Tencent Cloud EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** to be configured under **Website Security Acceleration**.
2. On the site details page, click on **Usage Policy > Usage Capping Policy**. This will take you to the Usage Cap Policy page. Click on **Add capping policy**.

- After the statistical period generates consumption exceeding the set threshold, the service will be disabled. You can adjust the upper threshold first, **domain management page** re-enable the domain
- There is a certain delay (about 10 minutes) for the usage cap configuration to take effect. During this period, the generated consumption will be billed normally.
- The capping strategy is calculated based on the subdomain dimension. When site or all subdomains are selected to take effect, it means that all subdomains under the site share a single capping strategy.
- When traffic strategy and request count strategy for the same domain exist at the same time, the domain service will be disabled as long as one of them reaches the threshold.

Add capping policy								
Enter acceleration domain/policy ID								
Policy ID	Effective range	Statistical period	Policy type	Capping threshold	Action	Custom threshold	Status	Operation
	Subdomain of the current site	5 minutes	L7 traffic	50 GB	Stop service	10%	Enabled	Edit Disable Delete
	zts.hughdszhou.club	5 minutes	L7 traffic	50 GB	Stop service	10%	Enabled	Edit Disable Delete
Total items: 2					10 / page 1 / 1 page			

3. In the **Add capping policy** window, configure the cap policy based on your actual requirements.

Add capping policy

Effective range

Subdomain

Please select

Simultaneously apply to subdomains you selected, sharing a common usage capping policy.

Statistical period

☒ 5 minutes
 ☐ hour
 ☐ day

Accumulation of usage is conducted within the time granularity of the statistical period.

Capping configuration

HTTP/HTTPS request count

—

300

+

10 thousand times

Exceeding the threshold

☒ Disable service

Domains exceeding the threshold will have their service disabled and need to be re-enabled in the domain list.

Custom threshold

—

10

+

%


When the request usage/usage threshold reaches the configured alarm threshold (10% - 90%), an alarm message will be sent.

Save

Cancel

Configuration Item	Description
Scope of Effectiveness	Choose the scope of effectiveness for the cap policy: <ul style="list-style-type: none"> • Site: All subdomains under the site share a single cap policy. • Subdomain: All selected subdomains share a single cap policy.

Statistics Period	<p>Choose the data statistics period for the cap policy, and periodically compare the statistical data with the capping threshold:</p> <ul style="list-style-type: none">• 5 minutes: Statistics for usage generated within 5 minutes.• Hour: Statistics for usage generated within 1 hour.• Day: Statistics for usage generated within 24 hours. <div><p>Note:</p><ul style="list-style-type: none">• When the statistics period is set to "5 minutes", it will calculate usage for each complete 5-minute interval. For example, if you configure and save an L7 traffic capping policy at 15:26:00 on October 25, 2023, the first 5-minute interval will calculate L7 traffic from 15:25:00 to 15:29:59, and the second 5-minute interval will calculate L7 traffic from 15:30:00 to 15:34:59, and so on.• When the statistics period is set to "1 hour", it will calculate usage for each complete 1-hour interval. For example, if you configure and save an L7 traffic capping policy at 15:26:00 on October 25, 2023, the first 1-hour interval will calculate L7 traffic from 15:00:00 to 15:59:59, and the second 1-hour interval will calculate L7 traffic from 16:00:00 to 16:59:59, and so on.• When the statistics period is set to "day", it will calculate usage for each complete 24-hour interval. For example, if you configure and save an L7 traffic capping policy at 15:26:00 on October 25, 2023, the first day interval will calculate L7 traffic from 00:00:00 to 23:59:59 on October 25.• When usage exceeds the set threshold during the statistics period, the service will be disabled. It is recommended to adjust the cap threshold first, then go to the domain management page to re-enable the domain name. Otherwise, the next scan will disable the service again because the usage has exceeded the current cap threshold setting.</div>
Cap Configuration	<p>Choose the policy type for cap configuration. When both the traffic, bandwidth and request policy for the same domain exist simultaneously, triggering the threshold for either will disable the domain service:</p> <ul style="list-style-type: none">• L7 Traffic: represents setting the highest cap threshold for L7 traffic, with the option to choose units in MB, GB, TB.• HTTP/HTTPS Request Number: represents setting the highest cap threshold for HTTP/HTTPS request numbers, with the option to choose

	<p>units in ten thousand times, million times, and hundred million times.</p> <ul style="list-style-type: none">• L7 Bandwidth: represents setting the highest cap threshold for L7 bandwidth, with the option to choose units in Mbps, Gbps, and Tbps.
Exceeding Threshold	Service Deactivation: indicates that when the cap threshold is triggered, service will be deactivated for all subdomains within the effective scope.
Alarm Threshold	<p>When the usage/usage threshold within the statistical period reaches the configured alarm threshold (10% – 90%), an alarm message will be issued.</p> <div><p> Note:</p><p>If the alarm threshold is already enabled: due to a scanning granularity of 5 minutes, if there is a significant increase in usage within a short period and the value is large, it is possible that the previous scan has not triggered the percentage alarm threshold, and the next scan directly reaches the access threshold. In this scenario, both percentage and access threshold alarm notification messages will be sent.</p></div>

4. After completing the capping policy configuration, click **Save** to deploy the capping policy configuration.

Billing Usage

Last updated: 2024-08-14 15:06:35

Overview

The Billing Usage page of EdgeOne provides usage data for billing items, allowing you to estimate fees based on this data before actual billing. After billing, you can view the bill details in the [Tencent Cloud Billing Center console](#). You can also view more detailed usage reports on this page and filter by resource tag, billing region, package, site, domain, and L4 proxy instance. This document explains the relationship between the component name fields in the Tencent Cloud Billing Center's detailed bill and the metric names on the EdgeOne Billing Usage page.

Note

1. The data displayed on the Billing Usage page may differ from that on other pages (Traffic Analysis, Service Overview, and Site Overview). If you are concerned with fees-related issues, it is recommended to refer to the Billing Usage page. The relationships among the various data provided by EdgeOne are as follows:

Tencent Cloud billing usage data = Data displayed on the Billing Usage page ≈ Data displayed on the Traffic Analysis, Service Overview, and Site Overview Pages > Data calculated using raw logs.

The explanation for the differences between billing usage data and the data in logs can be found in [Why are the traffic data in the console and the traffic data derived from logs inconsistent?](#)
2. Due to latency and algorithm impacts, the data on this page may have some latency and generally stabilizes after 2 hours.

Relationship Between Metrics on the Billing Usage Page and Billing Items

For Personal/Basic/Standard Edition Users

Component Name Field in Tencent Cloud Billing Center Detailed Bill	Metric Name Displayed on EdgeOne Billing Usage Page	Billing Standard
SCDN – Traffic – Hourly Settlement	Corresponds to the total usage generated by the following services: <ul style="list-style-type: none">● Content acceleration traffic: L7 (application layer) traffic generated by all domains when Smart Acceleration is not enabled; only downstream traffic is counted;	L7 (application layer) traffic price

	<ul style="list-style-type: none"> ● Smart acceleration traffic: L7 (application layer) traffic generated by all domains when Smart Acceleration is enabled; both upstream and downstream traffic is counted. 	
HTTP/HTTPS Security Requests – Hourly Settlement	<ul style="list-style-type: none"> ● HTTP/HTTPS Requests: Application layer requests generated by all domains, regardless of protocol or whether they are static or dynamic requests. 	HTTP/HTTPS request price
Value-Added Service Usage Unit – Hourly Settlement	<p>Corresponds to the total value-added service usage units generated by the following value-added services:</p> <ul style="list-style-type: none"> ● Smart Acceleration Requests: HTTP/HTTPS requests generated by domains with Smart Acceleration enabled; ● QUIC Requests: Requests using the QUIC protocol generated by domains with HTTP/3 (QUIC) enabled; ● Bot Requests: HTTP/HTTPS requests generated by domains with Bot management enabled; 	VAU Fee (Pay-as-You-Go)

For Enterprise Edition Users

Component Name Field in Tencent Cloud Billing Center Detailed Bill	Metric Name Displayed on EdgeOne Billing Usage Page	Billing Standard
L7 content acceleration – Traffic	<ul style="list-style-type: none"> ● Content acceleration traffic: L7 (application layer) traffic generated by all domains when Smart Acceleration is not enabled; only downstream traffic is counted. 	L7 (application layer) traffic price
L7 smart acceleration – Traffic	<ul style="list-style-type: none"> ● Smart acceleration traffic: L7 (application layer) traffic generated by all domains when Smart Acceleration is 	L7 (application layer) traffic price

	enabled; both upstream and downstream traffic is counted.	
L4 acceleration – Traffic	<ul style="list-style-type: none"> ● L4 acceleration traffic: The sum of L4 (transport layer) upstream and downstream traffic generated by all L4 proxy instances. 	L4 (transfer layer TCP/UDP application) traffic price
Exclusive DDoS Protection – Traffic	<ul style="list-style-type: none"> ● Exclusive protection traffic: Business traffic generated by domains/L4 proxy instances with Exclusive DDoS Protection enabled. 	Exclusive DDoS protection traffic fee
Chinese Mainland Network Optimization – Traffic	<ul style="list-style-type: none"> ● Cross-MLC-border acceleration traffic: Business traffic generated by sites/L4 proxy instances with the Cross-MLC-border Acceleration feature enabled. 	Cross-MLC-border acceleration traffic fee (pay-as-you-go)
HTTP/HTTPS Security Requests – Monthly Settlement	<ul style="list-style-type: none"> ● HTTP/HTTPS Requests: Application layer requests generated by all domains, regardless of protocol or whether they are static or dynamic requests. 	HTTP/HTTPS request price
Value-Added Service Usage Unit – Monthly Settlement	<p>Corresponds to the total value-added service usage units generated by the following value-added services:</p> <ul style="list-style-type: none"> ● Smart Acceleration Requests: HTTP/HTTPS requests generated by domains with Smart Acceleration enabled; ● QUIC Requests: Requests using the QUIC protocol generated by domains with HTTP/3 (QUIC) enabled; ● Bot Requests: HTTP/HTTPS requests generated by domains with Bot management enabled; 	VAU Fee (Pay-as-You-Go)
Exclusive DDoS Protection – Elastic Protection Bandwidth Package	<ul style="list-style-type: none"> ● Elastic DDoS Protection Bandwidth: The part of attack bandwidth exceeding the guaranteed protection bandwidth generated by exclusive DDoS protection instances within Chinese mainland. 	Elastic Protection Bandwidth Fees

Supported Filter Criteria

- Selecting the time period for data queries is supported. You can query data from February 9, 2022 onwards on this page, with a maximum single filter duration of 31 days.
- Filtering based on the following criteria is supported, with an "and" relationship between multiple conditions:
 - **Billing region:** Filter by the billing region of the traffic, which is the region where the EdgeOne node serving user clients is located. For details, see [Mapping Relationship Between Billing Regions and Countries](#).
 - **Site tag:** Filter by the resource tag key-value pairs bound to the site.
 - **EdgeOne billing package:** Filter by all sites included in the package.
 - **Site:** Filter by specified site, including sites deleted within the last 3 months.
 - **Acceleration domain:** Filter by specified acceleration domain, and cannot simultaneously add L4 proxy instance filter criterion.
 - **L4 proxy instance:** Filter by L4 proxy instance, and cannot simultaneously add acceleration domain filter criterion.

Example: Querying Billing Usage for Sites Bound with Specified Tags

Sample Scenario

Tencent Cloud [Tag](#) feature provides a flexible resource management method. By tagging cloud resources, users can more easily organize, search, and manage their resources on Tencent Cloud. If a company has deployed multiple projects on Tencent Cloud, to improve the efficiency and accuracy of resource management, the company classifies existing cloud resources. Based on dimensions such as projects, environments (such as development, testing, and production), and cost centers, the company plans a tag system. For example, for the project dimension, the company can set the tag key as `Project` and the tag value as the specific project name; for the environment dimension, set the tag key as `Environment` and the tag value as `Dev`, `Test`, `Prod`, or other values. According to the planned tag system, the company tags the existing resources using the [EdgeOne console](#) or APIs. For example, a site belonging to project A and in the development environment would be tagged with `Project: Project A` and `Environment: Dev`. After the current billing cycle ends and the bill is issued, the company wants to review the billing usage by tag for the previous billing cycle.

Directions

1. Log in to the [EdgeOne console](#), and click **Billing Management > Billing Usage** in the left sidebar.
2. On the Billing Usage page, click **Last month** to quickly filter data from 00:00 on the 1st day of last month to 23:59 on the last day.

Last 6 hours

Today

Yesterday

Last 7 days

Current month

Last month

2024-07-16 00:00 ~ 2024-07-16 11:33



3. Click **Select site tags**, choose the **Tag Key** and **Tag Value** you want to view, such as

Project: Project A and Environment: Dev , and click **OK**.

The screenshot shows the Tencent Cloud EdgeOne Billing Usage page. At the top, there are tabs for time periods: Last 6 hours, Today, Yesterday, Last 7 days, Current month, and Last month. A date range selector shows 2024-07-16 00:00 to 2024-07-16 11:33. Below these are filters for 'All billing areas' and 'All sites'. A 'Select site tags' dialog box is open, showing a 'Tag Key' dropdown and a 'Tag Value' dropdown. The dialog has an 'Add' button and 'OK'/'Cancel' buttons. The main content area displays five traffic metrics: Content acceleration traffic, Smart acceleration traffic, L4 acceleration traffic, Exclusive protection traffic (/secure acceleration traffic), and Cross-MLC-border acceleration traffic. Each metric shows a value of 0 B. A 'Compare data' link is visible at the bottom left.

4. The page will automatically display all sites bound with the selected tag key–value pairs. You can view or download the billing usage of these sites.

The screenshot shows the same Tencent Cloud EdgeOne Billing Usage page, but now the 'Select site tags' dialog box is closed. The 'All billing areas' dropdown is set to 'All billing areas'. The '1 tags selected.' and '1 sites selected.' dropdowns are visible. The main content area displays the same five traffic metrics: Content acceleration traffic, Smart acceleration traffic, L4 acceleration traffic, Exclusive protection traffic (/secure acceleration traffic), and Cross-MLC-border acceleration traffic. Each metric shows a value of 0 B. A 'Compare data' link is visible at the bottom left.

APIs

[DescribeBillingData](#)

Tag-based Cost Allocation

Last updated: 2025-10-28 16:03:30

Tag-based cost allocation is a feature that enables custom management of users' cloud resource bills from the perspective of statistical analysis by leveraging the tag tool and cost allocation capabilities. Users can use tags to reallocate and analyze the costs or expenses of cloud resources in the bill according to their management or analysis needs by cost allocation dimensions such as the department using the resource or the application project for the resource.

Note:

- EdgeOne tag-based cost allocation is an allowlist feature. You need to [contact us](#) for allowlist configuration before you can implement tag-based cost allocation.
- The EdgeOne tag-based cost allocation feature is only available to Enterprise edition users. Once activated, it will take effect from the 1st of the following month and cannot be applied to historical bills.

Creating Tags

1. Log in to the [Tencent Cloud tag console](#).
2. Click **Tag List** in the left sidebar to go to the tag list page and select **Custom Tag**.
3. Click **Create Tag**. In the Create Tag dialog box, create a tag, or select an existing tag key and add a tag value to it. Click **Add Tag Key** to create multiple tags at a time.
 - Tag key (required): Enter a new tag key to create a tag, or select an existing tag key and add a tag value to it.
 - Tag value (required): Enter a new tag value.

Create Tag

- Enter a new tag key and value, or select a tag key and add a new value to it.
- Each tag key can have a maximum of 1,000 values. You can add 10 values at a time.

Tag Key

:

Tag Value

Enter a tag value

Delete

Add Tag Key

OK

Cancel

4. Click **OK** to start creation. All successfully added tags will be displayed.

Create Tag				Delete
<input type="checkbox"/> Tag Key	Tag Value	Resource Count	Operation	
<input type="checkbox"/> 云资源	云资源	0	Bind Resources	Delete
<input type="checkbox"/> 云资源	云资源	0	Bind Resources	Delete
<input type="checkbox"/> 云资源	云资源	2	Bind Resources	Delete
<input type="checkbox"/> 云资源	云资源	2	Bind Resources	Delete
<input type="checkbox"/> 云资源	云资源	0	Bind Resources	Delete
<input type="checkbox"/> 云资源	云资源	5	Bind Resources	Delete
<input type="checkbox"/> 云资源	云资源	0	Bind Resources	Delete
<input type="checkbox"/> 云资源	云资源	2	Bind Resources	Delete
<input type="checkbox"/> 云资源	云资源	3	Bind Resources	Delete
<input type="checkbox"/> 云资源	云资源	2	Bind Resources	Delete
Total Items: 357				10 / page 1 / 36 pages

Setting Cost Allocation Tags

1. Go to [Billing Center > Cost Allocation Management > Cost Allocation Tags](#).
2. On the Cost Allocation Tags page, select the tag key to be operated and click **Set as Cost Allocation Tag**.

Cost Allocation Tags

Cost Allocation Tags

Tags are the labels you assign to Tencent Cloud resources. You can use tags to organize your resources and to group your costs in a detailed way on a bill. The bills will show columns for each tag set as a cost allocation tag. Each column shows one tag key and the related key values. Tags that are not set as cost allocation tags will not appear on the bills. You can also use cost allocation tags as filter conditions for different views of bill summary and breakdown. [User Guide of Cost Allocation Tags](#)

[Set as Cost Allocation Tag](#) [Cancel Cost Allocation Tag](#) [Manage tags](#)

Enter tag key to search

Tag Key	All Tag Keys	Date-time	Operation
<input checked="" type="checkbox"/> Department	-	-	Set as Cost Allocation Tag
<input checked="" type="checkbox"/> Product	-	-	Set as Cost Allocation Tag

Total items: 2

20 / page 1 / 1 page

3. In the pop-up message box, click **OK**. If a message shown below appears in the upper right corner of the console or cost allocation tags are identified in the list, it indicates that the setting is complete.

Cost Allocation Tags

Cost Allocation Tags

Tags are the labels you assign to Tencent Cloud resources. You can use tags to organize your resources and to group your costs in a detailed way on a bill. The bills will show columns for each tag set as a cost allocation tag. Each column shows one tag key and the related key values. Tags that are not set as cost allocation tags will not appear on the bills. You can also use cost allocation tags as filter conditions for different views of bill summary and breakdown. [User Guide of Cost Allocation Tags](#)

[Set as Cost Allocation Tag](#) [Cancel Cost Allocation Tag](#) [Manage tags](#)

Enter tag key to search

Tag Key	All Tag Keys	Date-time	Operation
<input type="checkbox"/> Department	Cost Allocation Tags	2024-12-13 15:43:32	Cancel Settings
<input type="checkbox"/> Product	Cost Allocation Tags	2024-12-13 15:43:32	Cancel Settings

Total items: 2

20 / page 1 / 1 page

Cost allocation tags set successfully

Binding Tags to a Site

The finest resource granularity of EdgeOne is the site, so tags can only be bound to the site. You can bind tags when adding a new site or after the site is added. Below is a brief description:

Binding Tags When Adding a New Site

1. Log in and go to [EdgeOne console > Service Dashboard](#), under the Website security acceleration TAB, click **Add new site**.

EdgeOne

Site List

[+ Add new site](#)

Separate keywords with ";", press Enter to separate filter tags

SiteID	Service area	Access mode	Status	Plan Info	Tag	Operation
--------	--------------	-------------	--------	-----------	-----	-----------

2. On the site addition page, click **Add** under Tag, and select the corresponding tag key and tag value,

such as Operation Product: Tencent Cloud EdgeOne.

1 Specify a site

2 Select a plan

3 Select acceleration area and access mode

Enter your site

No domain access

example.com

example.com is already added by the current account. If you want to add it, specify an alias to distinguish the same sites

Alias AAA

Tag (optional) ⓘ

Operation ProductTencent Cloud EdgeOne✕

+ Add Paste

NextCancel

Help

- How to add a site?
- What is the difference between NS access and CNAME access?
- When do I have to verify my site?

3. Complete the site access according to the site addition steps. If you can query the bound tag information on the site list page, it indicates that the tag binding is successful.

+ Add new site

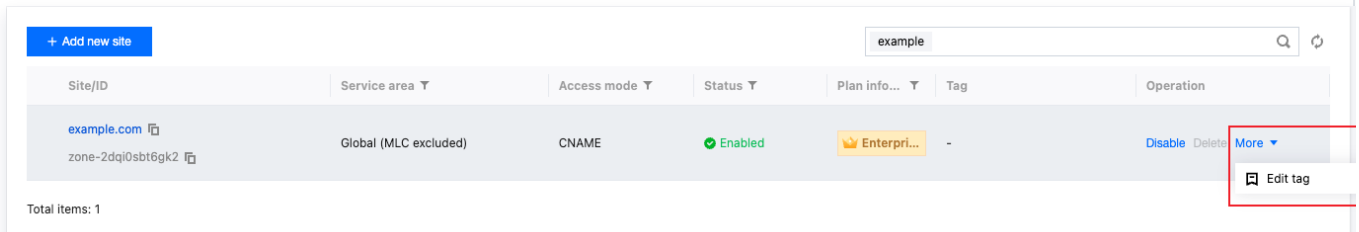
Tag: Operation Prod...

Site/ID	Service area	Access mode	Status	Plan info...	Tag	Operation
example.com zone-2dq10sbt6gk2	Global (MLC excluded)	CNAME	Enabled	Enterpri...	Operation Product: Tencent Cl...	Disable Delete More

Total items: 1

Binding Tags to an Added Site

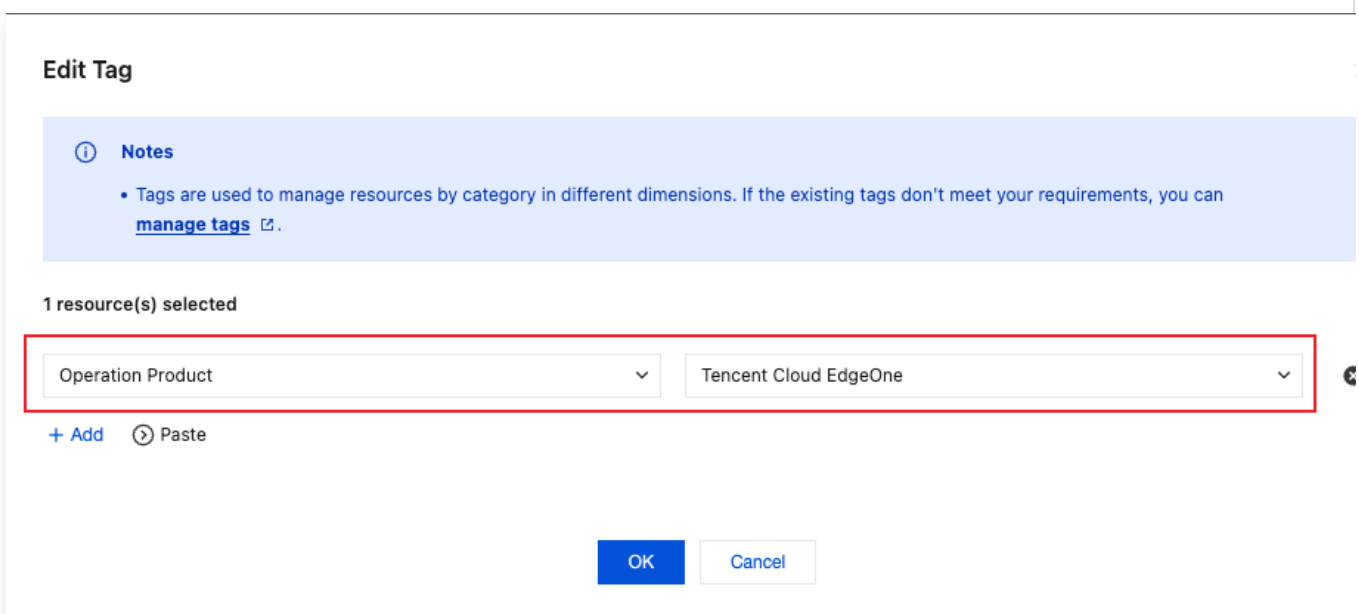
- Log in and go to [EdgeOne console > Service Dashboard](#), under the Website security acceleration TAB, select the site to be bound with tags, and click **More > Edit Tag**.



example						
Site/ID	Service area	Access mode	Status	Plan info...	Tag	Operation
example.com zone-2dqj0sbt6gk2	Global (MLC excluded)	CNAME	Enabled	Enterpri...	-	Disable Delete More

Total items: 1

2. In the pop-up window, add the corresponding tag key and tag value, and click **OK** to complete the tag binding.



Edit Tag

Notes

- Tags are used to manage resources by category in different dimensions. If the existing tags don't meet your requirements, you can [manage tags](#).

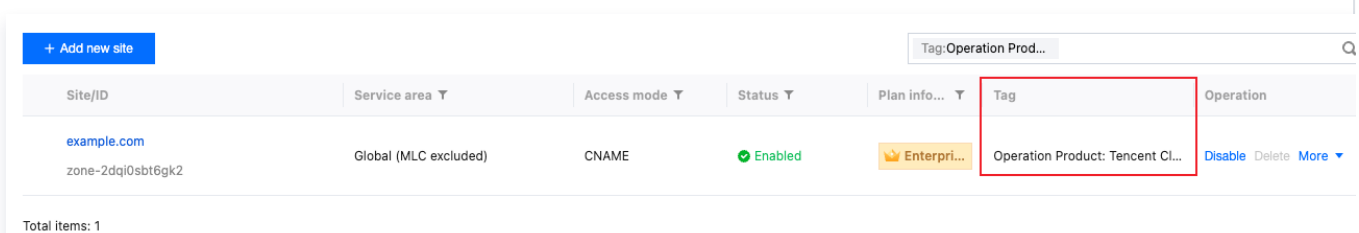
1 resource(s) selected

Operation Product Tencent Cloud EdgeOne

+ Add > Paste

OK Cancel

3. If you can query the bound tag information on the site list page, it indicates that the tag binding is successful.



Tag: Operation Prod...						
Site/ID	Service area	Access mode	Status	Plan info...	Tag	Operation
example.com zone-2dqj0sbt6gk2	Global (MLC excluded)	CNAME	Enabled	Enterpri...	Operation Product: Tencent CL...	Disable Delete More

Total items: 1

Note:

EdgeOne Tag Accounting can only split costs at the site level and summarize expenses by tag. If you need to split settlement for domain names under the same site, for example, the existing `example.com` site, where `1.example.com` and `2.example.com` belong to the acceleration department, and `3.example.com` and `4.example.com` belong to the security group, cost allocation by tag at the domain level is required. Refer to the following solution.

Option 1: Implement by accessing an EdgeOne site with the same name. For example:

1. Create site `example.com`, bind the "Acceleration Department" tag, and add domains `1.example.com` and `2.example.com` under this site. Subsequently, ALL subdomains of the acceleration department will be managed under this site.
2. Create another site `example.com` with the same name, bind the "Security Group" tag, and add domains `3.example.com` and `4.example.com` under this site. Subsequently, ALL subdomains of the security group will be managed under this site.

Achievable to split bills to different operation departments based on tags.

To summarize, if a site has more (N) department tags, it is required to first divide it into N sites during site addition, then bind tags separately, and proceed with subdomain addition.

Option 2: Implement via EdgeOne [content identifier](#) associated with designated domain name method:

View detailed addition instructions for [content identifier](#). Brief explanation here:

1. Create a content identifier to identify domain names responsible for the acceleration department and security group, and associate tags with the content identifier.

Add content identifier					
Separate keywords with " "; press Enter to separate filter tags					
Content Identifier	Description	Number of ref...	Plan	Tag	Open
eocontent-3httqy93mz4i	Acceleration	0	Enterprise / edgeone-3co9hgg4se8g		Delete
eocontent-3gftv5geoyve	Security	0	Enterprise / edgeone-3d8265urfq85		Delete
Total items: 2		10 / page 1 / 1 page			

2. In the rule engine, map and associate the domain names and content identifiers by department. For the association method, please refer to [configure content identifier](#). This method implements cost allocation for content identifiers and domain names simultaneously. Example configuration is shown in the figure below:

IF1 [+ Comment](#)

Matching type ⓘ	Operator	Value
HOST	is in	

[+ And](#) [+ Or](#)

Action	Content Identifier
Set Content Identifier	Acceleration

[+ Action](#)

[+ IF2](#)

Tag Bill Query

After binding the tags to the EdgeOne site and setting them as cost allocation tags, you can view the tag fee summary in the Billing Center in the following ways:

1. On the [Billing Center > Bills > View bills > Bill Overview](#) page, you can view the tag fee summary by cost allocation tags.

By Tag ⓘ [View more](#)

Tag key: Department

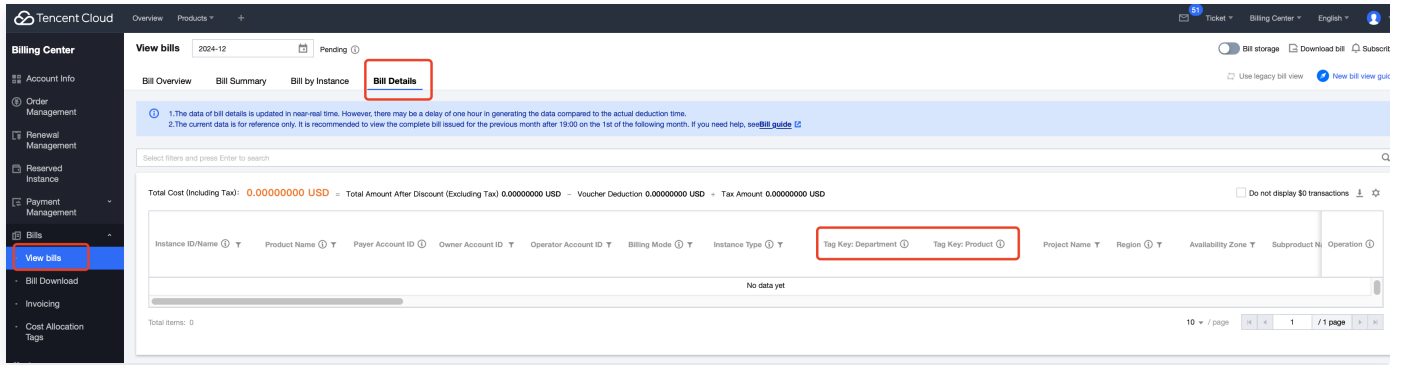
I

Department

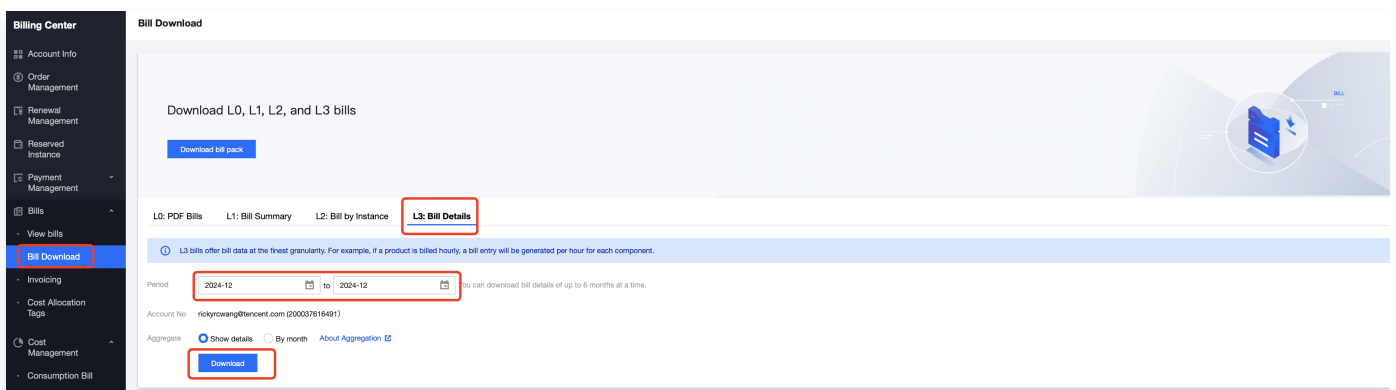
Product

No fees incurred this month

2. If you need to view bill details, go to [Billing Center > Bills > View bills > Bill Details](#). Each fee is marked with the corresponding cost allocation tag in bill details.



3. If you need to download a bill for detailed analysis, go to [Billing Center > Bills > View bills > Bill Download Center](#), and select the billing month to download the bill. Each fee is also marked with the cost allocation tag in the downloaded file.



Change Plan

Last updated: 2025-10-28 16:17:23

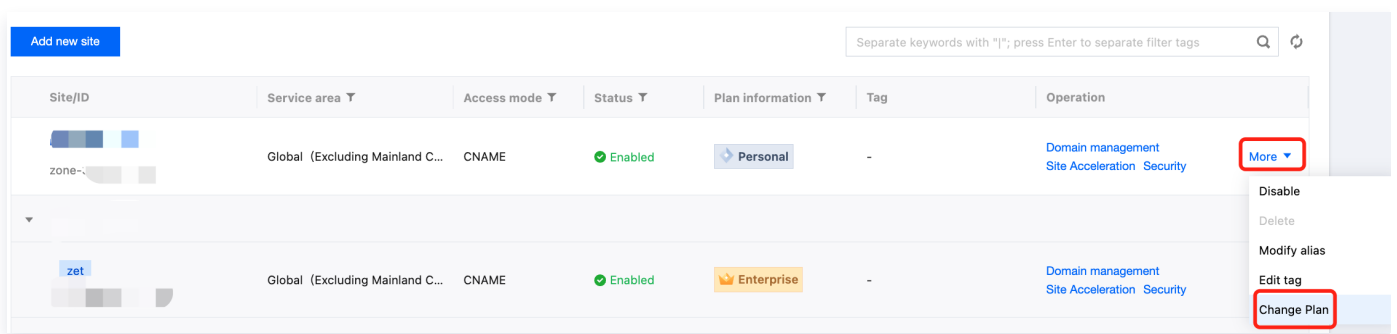
When the package you are using is about to expire and there are other idle packages under your account, you can switch to another package smoothly and losslessly through package rebinding. This document describes the directions for package rebinding.

Note:

- Package rebinding is only supported between packages of the same version or higher. It does not support rebinding a site to a lower version package. The package version sequence is: trial < personal < basic < standard < enterprise.
- Sites on the free plan do not support rebinding and only allow package upgrades.
- Upon success, the site configuration will seamlessly migrate to the new package. The original package will be released as an empty package. If the original package is still valid, you can continue accessing the site.

Operation Steps

1. Go to [EdgeOne console > Service overview](#), select the site for package rebinding, click **More**, and choose **Change Plan**.



2. Enter the package selection page. The page will display ALL available packages for rebinding. Select the package you need and agree to the service agreement.

← Change Plan

• Plan changes are only supported between the same version or higher version plans. Downgrading to a lower version plan is not supported. Plan version hierarchy: Trial < Personal < Basic < Standard < Enterprise.
• After successfully changing the plan, site configurations will be seamlessly migrated to the new plan. The original plan will be released as an empty plan and can still be used if it remains valid.

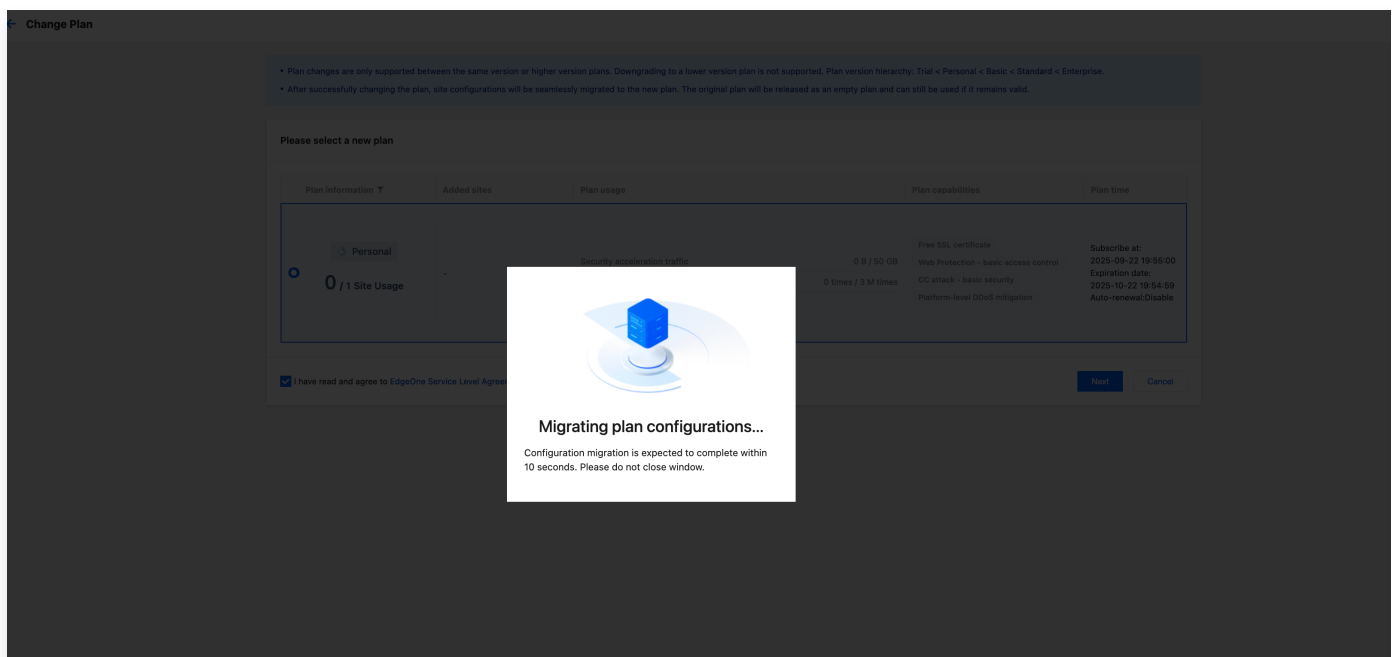
Please select a new plan

Plan information ▾	Added sites	Plan usage	Plan capabilities	Plan time
<p>Personal</p> <p>0 / 1 Site Usage</p>	-	<p>Security acceleration traffic 0 B / 50 GB</p> <p>Security acceleration requests 0 times / 3 M times</p>	<p>Free SSL certificate</p> <p>Web Protection - basic access control</p> <p>CC attack - basic security</p> <p>Platform-level DDoS mitigation</p>	<p>Subscribe at: 2025-09-22 19:55:00</p> <p>Expiration date: 2025-10-22 19:54:59</p> <p>Auto-renewal: Disable</p>

☒ I have read and agree to EdgeOne Service Level Agreement

Next Cancel

3. After confirming that everything is correct, click **Next** to start configuration migration and package rebinding.



4. Upon success, it will return to the package management page. At this point, it indicates that the

package rebinding is successful.

Purchase planRedeem planAuto-renew managementBatch renew

<input type="checkbox"/> Plan information	Added sites	Plan usage(update monthly)	Plan time	Auto-renewal	Operation
<input type="checkbox"/> Personal	No site has been bound, To bind	Security acceleration traffic0 B / 50 GB Security acceleration requests0 times / 3 M times	Subscribe at: 2025-09-22 19:55:00 Expiration date: 2025-10-22 19:54:59 Just 1 days left before expiration. Please renew in time to avoid automatic downgrade to the free plan.	<input type="checkbox"/> 5% off	Renew now Upgrade plan Self-service refund Destroy Plan
<input type="checkbox"/> Personal	rickywong1.site	Security acceleration traffic0 B / 50 GB Security acceleration requests0 times / 3 M times	Subscribe at: 2025-10-21 16:40:00 Expiration date: 2025-11-21 16:39:59	<input checked="" type="checkbox"/>	Renew now Upgrade plan Self-service ref... Destroy Plan

Plan Destruction Guide

Last updated: 2025-08-25 17:41:05

When you no longer need the Tencent Cloud EdgeOne (EdgeOne) service, you can destroy the EdgeOne plan. Once the plan is in the destroyed state, no further charges related to EdgeOne will be incurred. There are two ways to destroy a plan:

- **Automatic destruction upon expiration/overdue payment:** If the account is in arrears or the plan has expired, the plan will enter the isolated state. Your resources will be retained for 60 days during the isolation period. If no renewal or reversal is made within 60 days, the system will automatically destroy the plan.
- **Manual destruction:** For prepaid plans or Enterprise edition plans that have expired and entered the isolated state, you can choose to manually destroy them.

Note:

- Plan destruction is a sensitive and high-risk operation. Once a plan is destroyed, the system will reclaim your resources and delete related configurations, and **this is irreversible**. If you need re-access, you will have to reconfigure everything.
- Enterprise plan must be terminated completely to stop billing. If you only disable sites without terminating the plan, you will continue to be charged for the plan fee. If you are sure you no longer need it, please terminate the plan promptly.

Destroying a Prepaid Plan (Trial/Personal/Basic/Standard)

1. Go to [EdgeOne console > Service Dashboard](#), select the site corresponding to the plan to be destroyed, and click **Disable** to make the site enter the disabled state.

+ Add new site

example

🔍

🔄

Site/ID	Service area ▼	Access mode ▼	Status ▼	Plan info... ▼	Tag	Operation
<div><div>example.com</div><div>zone-2dq10sbt6gk2</div></div>	Global (MLC excluded)	CNAME	<div><div>✔️</div>Enabled</div>	<div><div>👑</div>Enterpri...</div>	-	<div><div>Disable</div><div>Delete</div><div>More ▼</div></div>

Total items: 1

2. After the site enters the disabled state, click **Delete** and **confirm the deletion** in the pop-up confirmation window.

+ Add new site

example

Site/ID	Service area	Access mode	Status	Plan info...	Tag	Operation
example.com zone-2dqi0sbt6gk2	Global (MLC excluded)	CNAME	Disabled	Enterpri...	-	Enable Delete More

Total items: 1

3. Go to [EdgeOne console > Billing Management > Plan Management](#) to check the state of the plan.

Different plan states require different handling methods:

3.1 If the plan is in the enabled state and meets the refund rules, click **Self-Service Refund** first. After the refund is completed, proceed to **destroy the plan**.

Auto-renew management

Batch renew

Plan information	Bound sites	Plan usage(update monthly)	Plan time	Plan time	Operation
<input type="checkbox"/> Personal / edgeone...	example.com	Security acceleration traffic 0 / 50 GB Security acceleration request 0 / 3 million times	Subscribe at: 2022-01-26 12:25:56 Expiration date: 2023-02-26 12:25:56	<input type="checkbox"/>	Renew n Upgrade Self-serv Destroy F

Auto-renew management

Batch renew

Plan information	Bound sites	Plan usage(update monthly)	Plan time	Plan time	Operation
<input type="checkbox"/> Personal / edgeone...	example.com	Security acceleration traffic 0 / 50 GB Security acceleration request 0 / 3 million times	Subscribe at: 2024-08-12 12:00:00 Expiration date: 2024-10-12 11:59:59 Plan will be destroyed after 1 days, please renew	<input type="checkbox"/>	Renew n Upgrade Self-serv Destroy f

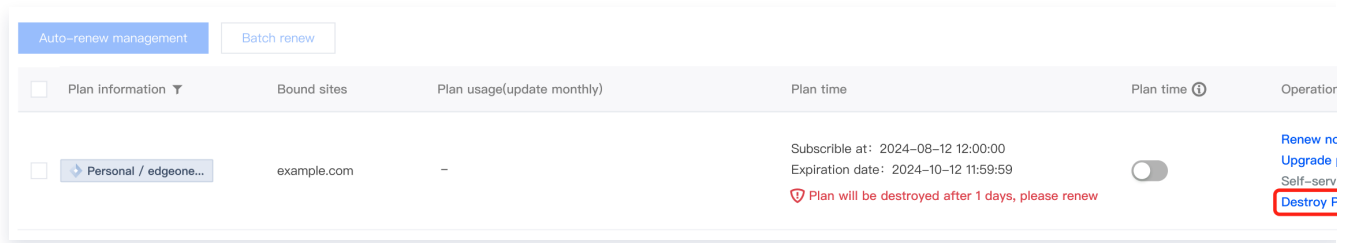
3.2 If the plan is in the enabled state but does not meet the refund rules, simply **disable the auto-renewal switch**. The plan will be automatically destroyed upon expiration.

Auto-renew management

Batch renew

Plan information	Bound sites	Plan usage(update monthly)	Plan time	Plan time	Operation
<input type="checkbox"/> Personal / edgeone...	example.com	Security acceleration traffic 0 / 50 GB Security acceleration request 0 / 3 million times	Subscribe at: 2024-08-12 12:00:00 Expiration date: 2024-10-12 11:59:59	<input type="checkbox"/>	Renew n Upgrade Self-serv Destroy f

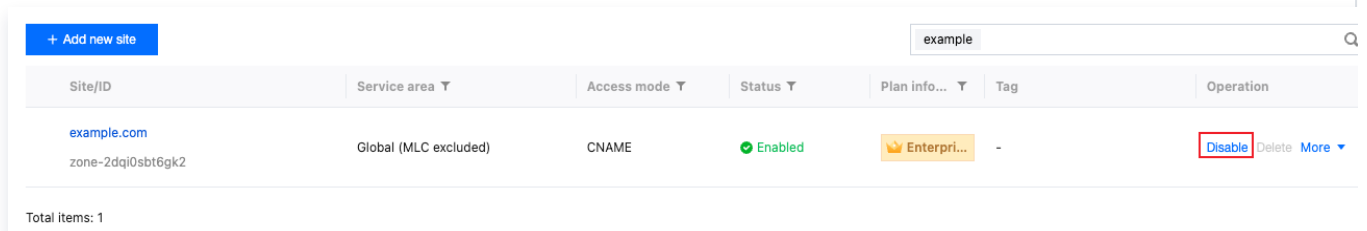
3.3 If the plan has entered the isolated state, click **Destroy Plan** directly. **Confirm** in the pop-up confirmation window to complete the plan destruction.



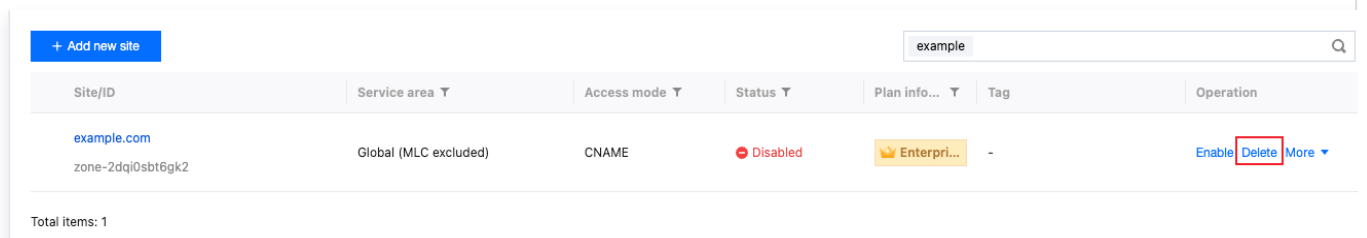
Destroying an Enterprise Edition Plan

Automatically Destroying a Plan by Deleting All Sites

1. Go to [EdgeOne console > Service Dashboard](#), select the site corresponding to the plan to be destroyed, and click **Disable** to make the site enter the disabled state.



2. After the site enters the disabled state, click **Delete** and **confirm the deletion** in the pop-up confirmation window.



3. After you **disable and delete** all sites under the Enterprise edition plan one by one according to Step 1 and Step 2, the Enterprise edition plan will be automatically destroyed.

Manually Destroying a Plan by Disabling All Sites

1. Go to [EdgeOne console > Service Dashboard](#), select the site corresponding to the plan to be destroyed, and click **Disable** to make the site enter the disabled state.

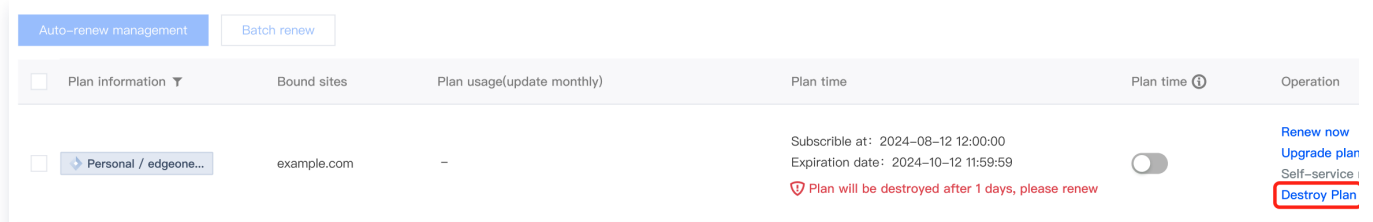
+ Add new site

example

Site/ID	Service area ▼	Access mode ▼	Status ▼	Plan info... ▼	Tag	Operation
<div>example.com</div> <div>zone-2dqj0sbt6gk2</div>	Global (MLC excluded)	CNAME	✔ Enabled	👑 Enterpri...	-	<div><div>Disable</div><div>Delete</div><div>More ▼</div></div>

Total items: 1

2. Disable all sites under the plan one by one according to Step 1. After confirming all sites are disabled, proceed to Step 3.
3. Go to [EdgeOne console > Billing Management > Plan Management](#), find the Enterprise edition plan you want to destroy, click **Destroy Plan**, and **confirm** in the pop-up confirmation window to complete the plan destruction.



Auto-renew management		Batch renew						
<input type="checkbox"/> Plan information	Bound sites	Plan usage(update monthly)	Plan time	Plan time ⓘ	Operation			
<input type="checkbox"/> Personal / edgeone...	example.com	-	Subscribe at: 2024-08-12 12:00:00 Expiration date: 2024-10-12 11:59:59 ⚠ Plan will be destroyed after 1 days, please renew	<input type="checkbox"/>	Destroy Plan Renew now Upgrade plan Self-service			

Site Management

Quickly Importing and Exporting Site Configuration

Last updated: 2025-07-28 14:24:06

This document describes how to quickly export site configuration from one site and import it to another within EdgeOne.

Note:

- This feature only supports sites linked to **Standard** and **Enterprise** plans.
- This feature currently only supports exporting and importing the configuration of the **Site Acceleration > Global Settings/Rule Engine** module in the console.

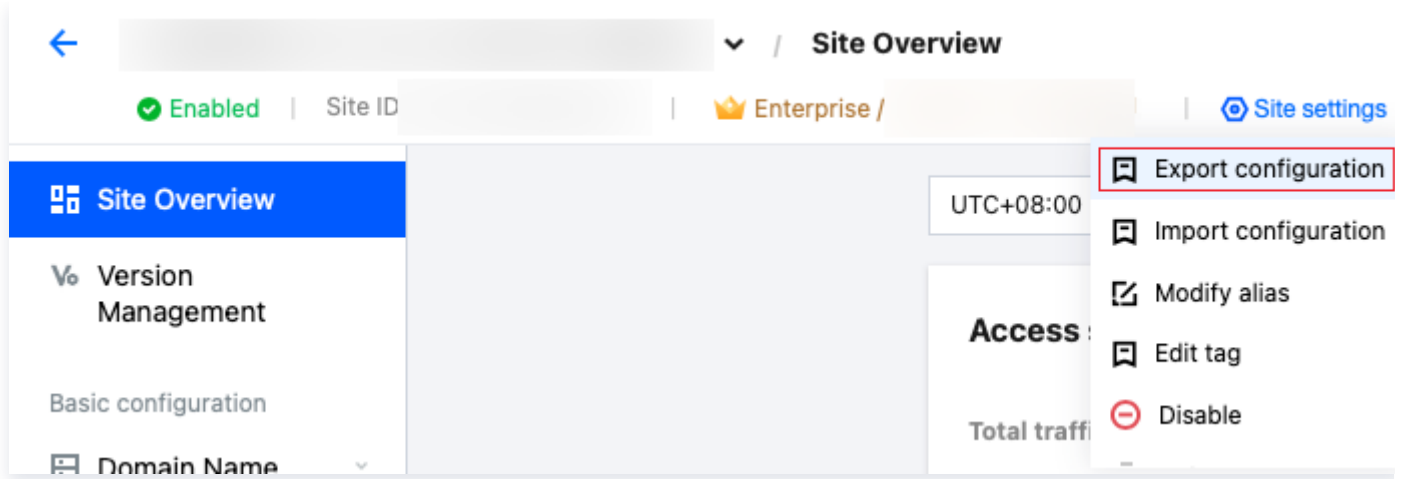
Use Cases

- When you have completed the configuration of one site and need to configure a large number of sites with settings in **Site Acceleration > Global Settings/Rule Engine** similar to those of the already configured site, you can quickly synchronize the configuration via site configuration import/export.
- If your business requires changing the Tencent Cloud account due to special reasons, you can migrate the configuration of **Site Acceleration > Global Settings/Rule Engine** from the old account to the new one through configuration import/export.

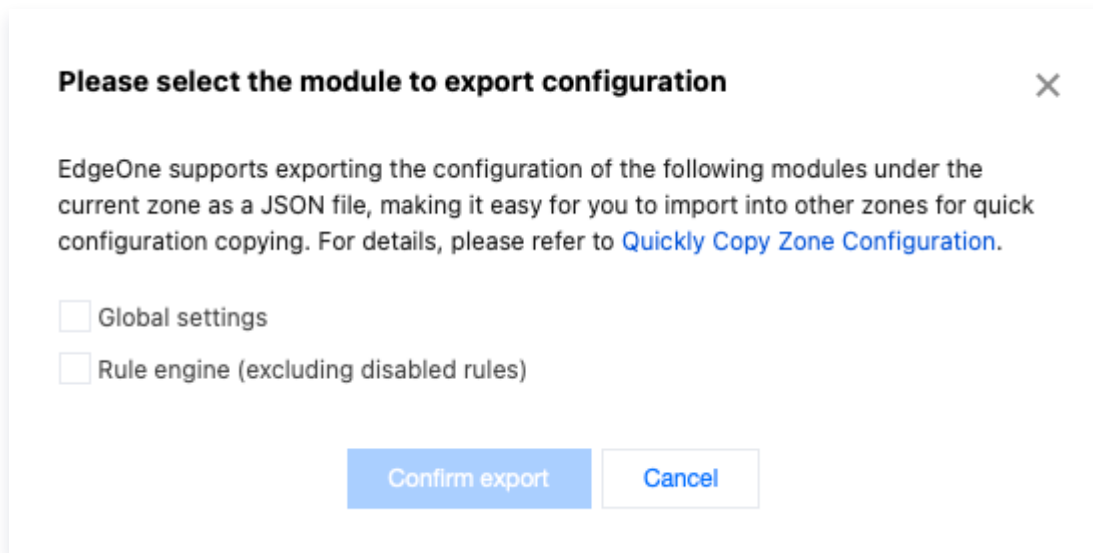
Directions

Step 1: Exporting Site Configuration

1. Log in to the [Tencent Cloud EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** to be configured under **Website Security Acceleration**.
2. In the top site navigation on the site details page, click **Site settings** and then **Export configuration**.



3. Select the module to be exported. You can export **Site Acceleration > Global Settings/Rule Engine** configuration separately, and click **Confirm export**. The exported file is in the JSON format. It is not recommended to modify the contents of the exported file directly. If you need any adjustment, you can [contact us](#).

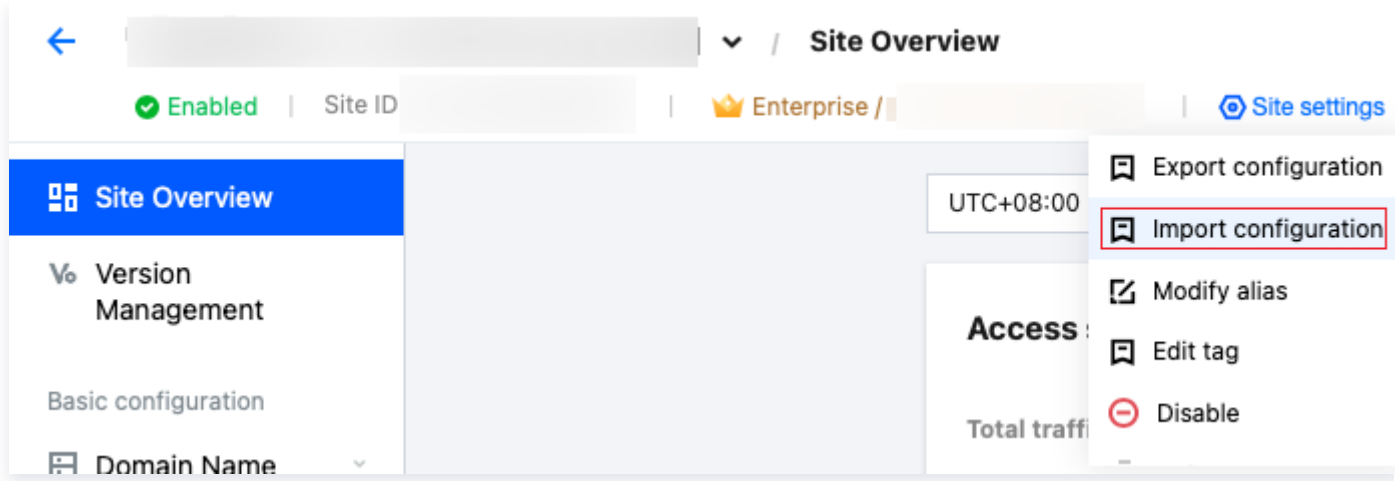


Note:

When **Site Acceleration > Rule Engine** is exported, only the rules that are enabled and actually effective will be exported, excluding the rules that have not been enabled.

Step 2: Importing Site Configuration

1. Log in to the [Tencent Cloud EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** to be configured under **Website Security Acceleration**.
2. In the top site navigation on the site details page, click **Site settings** and then **Import configuration**.

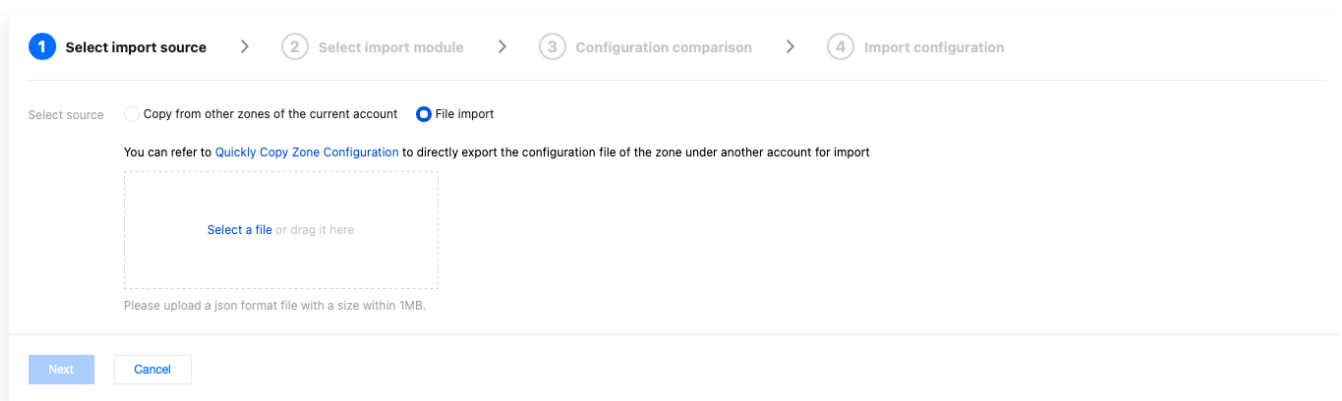


3. Select the import source. You can choose **Copy from other zones of the current account** or **File import**.

- If you choose **Copy from other zones of the current account**, you can directly select the origin server under the current account and click **Next**.



- If you choose **File import**, please select the JSON file exported from [Step 1](#), and drag and drop it into this area to implement cross-account configuration import. The file must be in the JSON format, with its size within 1 MB. Then click **Next**.



4. Select the import module. **Copy from other zones of the current account** allows you to choose **Global Settings** or **Rule Engine** to import configuration separately. If you need to fine-tune the imported configuration, you can modify it directly in this interface without affecting the original site configuration. When **File import** is used, EdgeOne will parse the modules contained in your imported file. You can select the module whose configuration needs to be imported for import and modification. After confirmation, click **Next**.

1 Select import source > 2 Select import module > 3 Configuration comparison > 4 Import configuration

Please select the module to import configuration

☒ Global settings
Global configuration effective for all domain(s) under the zone

☒ Rule engine
Domain-specific configuration

GUI ModeJSON Mode

Global SettingsRule Engine

Smart Routing

Smart routing Paid Add-on

Implement smart routing for clients requesting dynamic resources more quickly, stably and securely by detecting real-time network latency.[Details](#)

Notes:
After smart routing is enabled, the upstream traffic between the client and the EdgeOne node (client -> EdgeOne node) and the smart routing requests will be charged.[Billing description](#)
It's recommended to use this feature for domain names that only contain dynamic resources.

☐

Cache Configuration

EdgeOne Node Cache TTL

Adjust the caching time of resources on EdgeOne nodes, which only takes effect for 2XX status codes. Set the default cache time for 404 to 10 seconds, and do not cache other error status codes. If you need to configure cache for error status codes, please go to the 「Status Code Cache TTL」 operation. [Details](#)

Follow origin server Cache-ControlNo Cache-Control: Default cache policy ⓘGlobal settings

Browser cache TTL

Adjust the span for resources caching in the browser to optimize the browser cache and accelerate the loading of requested resources. [Details](#)

Follow origin server Cache-Control ⓘGlobal settings

BackNextCancel

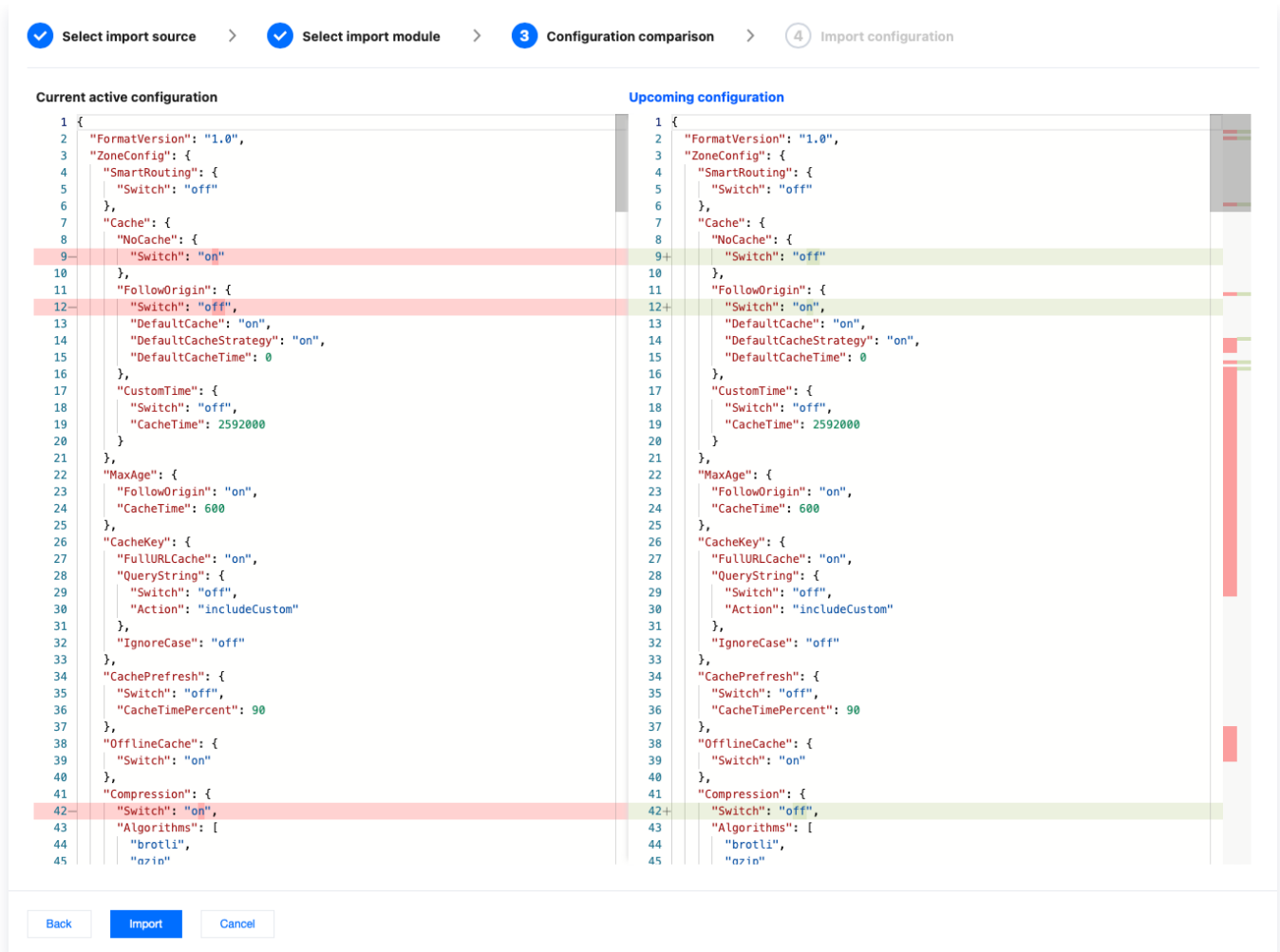
Note:

- EdgeOne offers two configuration display/modification methods: GUI Mode and JSON Mode. It is recommended to perform operation directly in GUI Mode. For configuration modifications via code in JSON Mode, please [contact us](#).
- The contents of the exported configuration file may change as features are iterated and added or decommissioned. When using file import, it is recommended to re-export a copy of site configuration, rather than using a historically saved configuration file.

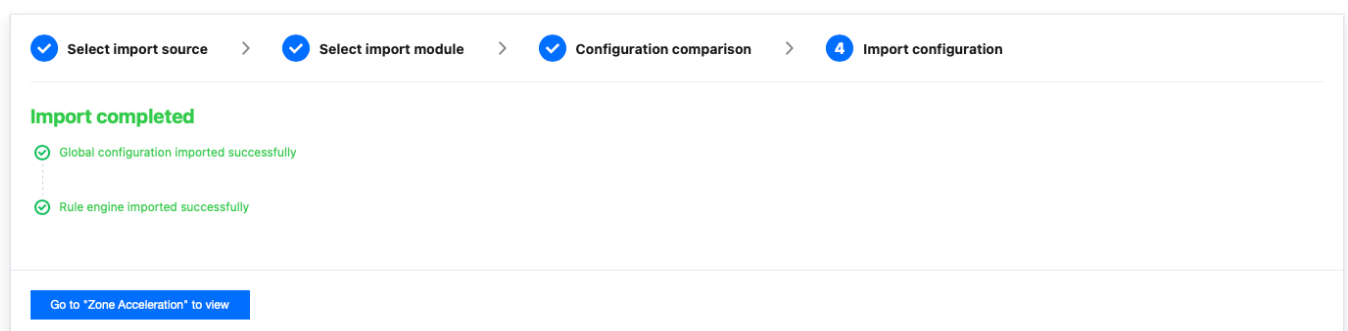
5. The configuration comparison will display differences between the imported configuration and the current effective configuration in the JSON format. You can check the imported configuration for any issue in this step. After confirming there is no issue, click **Import**.

Note:

The imported configuration will overwrite the existing configuration of the corresponding module of the site. Before proceeding with import, please confirm that overwriting the existing configuration will not impact your business.



6. In the secondary popup, click **Confirm No Impact, Continue Import**.
7. The backend will start importing the configuration. After the import is complete, you can go to the **Site Acceleration Module** to view the imported configuration.



General Policy

Custom Response Page

Last updated: 2025-08-14 15:08:31

Feature Overview

In some cases, users may encounter exceptions and receive a response status code when accessing the site. In order to help users better understand the problems and solutions, EdgeOne provides a custom response page feature. This feature can help you inform users of the current website status through a specified custom response page, and avoid users from failing to determine the specific reason and handling method in case of request errors.

EdgeOne offers the custom response page feature in both site acceleration and security protection features. You can perform configuration according to actual scenarios.

- **Custom Site Origin–Pull Error Response Pages:** You can customize the response page content for the origin–pull status codes 4xx or 5xx. For details, see [Custom Error Page](#).
- **Custom Security Protection Policy Block Response Pages:** You can customize the status code and response page content when Web protection or Bot protection block policies are triggered. For details, see [Configuring Custom Response Pages in Security Protection](#).

Additionally, to facilitate management and usage, EdgeOne offers the [Custom Response Page Template](#) feature, which can be used to manage the response page content and be referenced by different feature modules. By editing this response page template, you can simultaneously apply the modified response page content to all referencing feature modules.

Configuring the Custom Response Page Template

You can customize the Content-Type and the included content information of the response page. Refer to the following steps for configuration:

1. Log in to the [EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** to be configured under **Website Security Acceleration**.
2. On the site details page, click **Custom Response Page**.
3. Click **Add Custom Response Pages** and configure the custom response page content. The related parameters are explained as follows:
 - **Content-Type:** The value of the HTTP response header `Content-Type` included in the custom response page during response. Supported values are `application/html`, `application/json`, `text/plain`, and `application/xml`. For example, if

`text/plain` is selected, the HTTP response header `Content-Type: text/plain` will be returned when EdgeOne responds with the custom response page.

- **Page content:** The body of the custom response page, not exceeding 2 KB. It is recommended to contain `{{ EO_REQ_ID }}` in the page content. This field will automatically get the user's request ID information during response, and will be replaced with the request ID to facilitate problem locating.

Add custom response pages ×

Custom response pages name

Custom-Pages1

Supports Chinese, letters, numbers, hyphens, 2-120 characters.

Description

You can enter 60 more characters.

Content-Type

text/html ▼

Enter page content.

File size should not exceed 2KB. You can embed the content `{{EO_REQ_ID}}` in the body of the HTML page, and this field will be replaced with the request ID during the response for easy troubleshooting.[View sample](#)

Save

Cancel

4. Click **Save** to complete the creation of the response page.

Note:

- If the custom response page has already been referenced by other feature modules, it cannot be deleted. If deletion is required, navigate to the feature module referencing this page and dereference it first.
- After a created custom response page is edited and saved, all feature modules referencing this custom response page will automatically apply the edited page.

Referenced in the custom interception page of security protection

Assume that a custom Web protection rule configured for the current site domain `www.example.com` only allows accesses by users within the Chinese mainland, and blocks accesses by users in other regions. When the users in other regions attempt to access, you should inform them of the block reason through a custom response page. You have referred to [Configuring Custom Response Page Template](#) to configure a custom response page named `Custom-Pages1`. Then you can take the following steps to configure it:

1. Log in to the [EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** to be configured under **Website Security Acceleration**.
2. Click **Security > Web Security**. By default, it is a site-level security policy. To configure differentiated security policies for a specific domain name under the current site, you can enter the **Domain-level security policy** tab and click the **corresponding domain name** to enter the configuration page for the domain-level security policy. The subsequent steps are the same.
3. Under the custom block page classification, select the block page module you need to configure. For example, you can select the **Web Protection Block (except by Managed Rules)** page and click **Edit**.
4. On the edit page, configure the content of the custom response page, select **Use file page** for blocking, and choose the pre-configured page named `Custom-Pages1`. The configuration items are described as follows:
 - Page type: Supports three types: default page, URL page, and file page, where the file page refers to custom response page content.
 - Custom interception page status code: Supports configuring 200–299, 400–599 as custom interception page status codes. The default status code is used when not selected.

Edit Web Protection Block (except by Managed Rules) ✕

Customize the response sent to clients when their requests are blocked by Custom Rules, Rate Limiting or Bot Management.

Use file page ▼

Custom-pages1 ▼

✓

[View all custom response contents](#)

☐ Custom status code

567

Save

Cancel

5. Then click **Save** to complete the configuration.

IP Groups

Last updated: 2025-09-01 15:30:54

An IP group contains a list of IPs or CIDR IP ranges. You can reference the IP group in DDoS protection and Web protection rules to simplify configuration and maintenance.

Note:

1. IP groups support cross-site usage. After creating an IP group, you can directly reference it in other sites to ensure consistent policies across different sites.
2. Up to 100 groups can be configured under the same account, and each IP group can include up to 2,000 IPs or CIDR IP ranges. To configure IP group matching in Web protection rules, see [Match Condition](#) for related limits.

Scenario 1: Group Management of IP Information with Business Threats

Example Scenario

A large game customer has connected sites `example.com` and `site.com`. Currently, through the security intelligence library and their own business security, a blocklist of IPs with business threats has been identified. These IP addresses will change dynamically, so they need to be updated in real-time and applied to all site domain names, instantly blocking these IPs.

Directions

1. Log in to the [Tencent Cloud EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** to be configured under **Website Security Acceleration**.
2. On the site detail page, click **Security > General Settings**.
3. In the IP groups tab, click **Edit**.
4. Click **Create** to create a group. Enter the group name and the IP address or IP range contained in the group, such as `1.1.1.1/23` and `1.2.2.2`. Separate multiple IP addresses with carriage returns.
5. Click **Save** to complete the IP group creation.

Create Batch import

Enter the group name or CIDR address Q

ID	Group name	List of IP groups	Operation
	<input type="text" value="my_block_ip"/>	<div>1.1.1.1/23 ✕ 1.2.2.2 ✕</div>	Save Cancel

Total items: 0 10 / page 1 / 1 page

6. After creating the IP group, as an example for this scenario, you need to disable access for all IPs within the group. You can add basic access control rules on the `example.com` and `site.com` 's **Web Security** page. When adding rules, choose **Client IP equals the group name** to perform **Block**. This will intercept all IP access within the group and dynamically update based on included IPs. For detailed configuration steps, refer to [Custom Rules](#).

Add rule Batch disable Batch delete

Search rule ID/name Q

<input type="checkbox"/> Rule ID	Rule name	Field	Matching method	Value	Action	Status	Operation
<input type="checkbox"/>	<input type="text" value="block_ips"/>	<div>Client IP</div>	<div>Is</div>	<div>my_block_ip ✕</div>	<div>Block</div>	<div><input checked="" type="checkbox"/></div>	Save Cancel

Total items: 1 5 / page 1 / 1 page

7. (Optional) After configuring the rules, if you identify new risky IPs that need to be added to the group and applied to all sites, you can follow steps 1–3 to re-enter the site where the template was created, click **Edit**, enter the new IP addresses, and click **Save** to apply the new IPs to all protection policies that use this group.

[Create](#) [Batch import](#)

ID	Group name	List of IP groups	Operation
13453	<input type="text" value="my_block_ip"/>	<div>1.1.1.1/23 ✕ 1.2.2.2 ✕ 3.3.3.3 ✕</div>	Save Cancel

Total items: 1 10 / page 1 / 1 page

Scenario 2: Adding Automatically Expiring IPs in Batch to an Existing IP Group

Example Scenario

An e-commerce customer has configured a long-term valid custom interception rule on the site `example.com`, referencing the IP group named `block_ip` to manage blocklist IPs in a unified way. During promotional events, a batch of IPs exhibiting risk behaviors such as malicious crawling and abnormal order placement were identified through monitoring. Since these risks only exist during the activity period, the customer wants to temporarily add these IPs to `block_ip` and set a unified expiry date, automatically removing them at the end of activity to avoid long-term blocking of legitimate users, while keeping the existing interception rules in effect without additional maintenance of new protection policies.

Directions

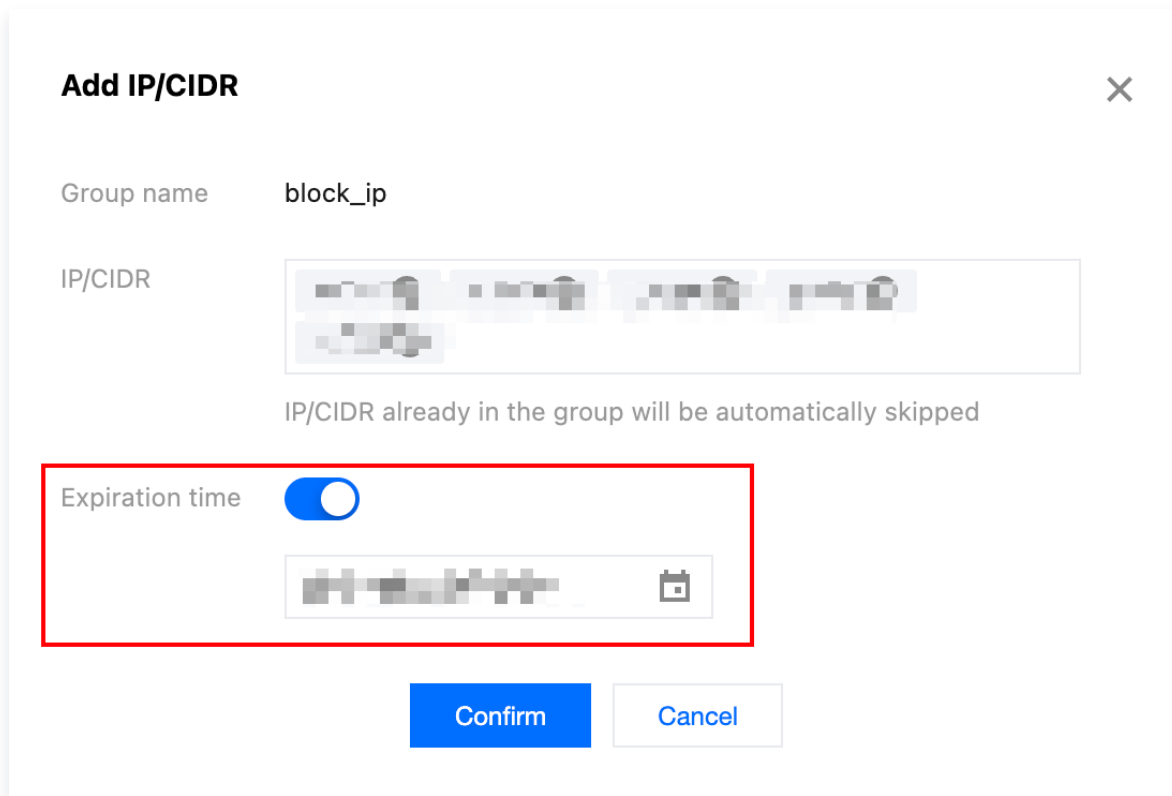
- Log in to the [EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** that needs to be configured under **Website Security Acceleration**.
- Click **Security Protection > General Settings** to enter the configuration options details page.
- In the IP group card, locate the target IP group (such as `block_ip`), then click **Edit**.
- In the editing page, click **Add**.

block_ip ✕

ⓘ • Expired IP/CIDRs will be retained for 7 days.

[Add](#) [Delete](#) [Modify](#)

5. In the pop-up window for adding IP or ranges, input the IP address or ranges that need temporary control (bulk entry is supported, multiple addresses are separated by pressing enter). Check **Expiration time** and set the expiration time.



Add IP/CIDR [X]

Group name `block_ip`

IP/CIDR [IP addresses]

IP/CIDR already in the group will be automatically skipped

Expiration time ☒ [Date/Time]

[Confirm] [Cancel]

6. Click **Confirm**. Once saved, the temporary control IP will take effect immediately and be automatically removed from `block_ip` upon expiration.

Scenario 3: Adjusting the Expiry Time of IPs with Scheduled Expiration

Example Scenario

For site `example.com`, the `block_ip` IP group has set a 7-day expiry for a batch of abnormal request source IPs. Subsequent analysis detected ongoing attack behavior, requiring these IPs' expiry dates to be extended by 14 days.

Directions

1. Log in to the [EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** that needs to be configured under **Website Security Acceleration**.
2. Click **Security Protection** > **General Settings** to enter the configuration options details page.
3. In the IP group card, locate the target IP group (such as `block_ip`), then click **Edit**.
4. On the editing page, select the IP address or ranges that need expiry time adjustment, then click **Modify**.

block_ip ×

ⓘ • Expired IP/CIDRs will be retained for 7 days.

Add **Delete** **Modify** 🔍 🔄

− IP/CIDR	Expiration Time	Status
<input type="checkbox"/> [blurred]	2025-08-31 00:00:00	✓ Active
<input checked="" type="checkbox"/> [blurred]	2025-08-31 00:00:00	✓ Active
<input checked="" type="checkbox"/> [blurred]	2025-08-31 00:00:00	✓ Active
<input checked="" type="checkbox"/> [blurred]	2025-08-31 00:00:00	✓ Active
<input checked="" type="checkbox"/> [blurred]	2025-08-31 00:00:00	✓ Active

Total items: 5 (Selected items: 4) 200 ▾ / page ⏪ ⏩ 1 / 1 page ⏴ ⏵

5. In the pop-up window for modifying scheduled expiration time, set a new expiry date.

Modify Expiration Time ×

Group name block_ip

IP/CIDR [blurred]

Expiration time ☐ Permanent retention ☒ Scheduled expiration

📅

Confirm **Cancel**

6. Click **Confirm**. Once saved, these IPs will be automatically removed based on the latest expiry time.

Content Identifier

Last updated: 2025-07-04 11:44:22

Content Identifier is a capability provided by Tencent Cloud EdgeOne (EdgeOne) to label request data. With Content Identifier, you can configure a unique identifier for each request, enabling more detailed statistics, analysis, and monitoring of your business distribution content through metric analysis and billing usage statistics.

Note:

The Content Identifier feature is only available to the allowlist. If you need to use it, please [Contact Us](#).

Feature Overview

EdgeOne configures content identifiers for requests that meet specific matching conditions through the **Rule Engine**. During the response, it identifies the request with the `Content-Identifier` header. Requests that meet this matching condition will be counted under the corresponding Content Identifier. In **Metric Analysis** and **Billing Usage Statistics**, data can be filtered and viewed through this Content Identifier.

```
[(曼谷-亚太一)root@43.152.224.88~]$ curl -v
* Rebuilt URL to:
* Trying
* TCP_NODELAY set
* Connected to port 80 (#0)
> GET / HTTP/1.1
> Host:
> User-Agent: 123
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx/1.14.1
< Content-Type: text/html
< ETag: "5d9bab28-fd9"
< Last-Modified: Mon, 07 Oct 2019 21:16:24 GMT
< Content-Length: 4057
< Accept-Ranges: bytes
< Connection: keep-alive
< Date: Tue, 17 Dec 2024 12:32:38 GMT
< EO-LOG-UUID: 15910223454641874849
< EO-Cache-Status: MISS
< Content-Identifier: eocontent-
<
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
  <head>
    <title>Test Page for the Nginx HTTP Server on Red Hat Enterprise Linux</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <style type="text/css">
      /**/
      body {
        background-color: #fff;
        color: #000;
        font-size: 0.9em;
        font-family: sans-serif,helvetica;
        margin: 0;
        padding: 0;</pre></div><div data-bbox="45 577 287 599" data-label="Section-Header"><h2>Applicable scenario</h2></div><div data-bbox="50 613 953 677" data-label="List-Group"><ol><li>1. Applicable for labeling and grouping requests that meet specific matching conditions for data analysis.</li><li>2. Applicable for labeling and grouping requests that meet specific matching conditions and querying billing usage statistics.</li></ol></div><div data-bbox="45 692 227 713" data-label="Section-Header"><h2>Best Practices</h2></div><div data-bbox="45 728 956 768" data-label="Text"><p>The following will introduce how to create and configure content identifiers for statistical analysis and usage queries in <b>Metric Analysis</b> and <b>Billing Usage</b>.</p></div><div data-bbox="45 782 234 803" data-label="Section-Header"><h2>Sample Scenario</h2></div><div data-bbox="45 817 956 880" data-label="Text"><p>Assuming you have already integrated the acceleration domain <code>www.example.com</code>, you want all requests to <code>www.example.com/image</code> to be tagged by the content identifier and use this content identifier to filter, count, and analyze access requests.</p></div><div data-bbox="45 894 477 915" data-label="Section-Header"><h2>Step One: Creating a Content Identifier</h2></div><div data-bbox="45 962 400 980" data-label="Page-Footer">©2013-2025 Tencent Cloud. All rights reserved.</div><div data-bbox="841 962 960 980" data-label="Page-Footer">Page 42 of 47</div>
```

1. Log in to the [EdgeOne Console](#), in the left menu bar, click **Content Identifier** to enter the content identifier list page.
2. On the content identifier list page, click **Add Content Identifier**.
3. To add a content identifier, you need to fill in the description and bind a package. Tags can be selected as needed. The configuration items are described as follows:

Configuration Item	Description
Description	Used to record the purpose of the content identifier, you can enter 1–128 characters.
Package	<p>Only supports binding to purchased Enterprise Edition packages. If you currently do not have an Enterprise Edition package to bind, please complete the purchase through the process of adding a new site.</p> <div><p>Note:</p><ol style="list-style-type: none">1. Content identifiers can be used to collect billing data, which is strongly associated with the package. Therefore, each content identifier needs to be bound to a package when created.2. To use a content identifier in a site, ensure that the package bound to the site matches the package bound to the corresponding content identifier.</div>
Tag	Optional parameter for permission control and billing. You need to first go to the Tag Console to create the corresponding tags before you can pass in the corresponding tag key and tag value here.

4. After creation, EdgeOne automatically generates an ID for the content identifier for you. For example:

```
eocontent-35jh1wm93khk
```

Content Identifier	Description	Number of references	Plan	Tag	Operation
eocontent-35jh1wm93khk	image	0	Enterprise /	-	Delete

Step Two: Configuring a Content Identifier

1. Log in to the [TencentCloud EdgeOne console](#), enter **Service Overview** in the left menu bar, and click the **site** to be configured under **Website Security Acceleration**.

- On the site details page, click **Site Acceleration** to enter the global configuration page, then click the **Rule Engine** tab.
- On the rule engine management page, click **Create Rule** and select **Add Blank Rule**.
- On the rule editing page, set the matching conditions that trigger the rule to
`HOST = 'www.example.com'` and `URL Path = '/image'`.
- Click **Operation > Selection Box**, in the pop-up operation list, select the operation as **Set Content Identifier**, and choose the content identifier with the ID `eocontent-35jh1wm93khk` created in Step One.

The screenshot shows the 'IF' configuration section with two conditions. The first condition has 'Matching type' as 'HOST', 'Operator' as 'is in', and 'Value' as 'www.example.com'. The second condition has 'Matching type' as 'URL Path', 'Operator' as 'is in', and 'Value' as '/image'. Below these conditions, there is an 'Action' section with 'Set Content Identifier' and a dropdown menu showing 'cid' as the selected content identifier.

Note:

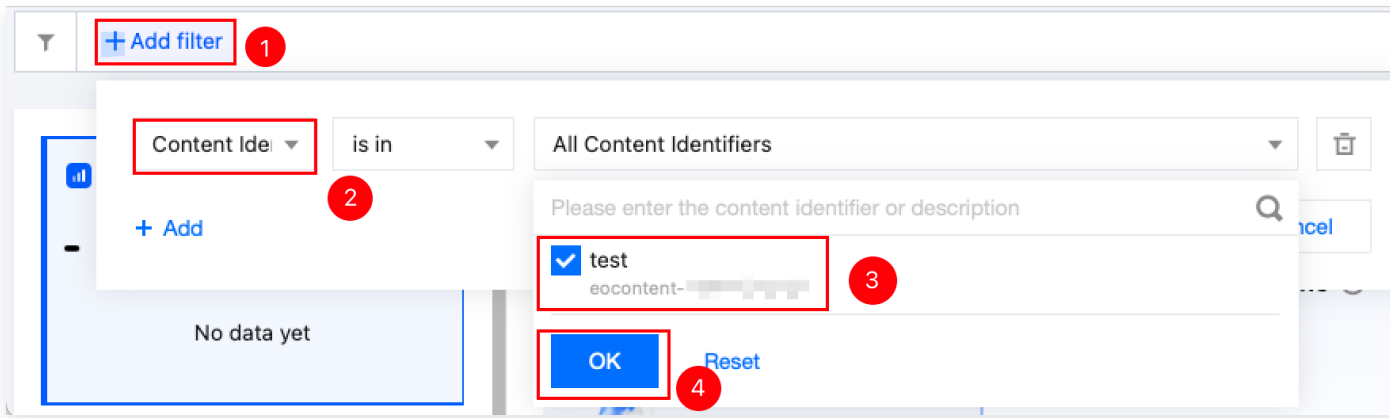
The content identifier drop-down list only displays content identifiers bound to the current site package and does not support cross-package configuration of content identifiers.

- Click on **Save and Publish** to complete the configuration of this rule.

Step Three: Analyzing Data Using a Content Identifier

If you currently need to view request access data of a specified type through a content identifier, you can refer to the following steps:

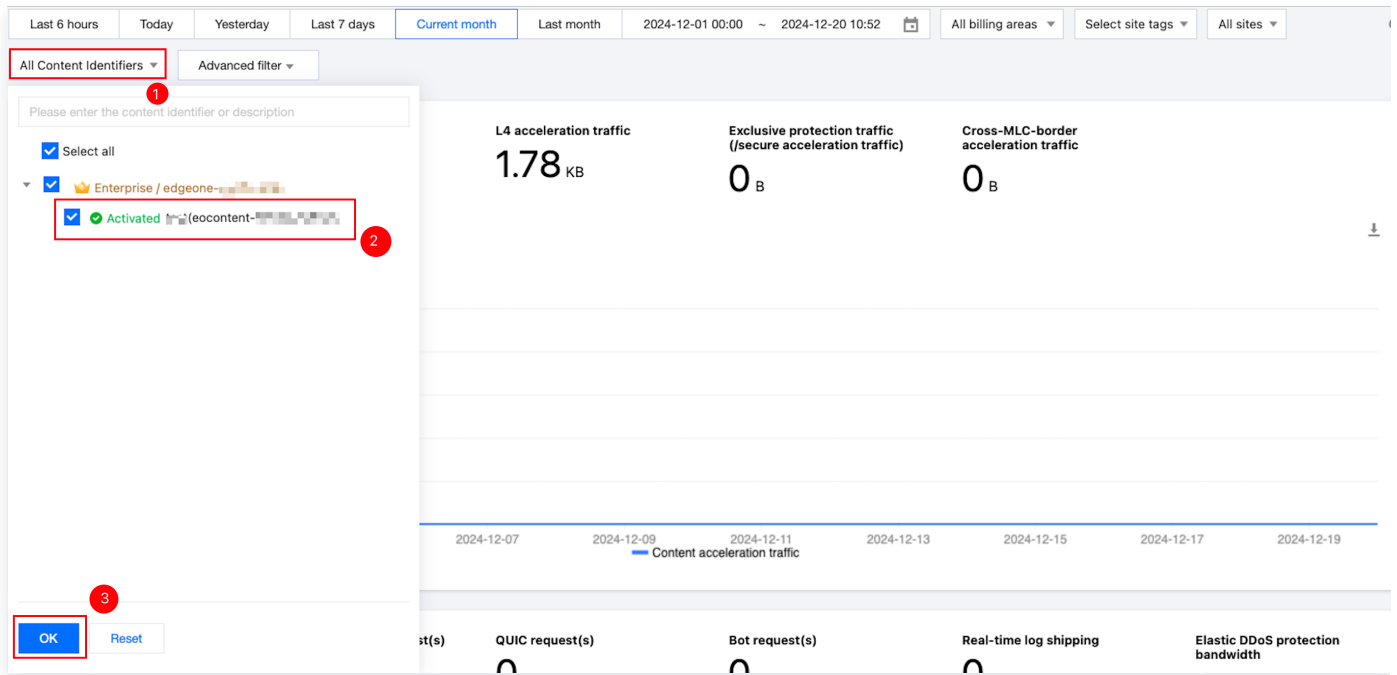
- Log in [EdgeOne console](#), in the left menu bar, click **Indicator Analysis**, to enter the Indicator Analysis page.
- Click **Add Filter**, select the specified content identifier as the filter condition, and click **OK** to apply the filter.

**Note:**

1. Currently, only querying L7 access data by content identifier is supported.
2. Content identifier filter conditions and site filter conditions cannot be added simultaneously.
3. To add other filter conditions, refer to [How to Use Filter Conditions](#) to add other filter conditions such as status code, cache status, etc. To adjust the query time range, refer to [How to Modify the Query Time Range](#).
4. Requests are counted under the site or content identifier based on a mutually exclusive logic. In the example scenario, requests to `www.example.com/image` can be queried under the filter condition " **Content identifier is in eocontent-35jh1wm93khk** ", while requests to all other paths of `www.example.com` can be queried under the filter condition " **Site is in example.com** ". They will not be counted twice. The site overview page only displays data belonging to the current site, and does not display data belonging to the content identifier.
5. If you want to directly query all request usage for the domain `www.example.com` in a scenario configured with a content identifier, you can set the filter condition to " **Host is in www.example.com** ".

Step Four: Querying Billing Usage by Content Identifier

1. Log in to the [TencentCloud EdgeOne console](#), click **Billing Management > Billing Usage** in the left sidebar to enter the Billing Usage page.
2. Click **All Content Identifiers**, select the specified content identifier as the filter condition, and click **OK** to apply the filter.



Note:

- Currently, only the following billing usage data can be queried by content identifier: content acceleration traffic, intelligent acceleration traffic, L7 independent protection traffic, L7 Chinese mainland network optimization traffic, HTTP/HTTPS requests, intelligent acceleration requests, QUIC requests, Bot requests;
- Content identifier filter conditions and site filter conditions cannot be added simultaneously.
- Requests are counted under the site or content identifier based on a mutually exclusive logic. In the example scenario, requests to `www.example.com/image` can be queried under the filter condition " **Content identifier is in eocontent-35jh1wm93khk** ", while requests to all other paths of `www.example.com` can be queried under the filter condition " **Site is in example.com** ". They will not be counted twice.
- If you want to directly query all request usage for the domain `www.example.com` in a scenario configured with a content identifier, you can set the filter condition to " **Host is in www.example.com** ".

Related API Reference

- [CreateContentIdentifier](#)
- [DescribeContentIdentifiers](#)
- [ModifyContentIdentifier](#)
- [DeleteContentIdentifier](#)
- [DescribeTimingL7AnalysisData](#)
- [DescribeTopL7AnalysisData](#)
- [DescribeBillingData](#)

Note:

When calling the API to query related usage by content identifier, please pass the content identifier (e.g., `eocontent-35jh1wm93khk`) into the `ZoneId` parameter for use.