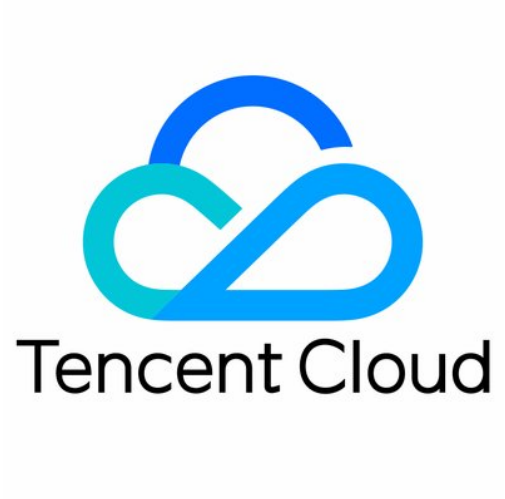
# Tencent Cloud EdgeOne

# Operation Guide

## Product Documentation



# Contents

# Operation Guide
# Site Overview

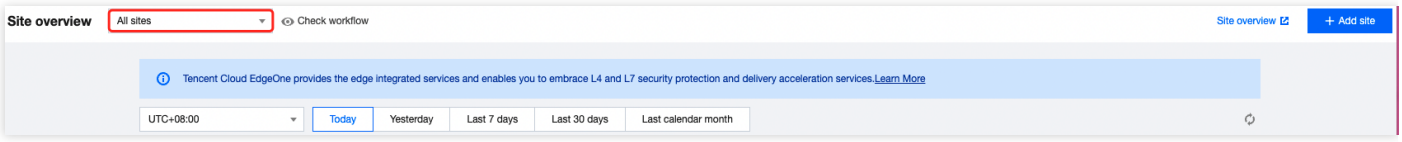
Last updated：2022-08-01 11:35:03

## Overview

The EdgeOne overview page allows you to quickly view the overall status of the current site and access feature pages and product documentation through quick links. It contains the acceleration and security service data, site management, service status, FAQs, and documentation modules.

## Directions

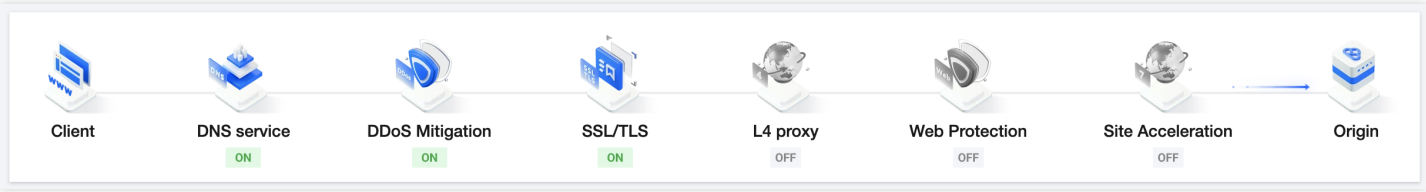
1. Log in to the EdgeOne console and click **Service Overview** on the left sidebar.
2. On the service overview page, **All sites** is selected by default. You can select a specific site to view its details.




3. On the service overview page, you can view workflows, site management information, data overview, FAQs, and documentation.

### Workflow

On the top of the page, you can see the different service modules, core features, and connection status of the selected site. You can quickly view its enabled and disabled product services and enter core feature pages through quick links.




Note：
If **All sites** is selected, the connection statuses of different service modules don't change dynamically. They will change dynamically only when a specific site is selected.

## Site management

1. In the site management module, you can view the site's status and package information.

- Status:
  - Enabled: It is detected that the NS or CNAME record of a connected site has been updated successfully and pointed to EdgeOne.
  - Ineffective: A site has been added, but its NS or CNAME record has not been updated.
  - Disabled: All EdgeOne services (DNS, acceleration, and security protection services) have been disabled for a previously enabled site.
- Package information: Package version and expiration time of each site.

2. In the site management module, you can click **Manage** to enable, disable, and delete a site.

- Enable: Enable all EdgeOne services again for a disabled site.

> Note：
> After enabling the site, check whether the services take effect (you may need to modify the NS or CNAME record).

- Disable: Disable all EdgeOne services for an enabled site.

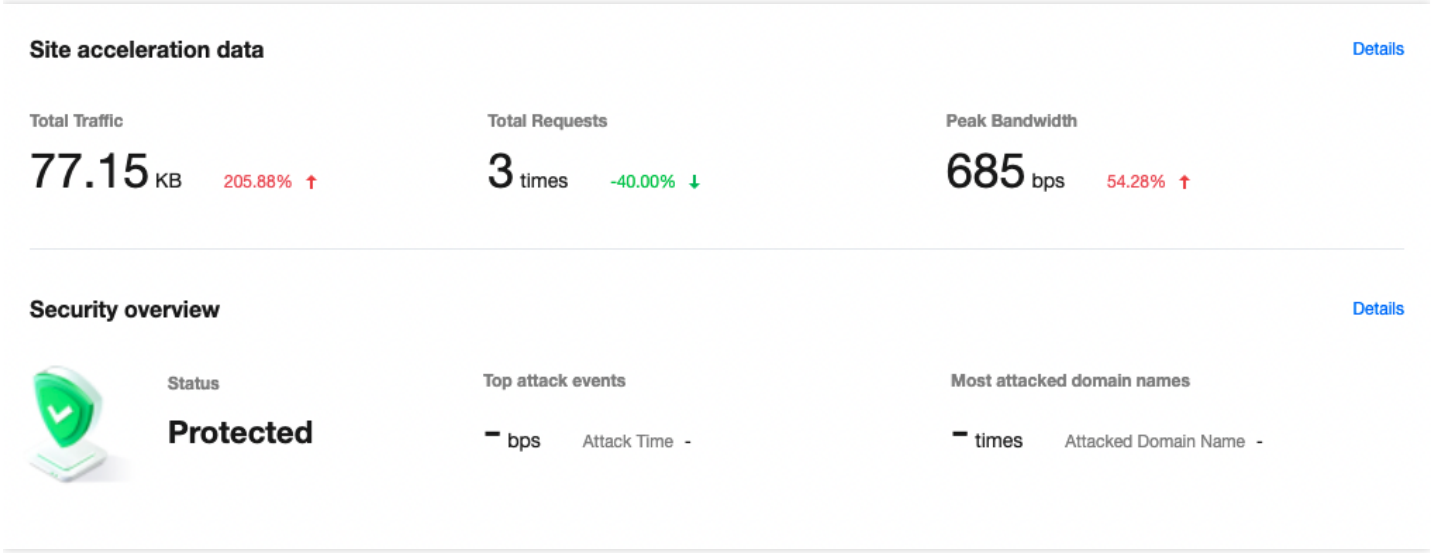
> Note：
> Check and confirm your site's DNS.

- Delete: Delete a site. Once the site is deleted, all its configuration data will be cleared. To use the site again, you need to connect it again.

> Note：
> You must disable the site service first before deleting a site.

## Data overview

The data overview module displays the overview of business access and security protection data of all sites. As data aggregation has a delay, all data is for reference only. For detailed data, see Data Analysis.




Note：
All data is client access log data (i.e., application layer data), which may differ from the data used for billing.
The volume of data generated during actual network transfer will be greater than that of application layer data.
For specific billable usage, the actual bill shall prevail.

## FAQs

The FAQs module displays FAQs about product services.

## Documentation

The documentation module lists product service documents.

# Data Analysis
# Traffic Analysis

Last updated：2022-08-03 10:17:23

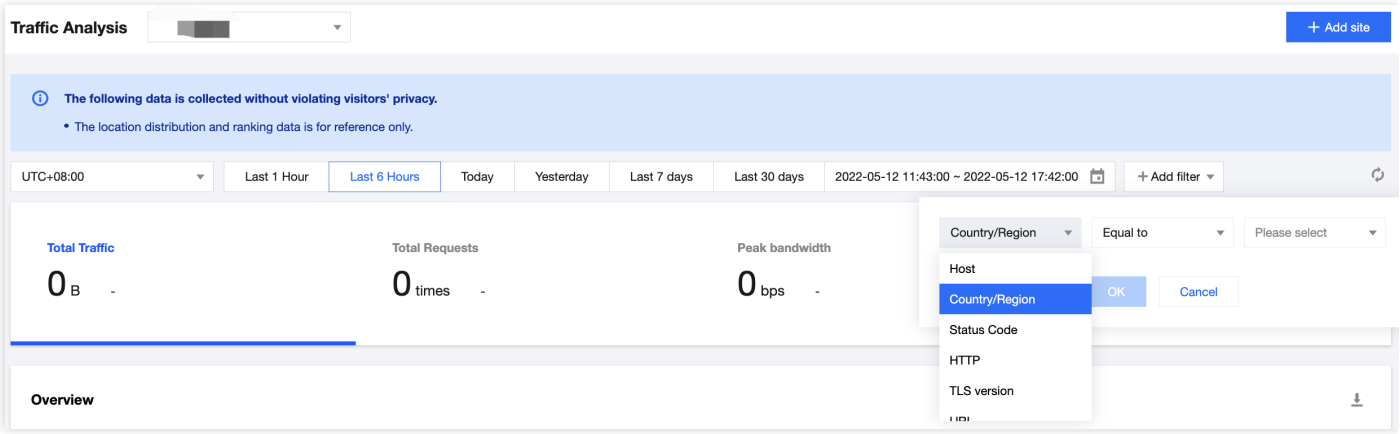
## Overview

EdgeOne provides diverse metrics for you to stay on top of the business data in multiple dimensions by analyzing the business access log data. Due to the impact of latency and algorithm, the distribution and ranking data is for reference only, and actual log analysis data shall prevail.

## Directions

### Query conditions

1. Log in to the EdgeOne console. Click **Data Analysis** > **Traffic analysis** on the left sidebar.
2. On the **Traffic analysis** page, select the target site. You can also filter data by time or click **Add filter** to filter data by conditions such as country/region, host, and device type.




**Parameter description:**

- Site: View the data of all sites or a single site.
- Metric: You can click **Total traffic** or **Total requests** to view metrics such as hosts, client IPs, URLs, and referers collected based on the total traffic or requests. To view peak bandwidth over time and by region (country/region), you can click **Peak bandwidth**.

Note：

- Bandwidth-related metrics only support "Host", "Country/Region", and "HTTP".
- Time zone adjustment will take effect for the entire **data analysis** feature.
- The period between the query start time and end time cannot exceed 30 days.

- Time granularity:
  - Within 1 hour: 1 minute.
  - 1 hour - 1 day: 5 minutes.
  - Within 7 days: 1 hour.
  - 7 days and above: 1 day.

- Filters:
  - **Country/Region**: Country/Region of the access source. You can select multiple countries/regions.
  - **Host**: Subdomains under the site.
  - **Status code**: Access status code.
  - **Device type**: Hardware device type of the access source. Valid values include Empty, TV, Tablet, Mobile, Desktop, and Others.
  - **Browser type**: Browser of the requester
  - **System type**: OS of the requester
  - **Network protocol**: Network protocol of the request. Valid values include **http/2.0**, **http/1.1**, **https/2.0**, and **https/1.1**.
  - **TLS version**: Version of TLS. Supported versions: TLS1.0, TLS1.1, TLS1.2, and TLS1.3.
  - **URL**: URL to access, such as "/content".
  - **Referer**: Referer information, such as "example.com".
  - **Resource type**: Type of resources, such as PNG and JSON.

### Data Overview

The **Overview** section shows the data trend by the set filters and metrics for the specified time period.

## Distribution of Country/Region

The Country/Region module displays the top 10 countries/regions by identifying client IPs by the set filters and metrics.

## Status Codes

The Status Code module displays the numbers and distribution of status codes returned for different client access requests.

### Rankings

The data ranking module displays the top 5 and top 10 hosts (subdomains), client IPs, URLs, Referers, resource types, and client device types by the selected filters. You can download the complete statistics to view more details for business analysis. You can also view the specific logs to get more data.

# Cache Analysis

Last updated：2022-10-08 18:29:25

## Overview

The multi-dimensional cache analysis provides a detailed image of access traffic or client requests responded by the cache on EdgeOne nodes. This helps determine your optimal configuration that can reduce the load on the origin server and response time.

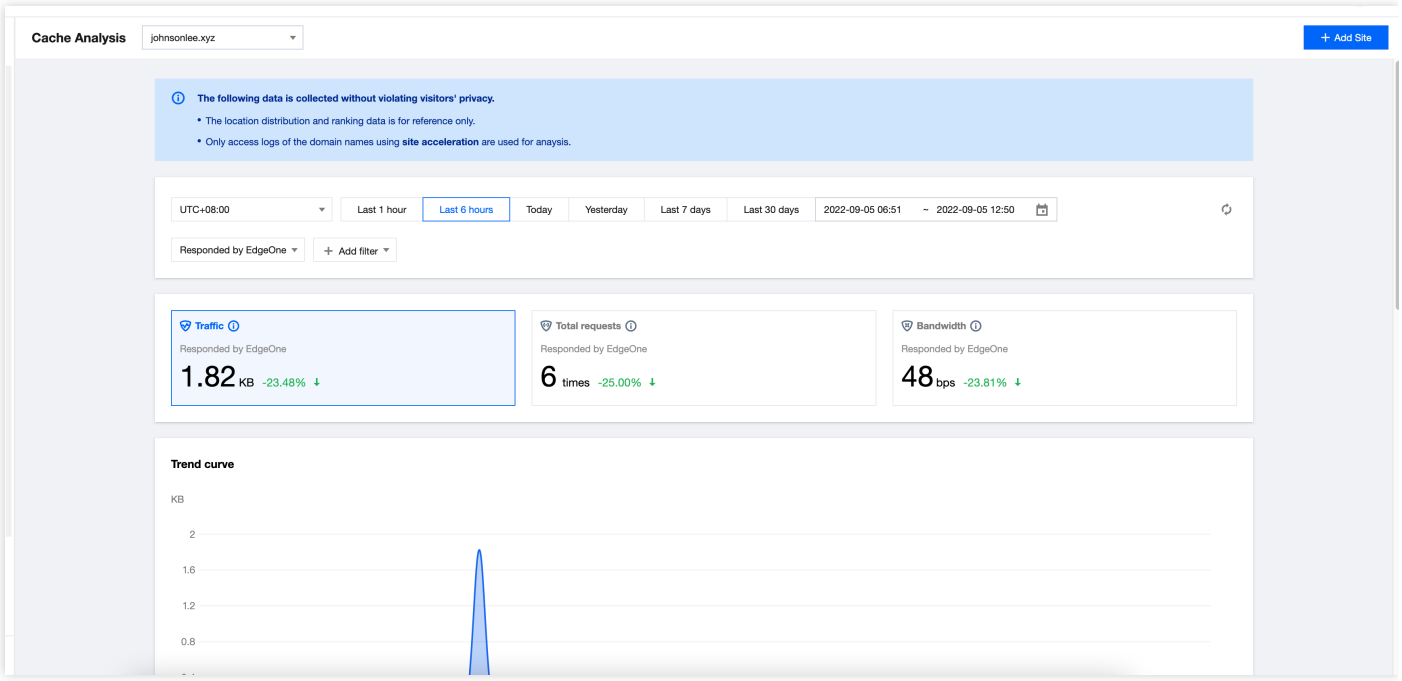
> Note：
> The EdgeOne console is now only available to beta users. Contact us to join the beta.

## Directions

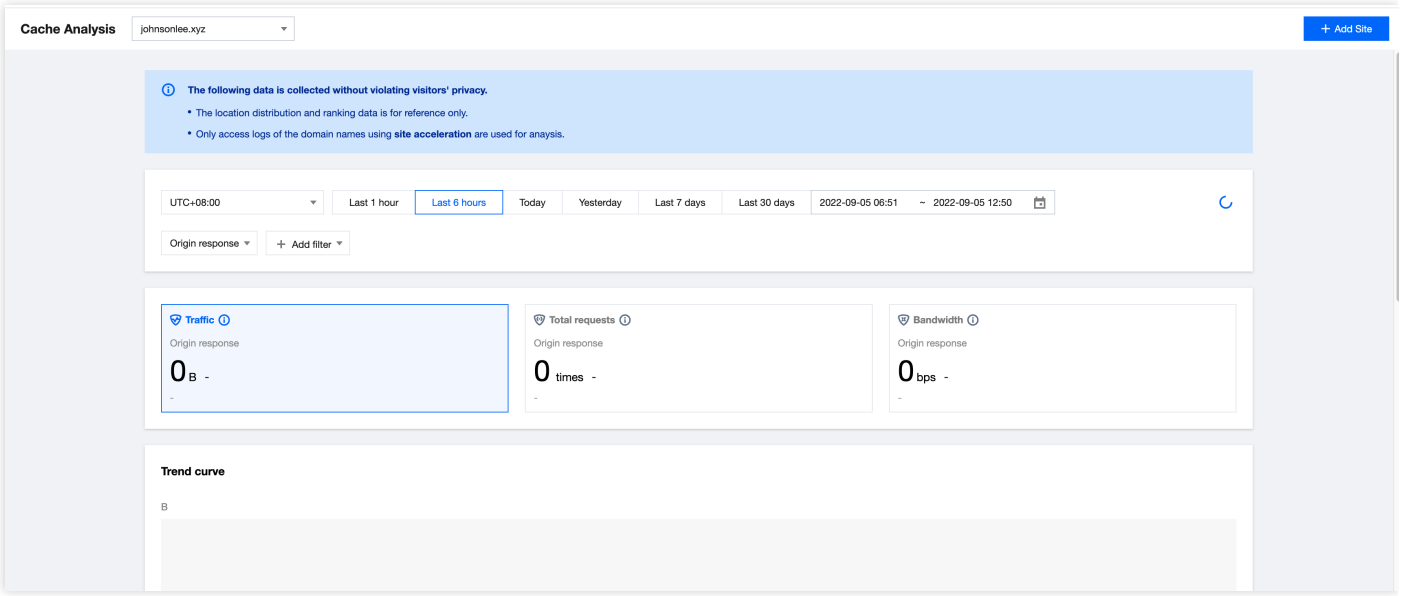
**Query conditions**

1. Log in to the EdgeOne console. Click **Data Analysis** > **Cache Analysis** on the left sidebar.
2. On the page that appears, select the target site and query filters.

- Responded by EdgeOne: The client requests are directly responded by the cache on EdgeOne nodes.



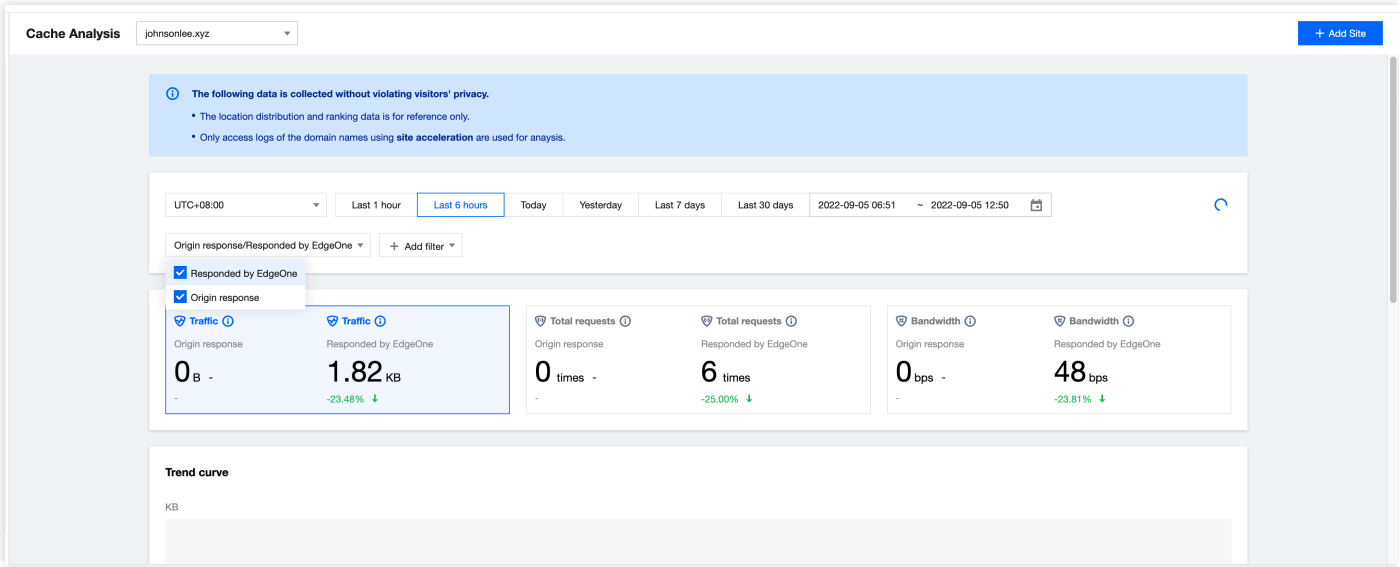

- Responded by origin: The client requests are responded by the origin server.




- You can switch between views of traffic and requests or view both while keeping filters (such as Hosts and URLs) enabled.

Note：

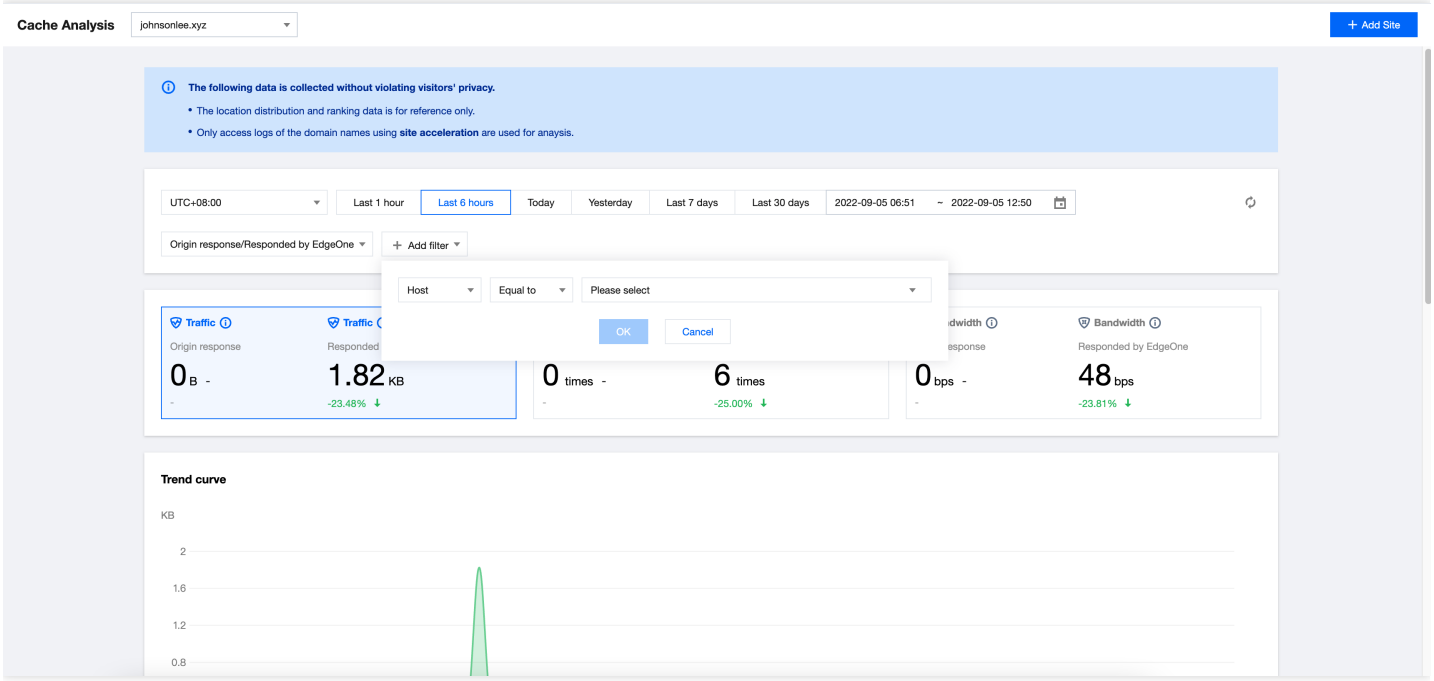
- Select **Responded by EdgeOne**/ **Responded by origin** to view the data you want to focus on, or select both to view two types of data.
- Only traffic generated when EdgeOne serves client requests is recorded.




- You can view data for a specific time period.

Note：

- Time zone adjustment will take effect for the entire **data analysis** feature.
- The time between the start time and end time of a single query cannot exceed 30 days.




- Time granularity:
  - Last 1 hour: Display data at 1-minute intervals.
  - Last 6 hours/Today/Yesterday: Display data at 5-minute intervals.
  - Last 7 days: Display data at 1-hour intervals.
  - Last 30 days: Display data at 1-day intervals.

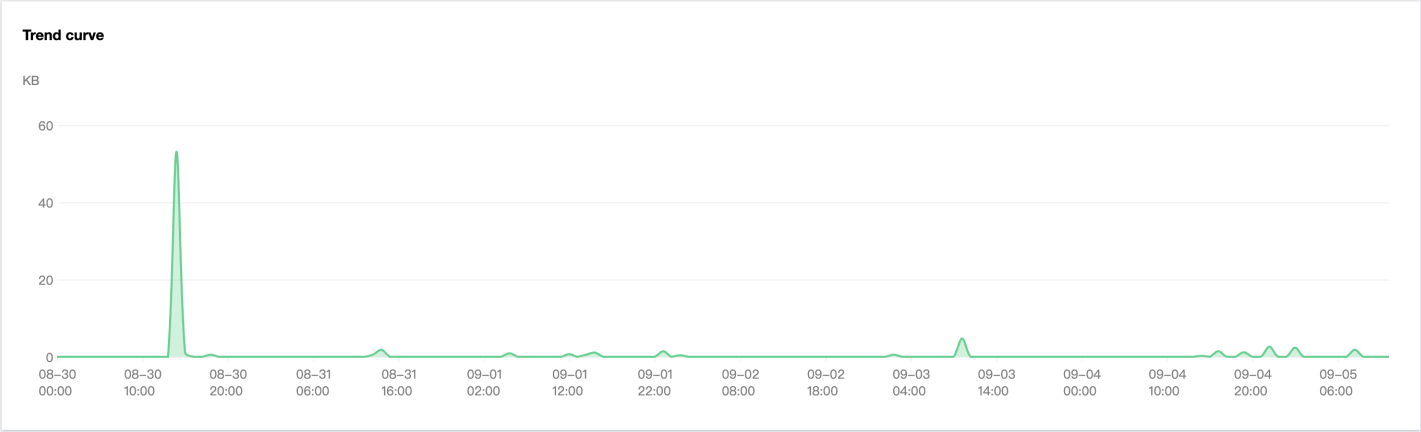
- Filter condition: Click **Add filter** to add the following filters: Host, URL, resource type and cache status.

Field description:

- Host: Subdomain name under the site.
- URL: URL to request resources, such as "/content".
- Resource type: Type of resources to request, such as PNG.
- Cache status: Cache status of a request.
  - Hit: A request hit the cache on EdgeOne nodes, indicating that the requested resources are provided by EdgeOne nodes.
  - Miss: A request missed the cache on EdgeOne nodes, indicating that the requested resources are provided by the origin server.
  - Dynamic: A request for resources not eligible or not configured for node caching, indicating that the requested resources are provided by the origin server.

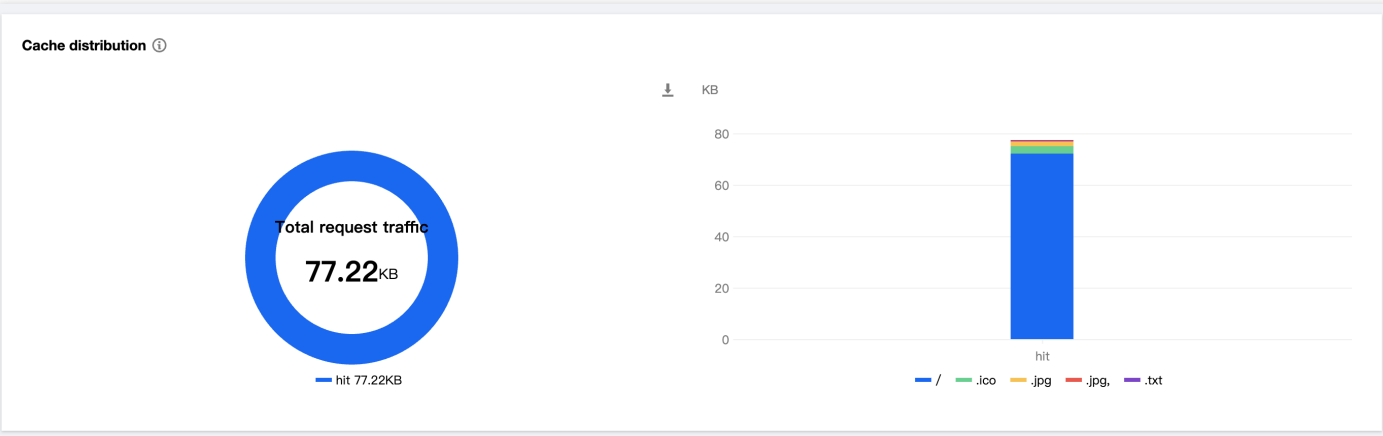
### Statistics overview

The trend curve for the specified time period is displayed by the set filters and metrics.



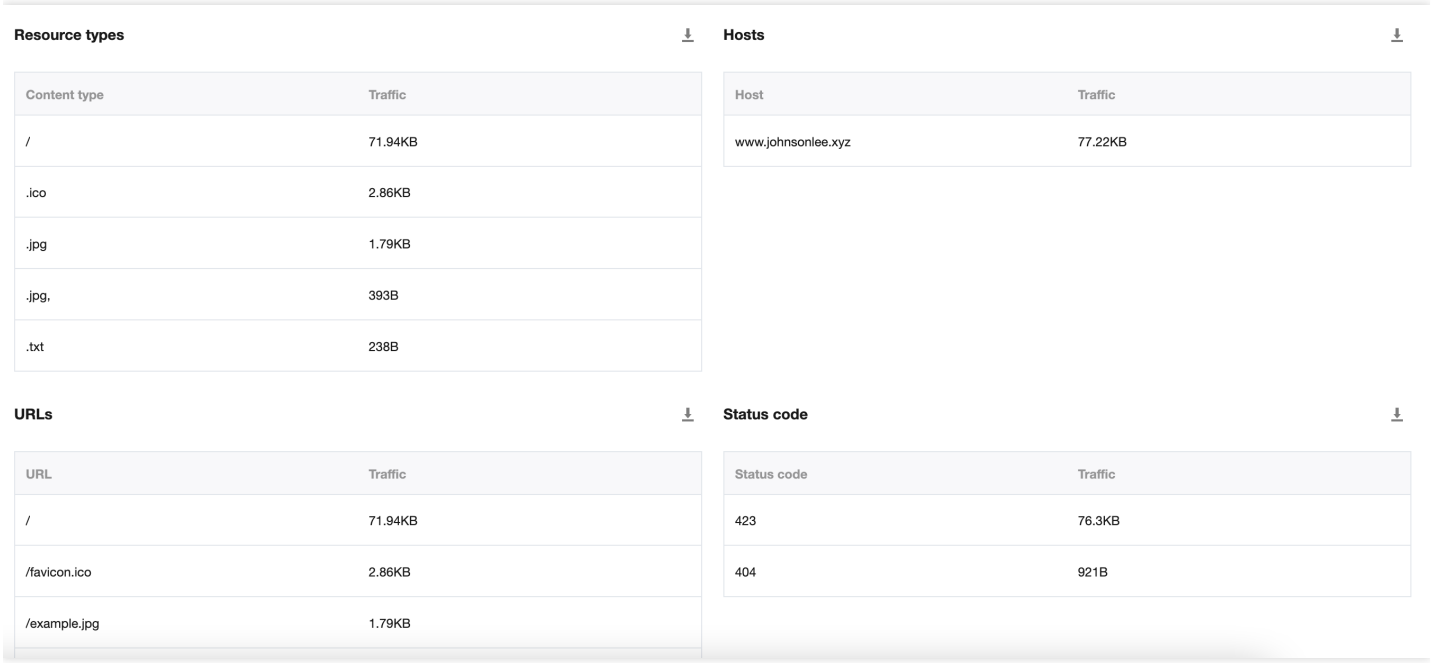

## Cache distribution

Types of requested resources and traffic usage are displayed based on the cache status of the requests for a specified time period.




## Data ranking

The top 5 and top 10 hosts (subdomain names), client IPs, URLs, Referers, resource types (available soon), and client device types are displayed by the selected filters. You can download the complete statistics to view more details for business analysis. You can also view the specific logs to get more data.



**Resource types**

| Content type | Traffic |
| --- | --- |
| / | 71.94KB |
| .ico | 2.86KB |
| .jpg | 1.79KB |
| .jpg, | 393B |
| .txt | 238B |

**Hosts**

| Host | Traffic |
| --- | --- |
| www.johnsonlee.xyz | 77.22KB |

**URLs**

| URL | Traffic |
| --- | --- |
| / | 71.94KB |
| /favicon.ico | 2.86KB |
| /example.jpg | 1.79KB |

**Status code**

| Status code | Traffic |
| --- | --- |
| 423 | 76.3KB |
| 404 | 921B |

### Field description:

- Resource types: File extensions of the requested resources.
- Hosts: Subdomain names under the site.
- URLs: Resource URLs that the client accesses.

# Log Service
# Real-time Logs

Last updated：2023-01-09 16:15:44

## Overview

EdgeOne provides the real-time logging feature to collect and ship access logs in real time, allowing for fast retrieval and analysis of log data.

## Use Cases

You can access log data to view or analyze business conditions in multiple dimensions in real time.

## Prerequisites

Activate CLS and grant EdgeOne access to create logsets.

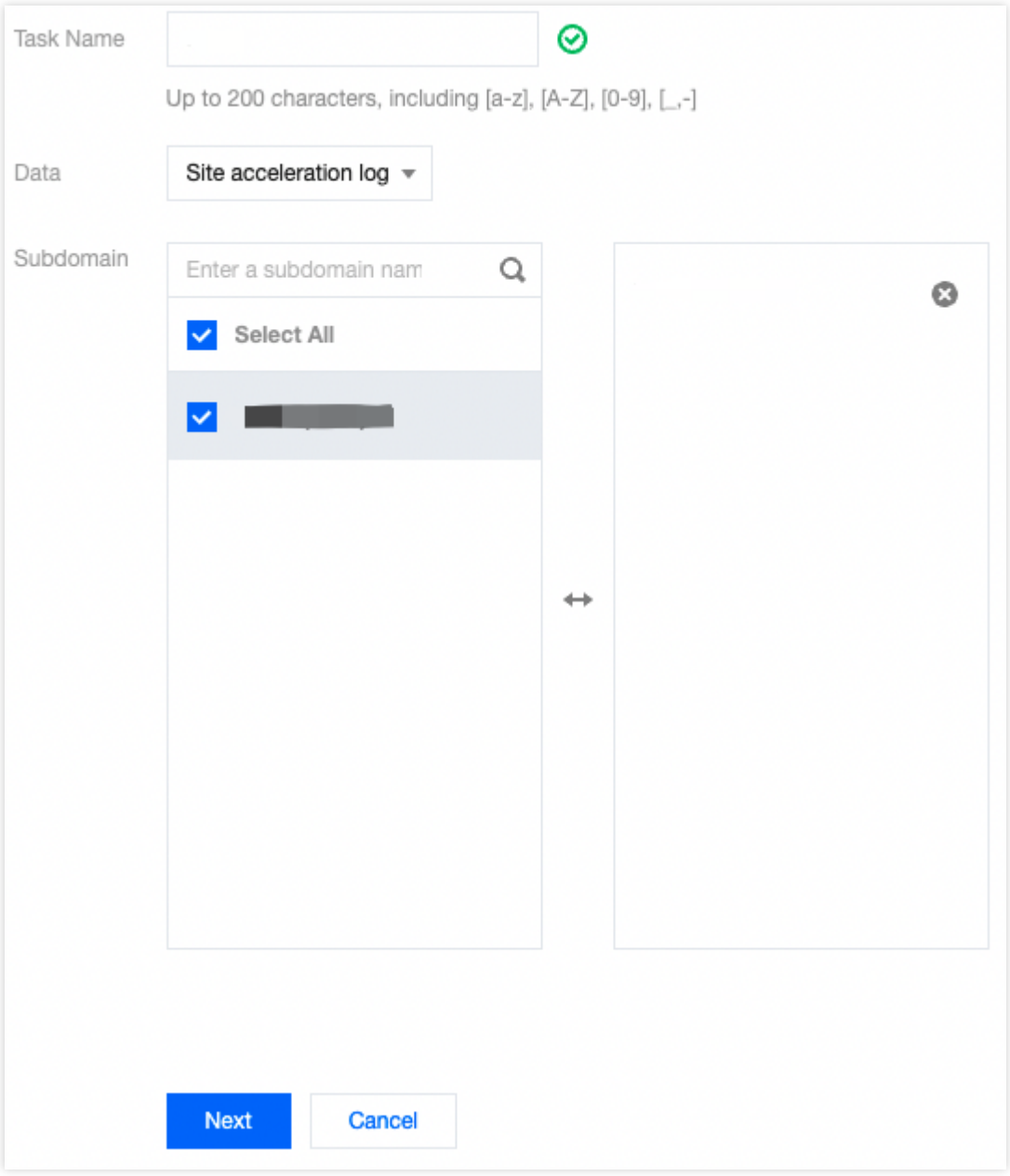
> Note：
> It's recommended to enable real-time logging by using a root account. If you are a sub-account or collaborator, you need to obtain the required permission.

## Creating a Push Task

1. Log in to the EdgeOne console. Click **Log Service** > **Real-time Logs** on the left sidebar.
2. On the **Real-time Logs** page, select the target site and click **Create push task**.

> Note：
> Real-time logs can only be shipped to CLS for now.

3. On the **Create push task** page, enter the task name, select the data to ship and the target subdomain under the current site, and click **Next**.

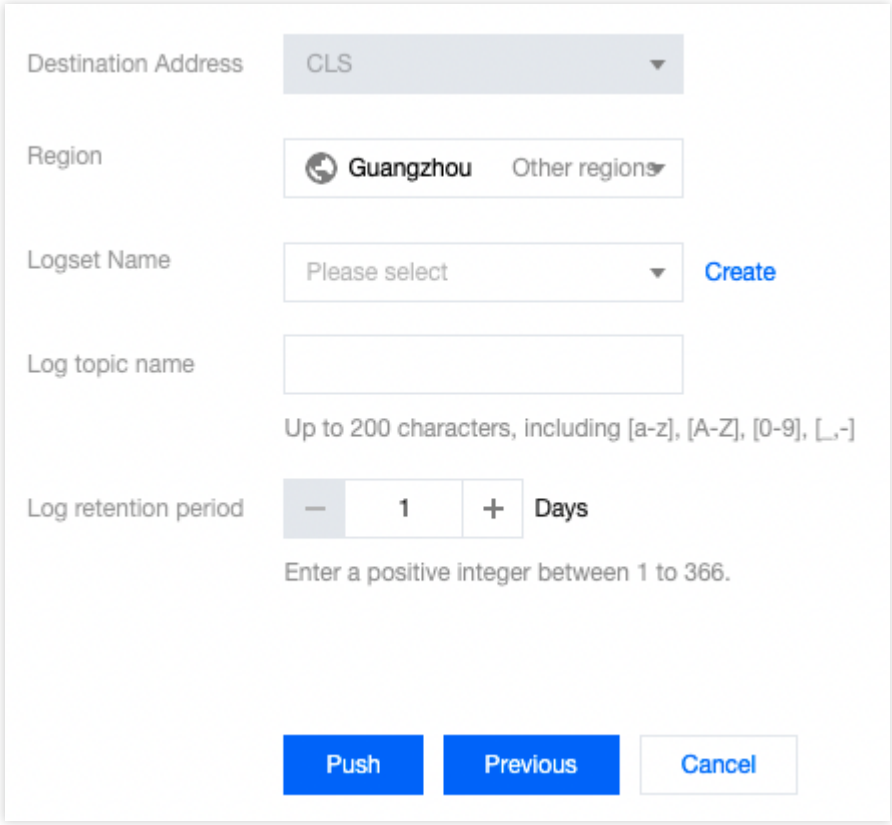



**Parameter description:**

- **Task name**: 1 to 200 characters, including `a-z, A-Z, 0-9, _, -` .
- **Data**: For now, only site acceleration data can be shipped.
- **Subdomain**: Subdomain of which you want to ship the logs. It must be under the current site.

> Note：
> You need to add all subdomain names in to one push task.

4. Configure the parameters below and click **Push**.




**Parameter description:**

- **Target address**: Only **CLS** is supported.
- **Region**: Select the destination region.
- **Target logset name**: Select a logset in the destination region.

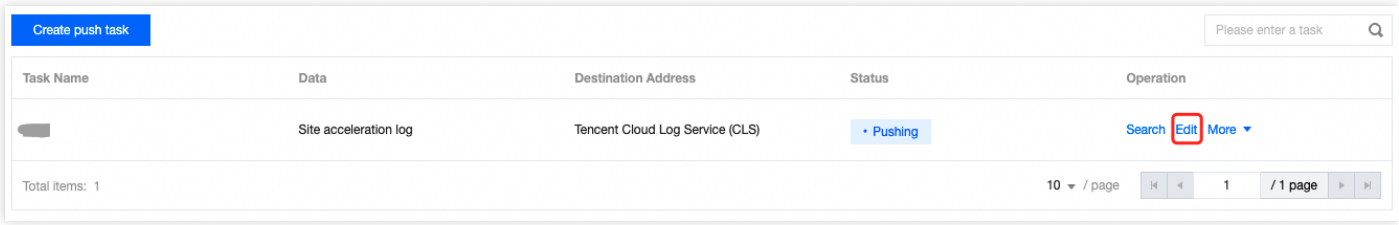
> Note：
> Click **Create** to create a logset in the selected region if necessary.

- **Log topic name**: 1 to 200 characters, including `a-z, A-Z, 0-9, _, -`.
- **Log retention period**: Enter a positive integer between 1 and 366.

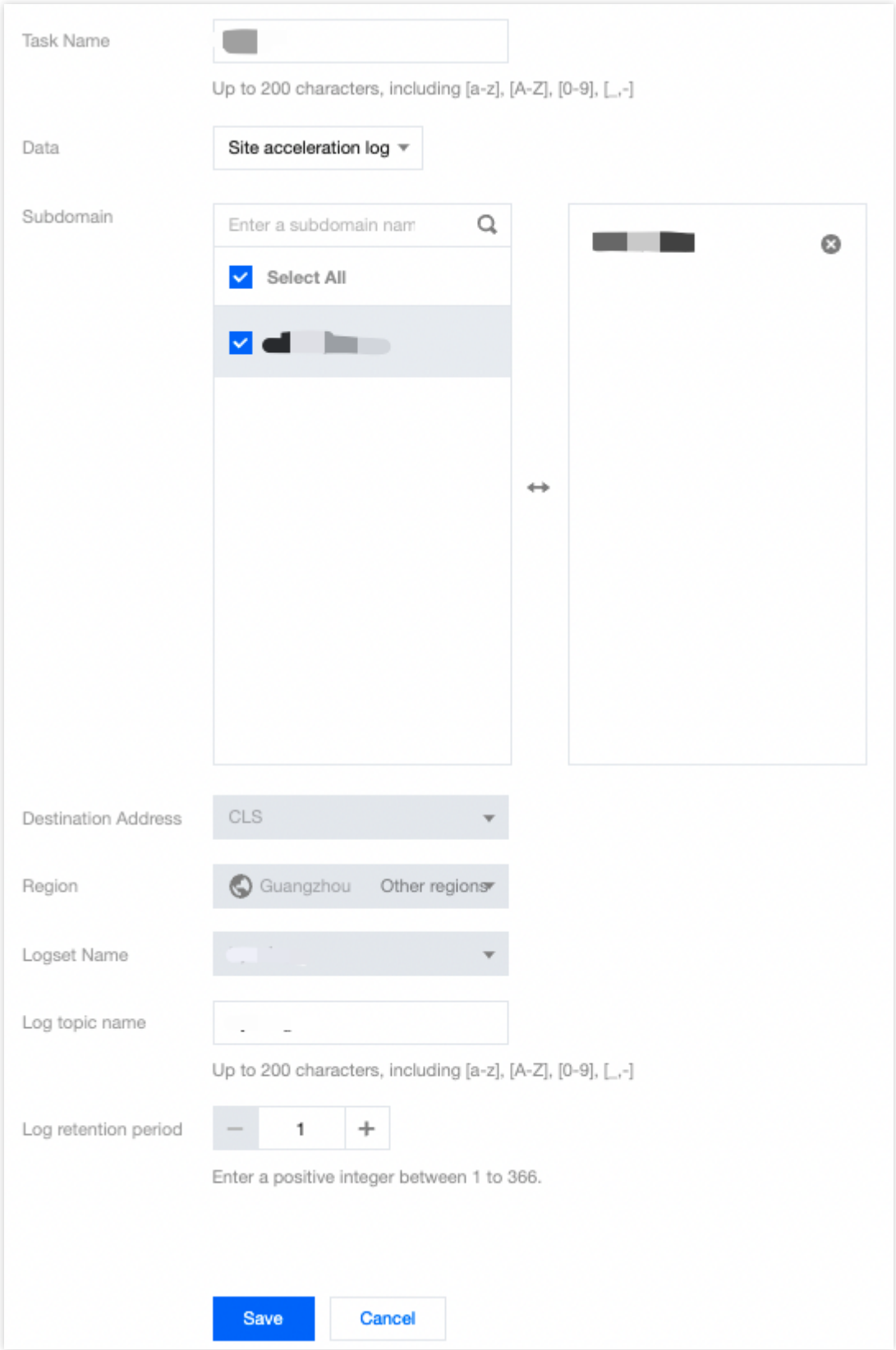
# Managing Push Tasks

**Editing push task**

1. On the Real-time Logs page, select the push task and click **Edit** in the **Operation** column.



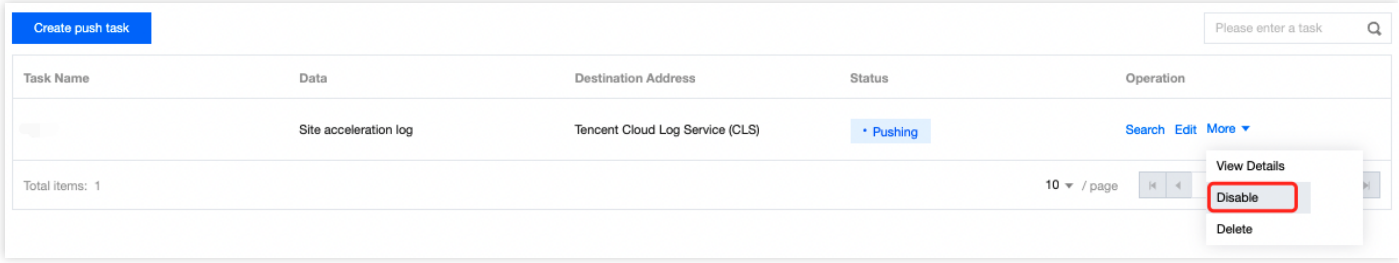

2. On the **Edit task** page, modify the task name, subdomains, push data, log topic name, and log retention time. Then, click **Save**.




### Disabling push task

You can suspend a log push task to stop shipping logs to the specified log topic.

1. On the Real-time Logs page, select the push task and click **More** > **Disable** in the **Operation** column.

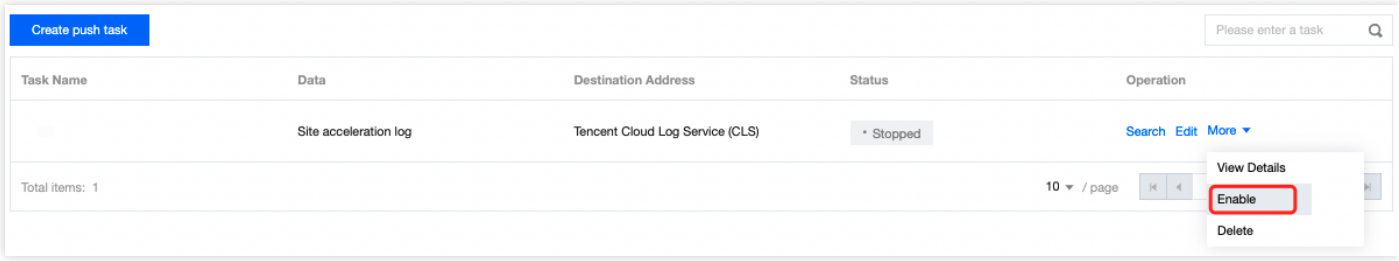



2. Once the push task is disabled, its subdomain logs will stop being shipped to the specified log topic, but shipped logs will be retained.

### Enabling a push task

You can enable a log push task to ship logs to the specified log topic.

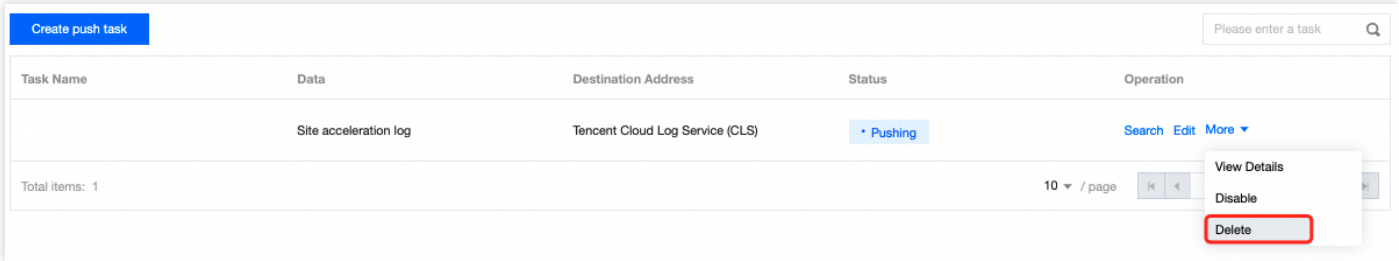
1. On the Real-time Logs page, select the target push task and click **More** > **Enable** in the **Operation** column.




2. Once the push task is enabled, its subdomain logs will be shipped to the specified log topic.

### Deleting a push task

1. On the Real-time log page, select the target push task and click **More** > **Delete** in the **Operation** column.

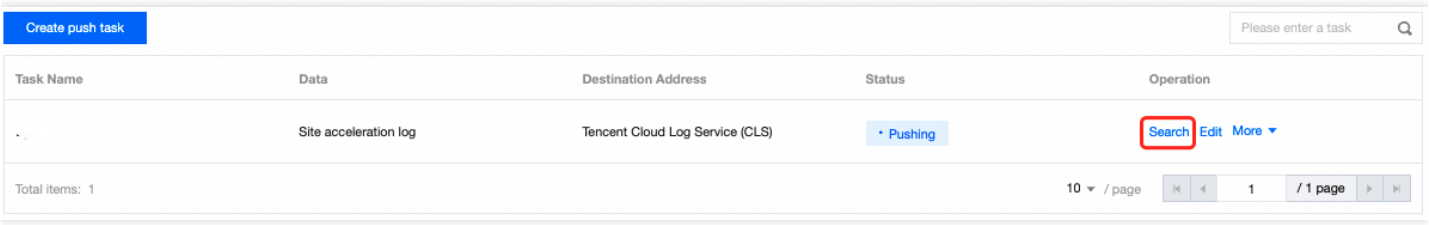



2. Once the push task is deleted, its subdomain logs will stop being shipped to the specified log topic, its log topic will be deleted, and all shipped logs will be cleared.

# Log Search

Log search supports various search and analysis methods and chart types. For more information, see Cloud Log Service.

EdgeOne logs can be searched for by push task. On the Real-time logs page, select the target push task and click **Search** to enter the log search page.




For more logset managing operations, such as renaming a logset, you can go to the CLS console.

# Glossary

### Logset

A logset is a project management unit in CLS. It is used to distinguish between logs of different projects and corresponds to a set. An EdgeOne logset has the following basic attributes:

- Region: The region to which a logset belongs.
- Logset name: The name of a logset.
- Retention period: The retention period of data in the current logset.
- Creation time: Logset creation time.

### Log topics

A log topic is the basic management unit in the Tencent Cloud log service (CLS). One logset can contain multiple log topics, and one log topic corresponds to one type of application or service. We recommend you collect similar logs on different machines into the same log topic. For example, if a business project has three types of logs: operation log, application log, and access log, you can create a log topic for each type of log.

The log service system manages different log data based on different log topics. Each log topic can be configured with different data sources, index rules, and shipping rules. Therefore, a log topic is the basic unit for configuring and managing log data in the log service. You need to configure corresponding rules first after creating a log topic before you can perform log collection, search, analysis, and shipping.

Log topic features include:

- Collect logs to log topics.
- Store and manage logs based on log topics.
- Search and analyze logs by log topics.

- Ship logs to other platforms based on log topics.
- Download and consume logs from log topics.

Note：

- For more information, see CLS documentation.
- Each real-time log push task ships logs of the selected subdomains to the corresponding log topic in CLS.

## Real-time Log Fields

| Field | Type | Description |
| --- | --- | --- |
| RequestID | String | Unique ID of the client request |
| ClientIP | String | Client IP |
| ClientCountry | string | The two-digit country code (ISO 3166-2) of the client location. |
| RequestTime | int | Client request time (a UNIX timestamp in seconds) |
| RequestHost | string | Client request host |
| RequestBytes | int | Client request size, which includes the size of the file itself and request headers |
| RequestMethod | string | HTTP client request method |
| RequestUrl | string | Client request URL |
| RequestUrlQueryString | string | A query string that is carried in the client request URL |
| RequestUA | string | Client request User-Agent |
| RequestRange | string | Client request Range |
| RequestReferer | string | Client request Referer |
| RequestProtocol | string | Client request HTTP protocol: HTTP, HTTPS, and HTTP/3 |
| RemotePort | int | Port connecting the client and nodes under the TCP protocol. This field will be "-" if the port does not exist. |

| Field | Type | Description |
| --- | --- | --- |
| EdgeCacheStatus | string | Whether the client request hits the node cache: HIT, MISS, and Dynamic |
| EdgeResponseStatusCode | int | Response status code returned to the client by the nodes |
| EdgeResponseBytes | int | Response size returned to the client by the nodes |
| EdgeResponseTime | int | The period from the point when the request is initiated from the client and the point when the client receives response from the server |

# FAQs

**Some of the CLS log topics are not visible in the EdgeOne console.**

In the EdgeOne console, you can only see log topics created by using the EdgeOne role.

**I cannot retrieve the data I want in the real-time logs. Are they lost?**

It may be because your log data volume is large, but the corresponding log topic has only a single partition, or automatic splitting is disabled for it. When you create a log topic, the default number of partitions is 1, and automatic splitting is enabled by default.

We recommend you estimate the number of required partitions based on your log volume and configure it in the advanced options in the CLS console. For more information, see Topic Partition.

**Can I delete CLS logsets?**

Yes. You can delete the logsets in the CLS console. Note that to delete a logset, you need to delete all its log topics first. The deletion will be synced to EdgeOne.

# Offline Logs

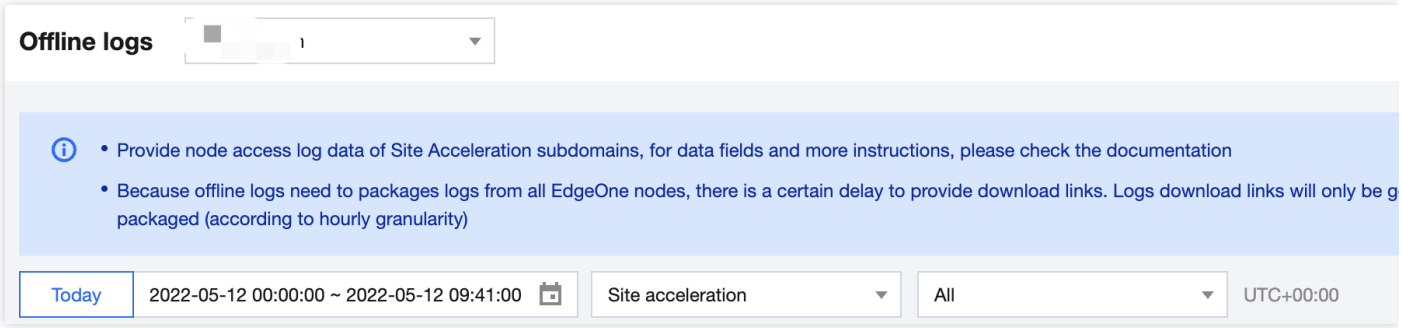
Last updated：2023-01-09 18:05:29

## Description

Access logs are collected at an hourly granularity, which can be downloaded within the default retention period of 30 days.

## Directions

1. Log in to the EdgeOne console. Click **Log Service** > **Offline Logs** on the left sidebar.
2. On the page that displays, select a site or the log file of a subdomain name. You can also filter logs by time.




Note

- The access logs are collected every hour by default. If the selected domain name is not requested during one hour, no logs will be generated for this hour.
- The access logs are compressed by gzip and marked with a .gz extension. Due to defects of the MacOS directory system, the .gz file may failed to be decompressed on MacOS by double-clicking it. In this case, you can run the following Terminal commands:

```
gunzip {your_file_name}.log.gz
```

- EdgeOne nodes are distributed over the globe. To synchronize the time across time zones, logs are stored and queried in UTC+00:00 by default.
- It normally takes around 30 minutes to generate log data as it is collected from all EdgeOne nodes. The log data will be complete within 24 hours after being generated.

# Field Description

Logs are stored in JSON format by default. The log fields are described as follows:
When a field is not specified:

- For a string field, the field value is set to `-` if the field has no data.
- For an integer field, the field value is set to `-1` if the field has no data.

### Site acceleration logs

| Name | Data Type | Description |
| --- | --- | --- |
| RequestID | String | Unique ID of the client request |
| ClientIP | String | The client IP |
| ClientRegion | Sting | Country/Region of the client IP. Format: ISO-3166-2 |
| RequestTime | int | The time that the client initiates a request, which is recored in UTC +00:00 and defined in the ISO-8601 standard. |
| RequestStatus | int | Status of the client request. Values: `0` (not completed), `1` (completed successfully), `2` (completed abnormally) |
| RequestHost | String | Host of the client request |
| RequestBytes | int | Size of the client request, in bytes |
| RequestMethod | String | The HTTP method used by the client |
| RequestUrl | String | The URL for the client request |
| RequestUrlQueryString | String | The query string contained in the request URL |
| RequestUA | String | The User-Agent sent by the client |
| RequestRange | String | The Range parameter sent by the client |
| RequestReferer | String | The Referer parameter sent by the client |
| RequestProtocol | String | The application layer protocol used by the client. Values: `HTTP/1.0`, `HTTP/1.1`, `HTTP/2.0`, `HTTP/3`, `WebSocket` |
| RemotePort | int | The port that connects the client and node over the TCP protocol. Note that a hyphen (-) is used if this port does not exist. |

| Name | Data Type | Description |
| --- | --- | --- |
| EdgeCacheStatus | String | Whether the client request results in a cache hit. Values: `HIT` (resources are served by the node cache), `MISS` (resources are served by the origin and can be cached), `Dynamic` (resources cannot be cached) |
| EdgeResponseStatusCode | int | The status code that the node returns to the client |
| EdgeResponseBytes | int | Size of the response that the node returns to the client, in bytes |
| EdgeResponseTime | int | The amount of time elapsed between EdgeOne receiving a request from the client and waiting till the client receives the response from the server side. Unit: ms |
| EdgeInternalTime | int | The amount of time elapsed between EdgeOne sending a request to the origin and receiving the first byte of the response from the origin. Unit: ms |
| EdgeServerIP | String | IP address of the EdgeOne server, which can be resolved from the host using DNS. |
| EdgeServerID | String | The unique ID that identifies the EdgeOne server accessed by the client |
| SecurityAction | String | The rule action. Values: `Monitor` (observe), `JSChallenge` (JavaScript challenge), `Deny` (block), `Allow` (allow), `BlockIP` (block the IP), `Redirect` (redirect), `ReturnCustomPage` (return the custom page), `ManagedChallenge` (implement the managed challenge) |
| SecurityRuleID | String | ID of the security rule used |
| SecurityUserNote | String | The tag defined by the user |
| SecurityModule | String | Security feature of the hit security rule. Values: `CustomRule` (custom rules), `BotManagement` (bot management), `RateLimiting` (preset rate limiting rules), `RateLimitingCustomRule` (custom rate limiting rules), `ManagedRule` (managed rules), `BotClientReputation` (client reputation), `BotBehaviorAnalysis` (bot intelligence), `RateLimitingClientFiltering` (client filtering) |

### L4 proxy logs

| Name | Data Type | Description |
| --- | --- | --- |

| Name | Data Type | Description |
| --- | --- | --- |
| ServiceID | String | Unique ID of the L4 proxy service |
| ConnectTimeStamp | String | The time that the connection is established, which is recorded in UTC +0 and defined in the ISO-8601 standard. |
| DisconnetTimeStamp | String | The time that the connection disconnects, which is recorded in UTC +0 and defined in the ISO-8601 standard. |
| DisconnetReason | String | The disconnection reason.<br>• Format: Direction: Reason<br>• Values of the Direction parameter: `up` (data flows from the client to the origin), `down` (data flows from the origin to the client)<br>• Values of the Reason parameter:<br>◦ `net_exception_peer_error`: The peer returned an error during a read/write attempt.<br>◦ `net_exception_peer_close`: The peer closed the connection.<br>◦ `create_peer_channel_exception: Failed to create a channel to the next hop.<br>◦ `channel_eof_exception`: The channel ended. Once this happens, the error message is sent from the node that ends the request to the adjacent node.<br>◦ `net_exception_closed`: The connection is closed.<br>◦ `net_exception_timeout`: Read/Write timed out. |
| ClientRealIP | String | The real client IP |
| ClientRegion | String | The 2-digit code that identifies the country/region of the client, which is defined in the ISO-3166-2 standard. |
| EdgeIP | String | IP address of the EdgeOne server accessed |
| ForwardProtocol | String | The TCP/UDP forwarding protocol configured by the client |
| ForwardPort | Int | The forwarding port configured by the client |
| SentBytes | Int | Inbound traffic produced when the log is generated, in bytes |
| ReceivedBytes | Int | Outbound traffic produced when the log is generated, in bytes |
| LogTimeStamp | Int or String | The time that the log is generated, which is recorded in UTC +0 and defined in the ISO-8601 standard. |

# Notes

- The traffic/bandwidth data (in bytes) recorded in the access log field "EdgeResponseBytes" may be different from the actual billing data for the following reasons:
  - Only application-layer data can be recorded in access logs. During actual data transfer, the traffic generated over the network is around 5-15% more than the application-layer traffic, including the following two parts:
    - Consumption by TCP/IP headers: in TCP/IP-based HTTP requests, each packet has a maximum size of 1,500 bytes and includes TCP and IP headers of 40-60 bytes, which generate traffic during transfer but cannot be counted by the application layer. The overhead of this part is around 3-4%.
    - TCP retransmission: during normal data transfer over the network, around 3% to 10% of packets are lost on the Internet and retransmitted by the server. This type of traffic, which accounts for 3-7% of the total traffic, cannot be counted at the application layer.
- When smart acceleration is enabled, the traffic/bandwidth generated when the client sends a request to the EdgeOne node incurs charges. For more details, see Billing Overview.

# Domain Service
# NS Connection

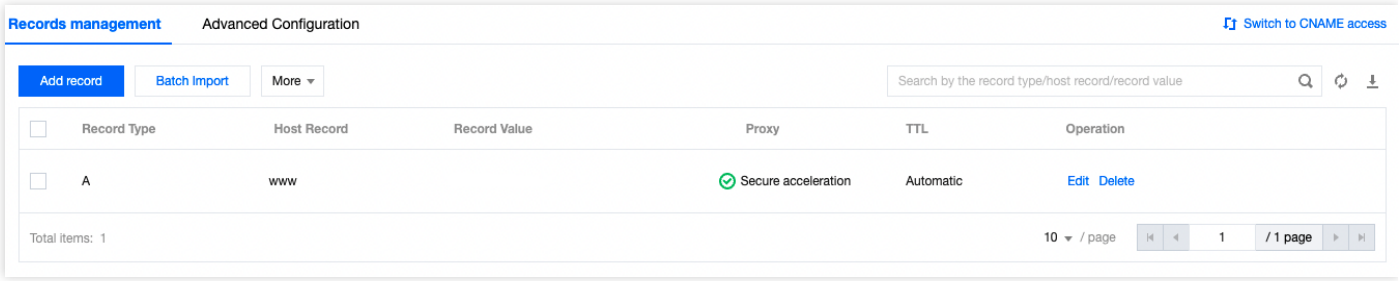
Last updated：2022-11-16 10:46:40

With the NS connection method, you can modify the NS to transfer your site's DNS resolution permission to EdgeOne. This quickly enables the EdgeOne security/acceleration services while implementing a stable and professional DNS service.

## NS Record

EdgeOne DNS supports the smart DNS service for various record types to intelligently return the optimal split zone based on end users' geographical locations and ISPs.

1. Log in to the EdgeOne console and click **Domain Name Service** on the left sidebar.
2. On the page that appears, select the target site and click **DNS records**.
3. On the page you enter, select the target record, click **Edit** to edit the parameters, and click **Save**.




**Parameter description:**

- Record type and value: Different record types have different purposes.

| Record Type | Sample Record Value | Usage Description |
| --- | --- | --- |
| A | 8.8.8.8 | It points a domain name to a public network IPv4 address such as `8.8.8.8`. |
| AAAA | 2400:cb00:2049:1::a29f:f9 | It points a domain name to a public network IPv6 address. |
| CNAME | cname.edgeone.com | It points a domain name to another domain, from which the final IP address will be resolved. |

| Record Type | Sample Record Value | Usage Description |
| --- | --- | --- |
| MX | 10 mail.edgeone.com | It is used for email servers. The record value and priority parameters are provided by email service providers. If there are multiple MX records, the lower the priority value, the higher the priority. |
| TXT | ba21a62exxxxxxxxxxcf5f06e | It identifies and describes a domain name and is usually used for domain verification and as SPF records (for anti-spam). |
| NS | ns01.edgeone.com | If you need to authorize a subdomain name to another DNS service provider for DNS resolution, you need to add an NS record. You cannot add an NS record for a root domain name. |
| SRV | 1 5 7001 srvhostname.example.com | It identifies a service used by a server and is commonly used in Microsoft directory management. |
| CAA | 0 issue trustasia.com | It specifies CAs to issue certificates for sites. |

Note：
For an A, AAAA, or CNAME record, if proxy acceleration or secure acceleration is enabled, the record value will be the origin server address for eventual origin-pull after proxy.

- Host record: It is equivalent to the prefix of a subdomain. If the root domain of the current site is `edgeone.com`, then common host records are as listed below:

| Record Type | A | AAAA | CNAME | MX | NS | TXT | SRV | CAA |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | ✓ |
| AAAA | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | ✓ |
| CNAME | × | × | × | × | × | × | × | × |
| MX | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | ✓ |
| NS | × | × | × | × | ✓ | × | × | × |
| TXT | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | ✓ |
| SRV | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | ✓ |

| Record Type | A | AAAA | CNAME | MX | NS | TXT | SRV | CAA |
|---|---|---|---|---|---|---|---|---|
| CAA | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | ✓ |

- Proxy mode: Select **Only DNS** or **Enable proxy** based on the record type.

| Record Type | Proxy Mode |
|---|---|
| A/AAAA/CNAME | Support both **Only DNS** and **Enable proxy**. |
| MX/TXT/NS/SRV/CAA | Only support **Only DNS**. |

Note：

- In the case that there are multiple DNS records contain the same host record (the same subdomain prefix), if the proxy is enabled for only one record, the other records will be invalid.
- When multiple DNS records contain the same host record (i.e., the same subdomain prefix): Proxy can be enabled for multiple A/AAAA records at the same time, but for only one CNAME record.

- TTL: It is the DNS record cache time. Generally, the shorter the TTL, the shorter the cache time, and the faster the record value will take effect when it is updated, but the DNS speed will be slightly affected.
  - Available TTL values include: Automatic, 1 minute, 2 minutes, 5 minutes, 10 minutes, 15 minutes, 30 minutes, 1 hour, 2 hours, 5 hours, 12 hours, and 1 day. If you select **Automatic**, the system will configure TTL to 300 seconds.
  - How to configure TTL:
    - If the record value changes infrequently, select one hour or longer to speed up DNS resolution.
    - If the record value changes frequently, select a shorter TTL value such as one minute, which, however, may slightly slow down DNS resolution.

Note：

- In proxy acceleration, the TTL is **Automatic** by default and cannot be modified.
- In actual conditions, TTL is not necessarily applied to LDNS cache configuration, which usually makes the time it takes for the record update to take effect much longer than the TTL.

# DNS Configuration

Advanced configuration items such as DNSSEC, custom NS, and CNAME acceleration are supported.

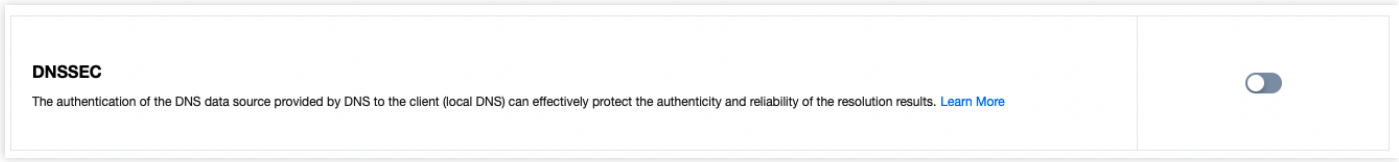
## DNSSEC

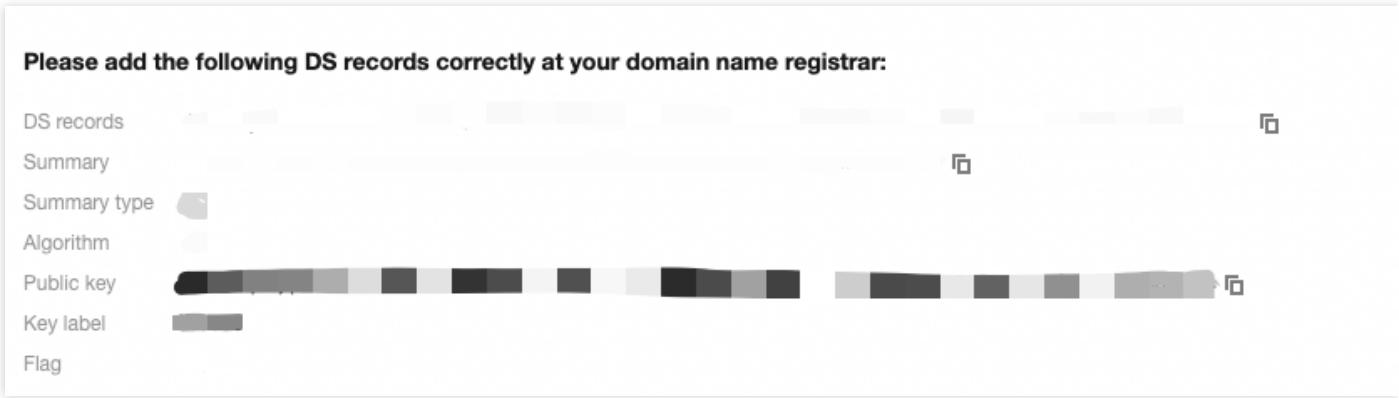
DNS Security Extension (DNSSEC) uses a digital signature to authenticate the DNS data source in order to effectively protect the security and integrity of DNS resolution results. It is commonly used to prevent DNS spoofing and DNS cache poisoning.

1. Log in to the EdgeOne console and click **Domain Name Service** on the left sidebar.

2. On the page that appears, select the target site and click **DNS configuration**.

3. On the DNS configuration page, click  in the DNSSEC module and confirm the operation. Then the DS information will be generated.




4. Add a DS record at your domain registrar according to the above information. For detailed directions with certain registrars, see the following documents:

- DNSimple
- GoDaddy
- Google Domains
- name.com
- Public Domain Registry

## Custom NS

The custom NS feature allows you to create a name server (NS) dedicated to your own site to replace the default assigned name server. After creation, EdgeOne will automatically assign an IP to it.

> Note：
> Custom NS has the following limits:
>
> - Only a subdomain (ns.example.com) of the current site (example.com) can be used as a custom NS.
> - You can add only two to five custom name servers.
> - If you enable custom NS for the first time, you need to add two custom name servers, and the custom names must be different from existing DNS records.

1. On the Domain Name Service page, select the target site and click **DNS configuration**.
2. On the DNS configuration page, click  in the custom NS module, enter a custom NS domain name, and click **Add**.
3. After adding a custom NS successfully, **you need to add its glue records at your domain registrar for it to take effect**.

## CNAME acceleration

Once enabled, CNAME acceleration can effectively accelerate DNS resolution. If multi-level CNAME records are set in EdgeOne DNS for a domain, the system will directly provide the final IP DNS resolution result to reduce the number of resolutions. This feature is enabled by default.

1. On the Domain Name Service page, select the target site and click **DNS configuration**.
2. On the DNS configuration page, you can toggle CNAME acceleration on or off.

> Note：
> To directly get the final IP DNS resolution result, all multi-level CNAME records must be in EdgeOne DNS.

# CNAME Access

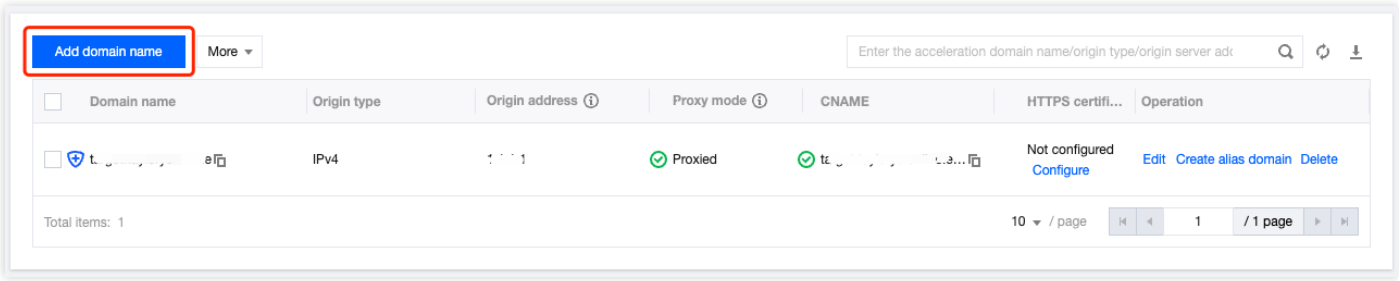
Last updated：2022-12-15 15:02:46

In CNAME access mode, you can connect your site to EdgeOne security/acceleration services simply by adding a record (subdomain name), enabling proxy, and adding the specified CNAME record at your DNS service provider. You don't need to transfer the DNS resolution permission to EdgeOne.

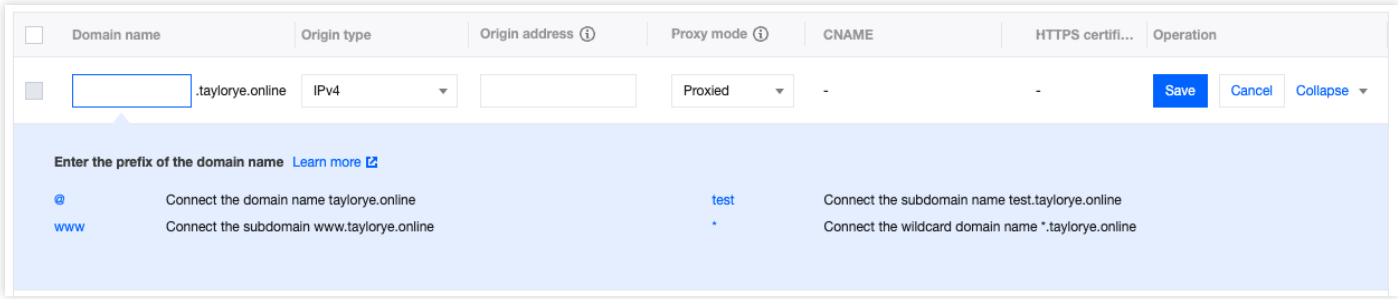
## Adding a record (connection via subdomain)

In CNAME access mode, you can add a record to connect site subdomain names to the corresponding service.

1. Log in to the EdgeOne console and click **Domain Name Service** on the left sidebar.
2. On the page that appears, select the target site and click **Add domain name**.




3. Enter the relevant parameters and click **Save**.




**Parameter description:**

- Acceleration domain name: Enter the subdomain name to be accelerated. Only the prefix of the subdomain name is required.
- Origin type: Select "IPv4", "IPv6", or "domain name" as needed.

- Origin address: Enter the origin address according to the origin type. Examples are given in the following table.

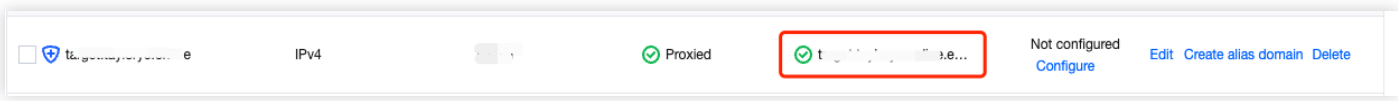
| Origin Type | Example of Origin Address | Usage Description |
| --- | --- | --- |
| IPv4 | 8.8.8.8 | Traffic is forwarded to an IPv4 origin server at `8.8.8.8`. |
| IPv6 | 2400:cb00:2049:1::a29f:f9 | Traffic is forwarded to an IPv6 origin server at `2400:cb00:2049:1::a29f:f9`.<br>EdgeOne supports dual-stack origin-pull by default. |
| Domain Name | www.origin.com | Traffic is forwarded to a domain origin server at `www.origin.com`. |

- Proxy mode: Set the proxy mode to **Proxied** or **Only DNS**. For more information, see Proxy Mode.

- CNAME: A CNAME record is generated when proxy is enabled. You need to add the CNAME record at your DNS service provider.

- HTTPS certificate: When CNAME access is used, EdgeOne does not provide a universal certificate. In this case, you need to associate each subdomain name with a certificate manually before you can use the HTTPS service normally.

4. After saving the record, EdgeOne will assign a CNAME record to your subdomain name. You need to configure the CNAME record at your DNS service provider before you can direct user access to EdgeOne nodes and make the acceleration take effect.
5. After the configuration, if a green icon appears in the CNAME column, the CNAME record has taken effect, and the subdomain name is accelerated.



# Traffic Scheduling Management

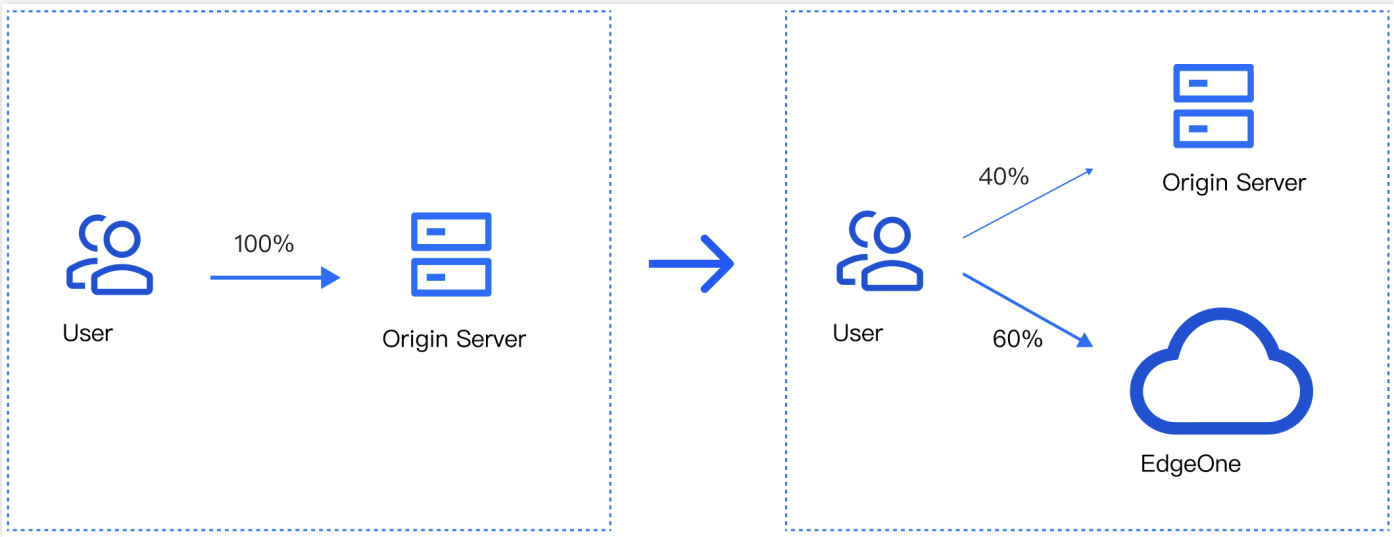
Last updated：2022-12-13 16:25:41

## Overview

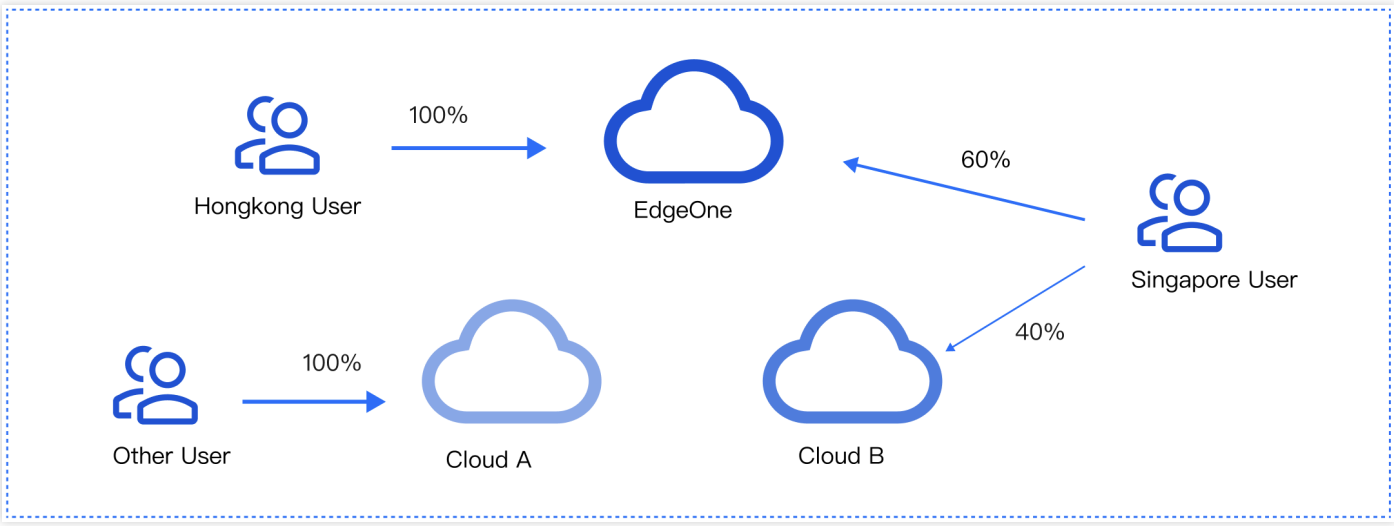
Traffic scheduling management is a multi-CDN smart resolution and scheduling tool provided by EdgeOne. It supports custom traffic scheduling policies between the origin server and service providers to implement smooth canary migration of traffic and flexible allocation of services, thereby ensuring a high service availability.

### Use Cases

- Canary migration: When a new service provider is added, canary switch is required to ensure the service availability and smooth migration.




- Multi-vendor scheduling: If businesses are large in scale and sensitive, traffic can be flexibly allocated to multiple vendors to spread risks and implement disaster recovery.




**Features**

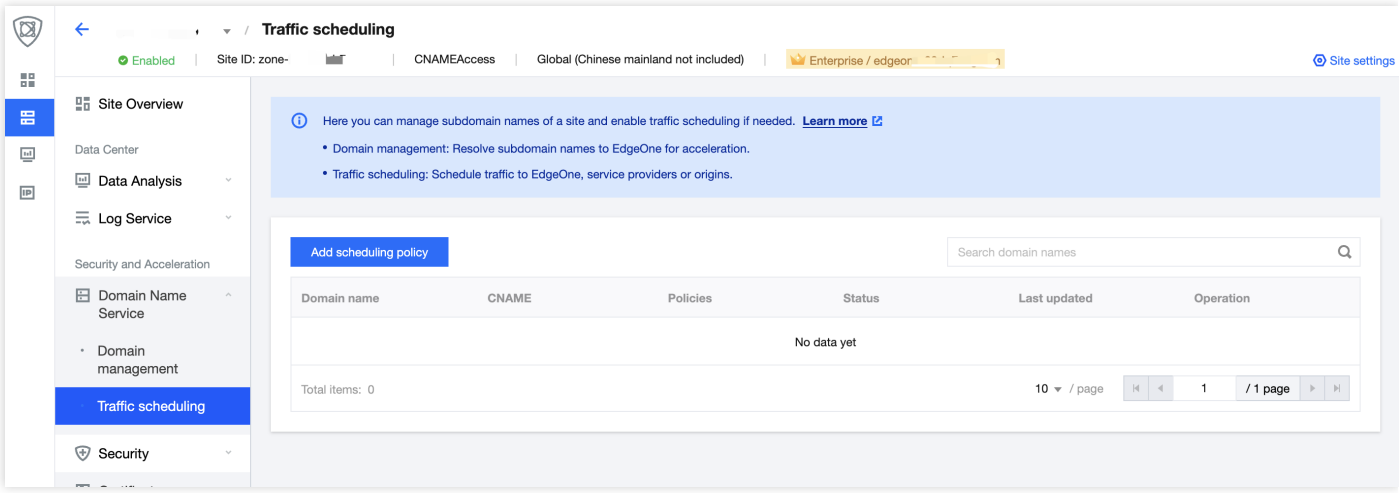
- Simple management: You can implement traffic scheduling management simply by selecting a domain name, adding a service provider, and adding a scheduling policy.
- Fast access: You can implement fast access only by adding the CNAME record allocated by EdgeOne at your DNS service provider.
- Multiple scheduling modes: Ratio-based and region-based scheduling modes are available to meet various requirements.
- Multiple scenarios: You can use either the origin server or services provided by other CDN vendors, implement canary switch, and use services from different vendors at the same time.

# Prerequisites

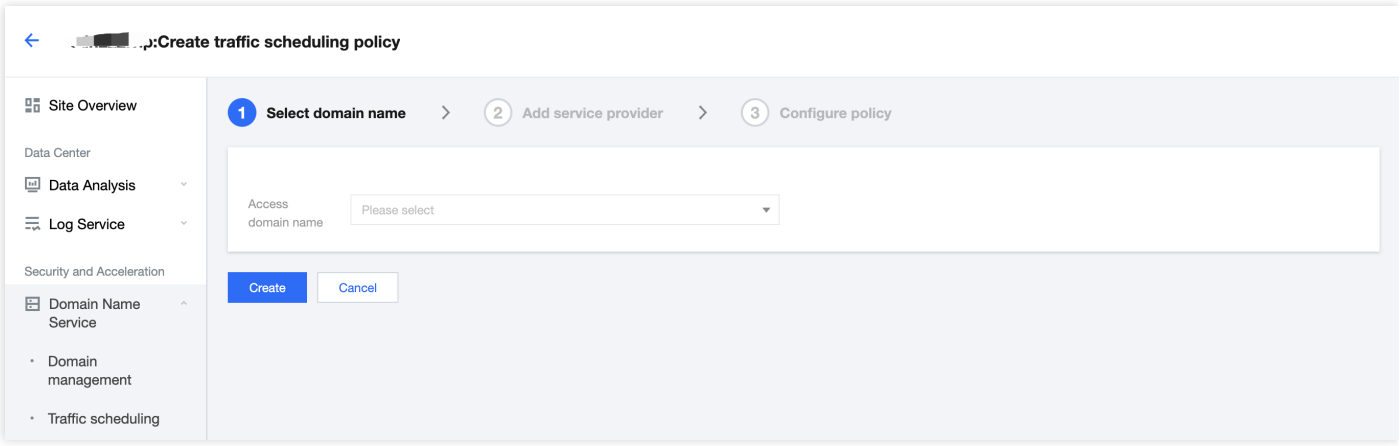
You have purchased the EdgeOne Enterprise plan and connected the site in CNAME access mode.

# Adding a Traffic Scheduling Policy

1. Log in to the EdgeOne console and click **Site** > **Domain Name Service** > **Traffic Scheduling Management**.

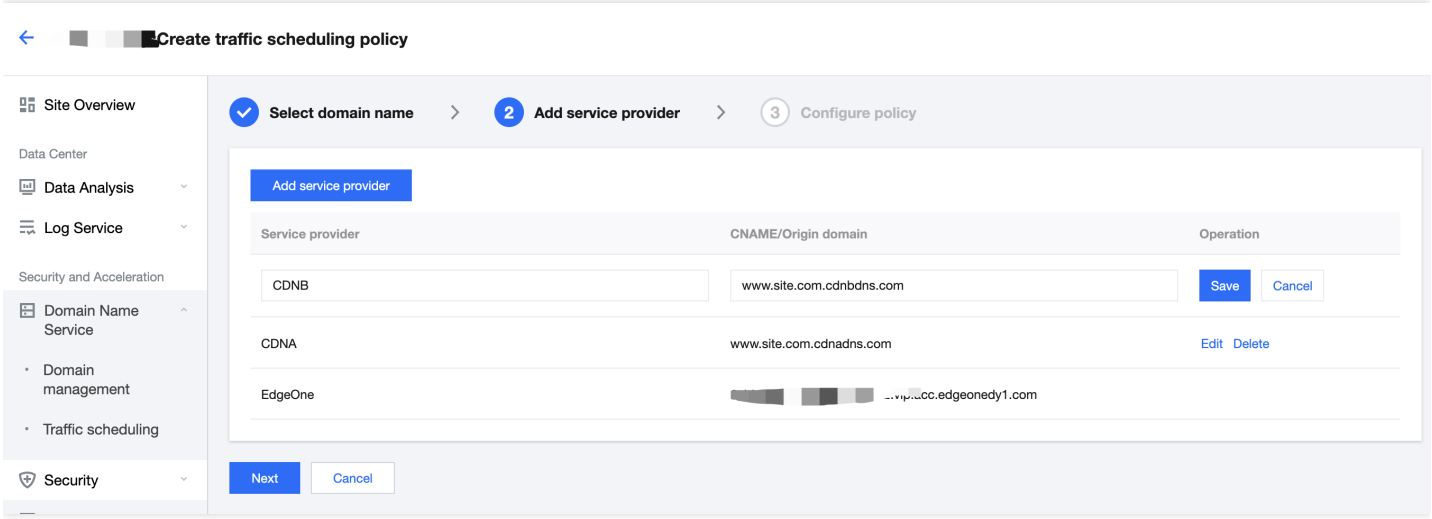



2. On the **Traffic Scheduling Management** tab, click **Add scheduling policy**, select the target domain name, and click **Create**.




3. Click **Add service provider**, configure parameters such as the service provider name and CNAME record as needed, and click **Next**.

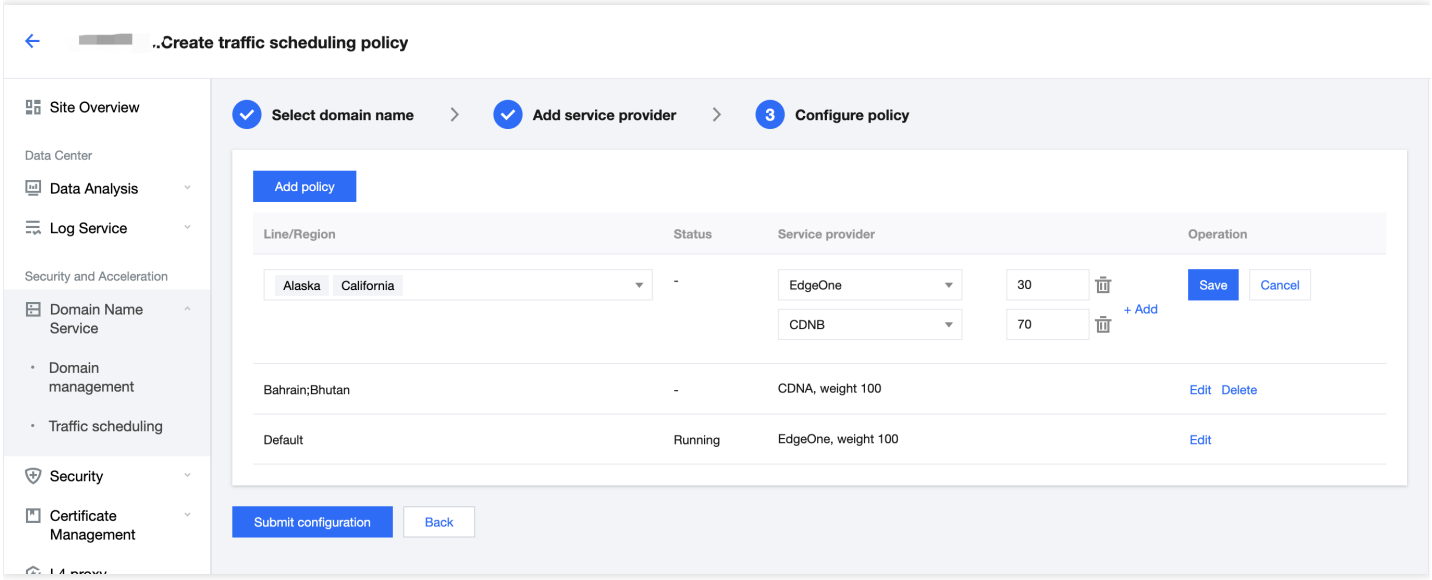
> Note：
> The default service provider is EdgeOne, which cannot be modified or deleted. You can add a domain name of the origin server or a CNAME domain name of another CDN service provider.



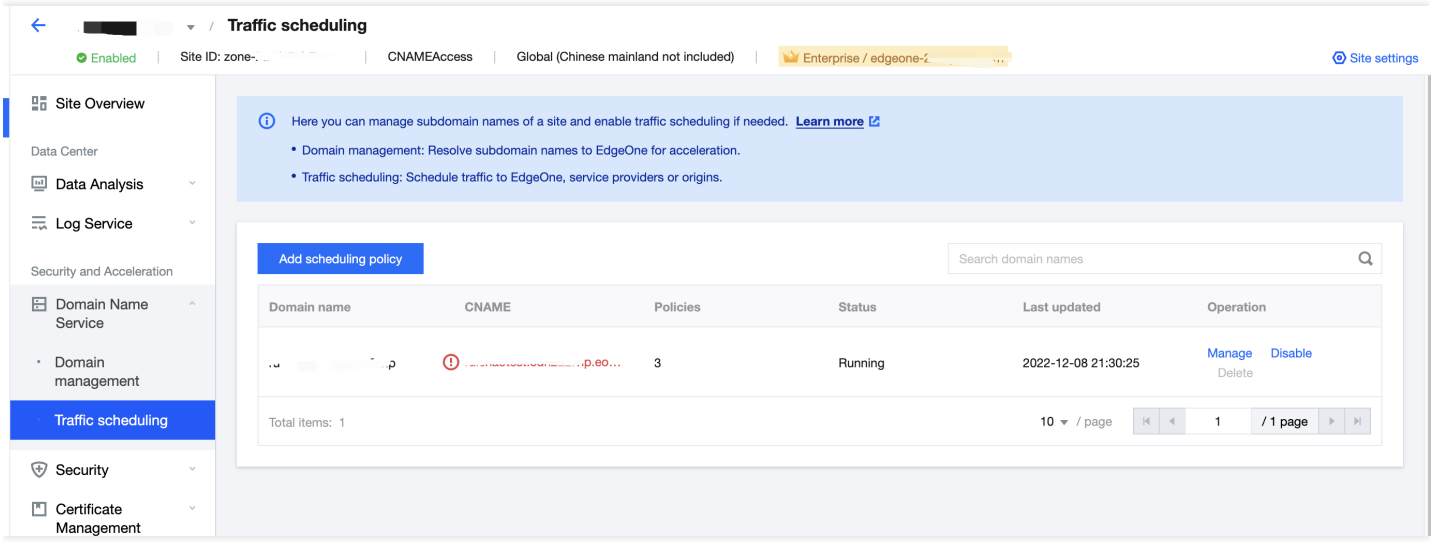

4. Click **Add policy**, select the split zone/region, configure the multi-service provider scheduling policy, and click **Submit configuration**. You can select multiple service providers and set their weights.

Note：

- By default, all traffic passes EdgeOne. This is the base policy, which cannot be deleted but can be changed to another service provider.
- Split zone/Region settings support countries/regions, ISPs and provinces in the Chinese mainland, and states in the US and India.
- Finer-grained regions/split zones have a higher priority. For example, if you select the origin server for Beijing, service provider A for the Chinese mainland, and service provider B for the default split zone, then traffic in Beijing region will pass the origin server, traffic in other regions in the Chinese mainland will pass service provider A, and overseas traffic will pass service provider B.




5. The traffic scheduling CNAME should be identical to the default domain name CNAME. After the policy is added, if the domain name resolution has been switched, no change is required, and the policy will take effect immediately in the production environment; otherwise, you need to switch the domain name resolution at your DNS service provider.




# Managing a Traffic Scheduling Policy

You can edit, disable, enable, and delete a policy on the **Domain Name Service** > **Traffic Scheduling Management** tab.

## Disabling a policy

Disabling a traffic scheduling policy will void it, and all traffic will be scheduled to EdgeOne.

### Enabling a policy

You can enable a disabled policy to resume traffic scheduling management, after which traffic will be scheduled as configured, rather than to EdgeOne.

### Deleting a policy

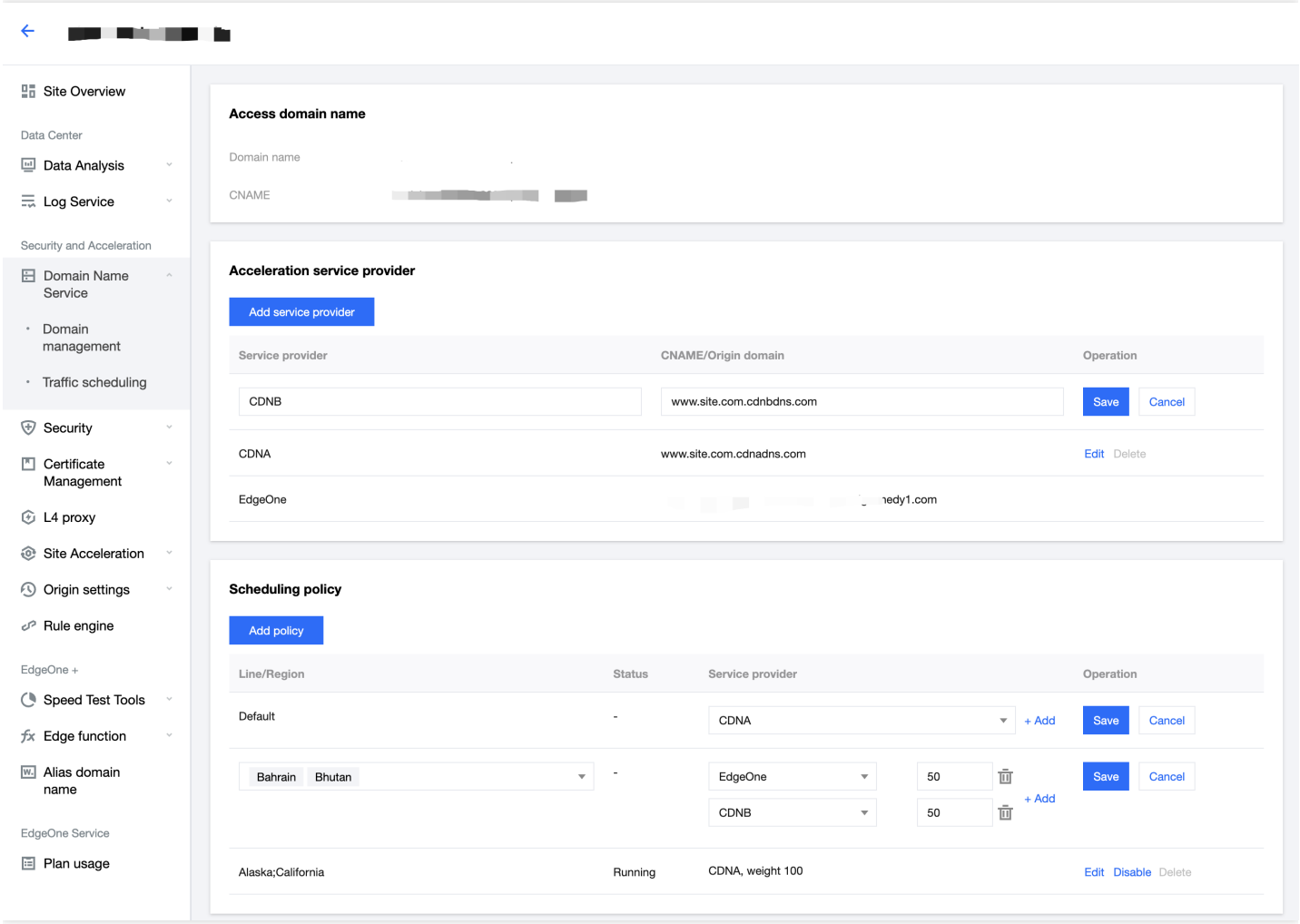
You can delete a disabled policy. This does not affect the service but cannot be recovered. Proceed with caution.

### Managing a policy

Click **Manage** to enter the **Scheduling Policy Management** page, where you can add, delete, modify, and disable a service provider and scheduling policy.

Note：

- Changing the service provider already referenced by a policy will take effect immediately.
- Deleting, modifying, enabling, and disabling a policy will take effect immediately.
- The service provider already referenced by a policy cannot be deleted.



# Security Protection
# Web Protection

Last updated：2022-08-01 11:44:52

## Feature Overview

### Overview

The web protection feature provides application layer protection for sites using the HTTP/HTTPS protocol. It also contains 500+ rules managed in the rules library and AI engine.

### Web/Bot action description

The web protection and bot protection features allows you to set actions based on your business scenarios. There are three actions available:

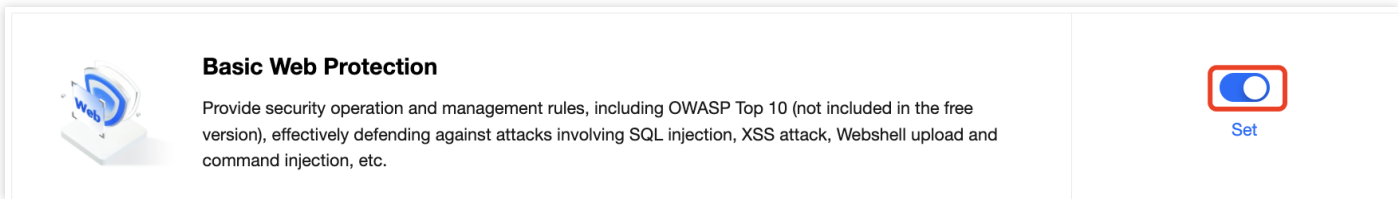
- Block: The traffic to forward will be blocked. Meanwhile, a block page will be returned and attacks will be recorded.
- Observe: The traffic will be observed, while attacks will be recorded.
- Allow: The traffic will be allowed, while attacks will not be recorded.

## Basic Web Protection

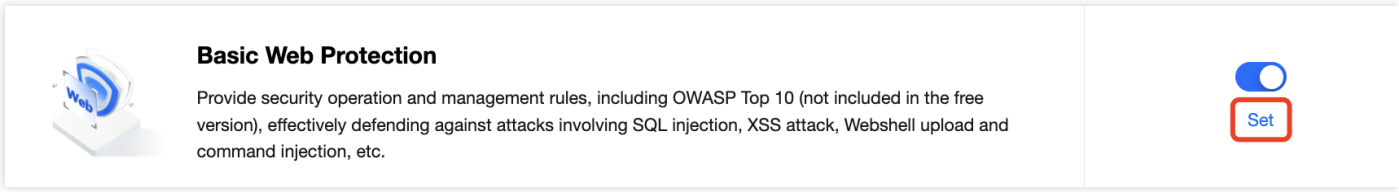
This feature provides protection rules developed by Tencent Cloud over the years, delivering very low false negative and false positive rates, and fast responses to 0day threats.

1. Log in to the EdgeOne console. Select **Attack Defense** > **Web Protection** on the left sidebar.

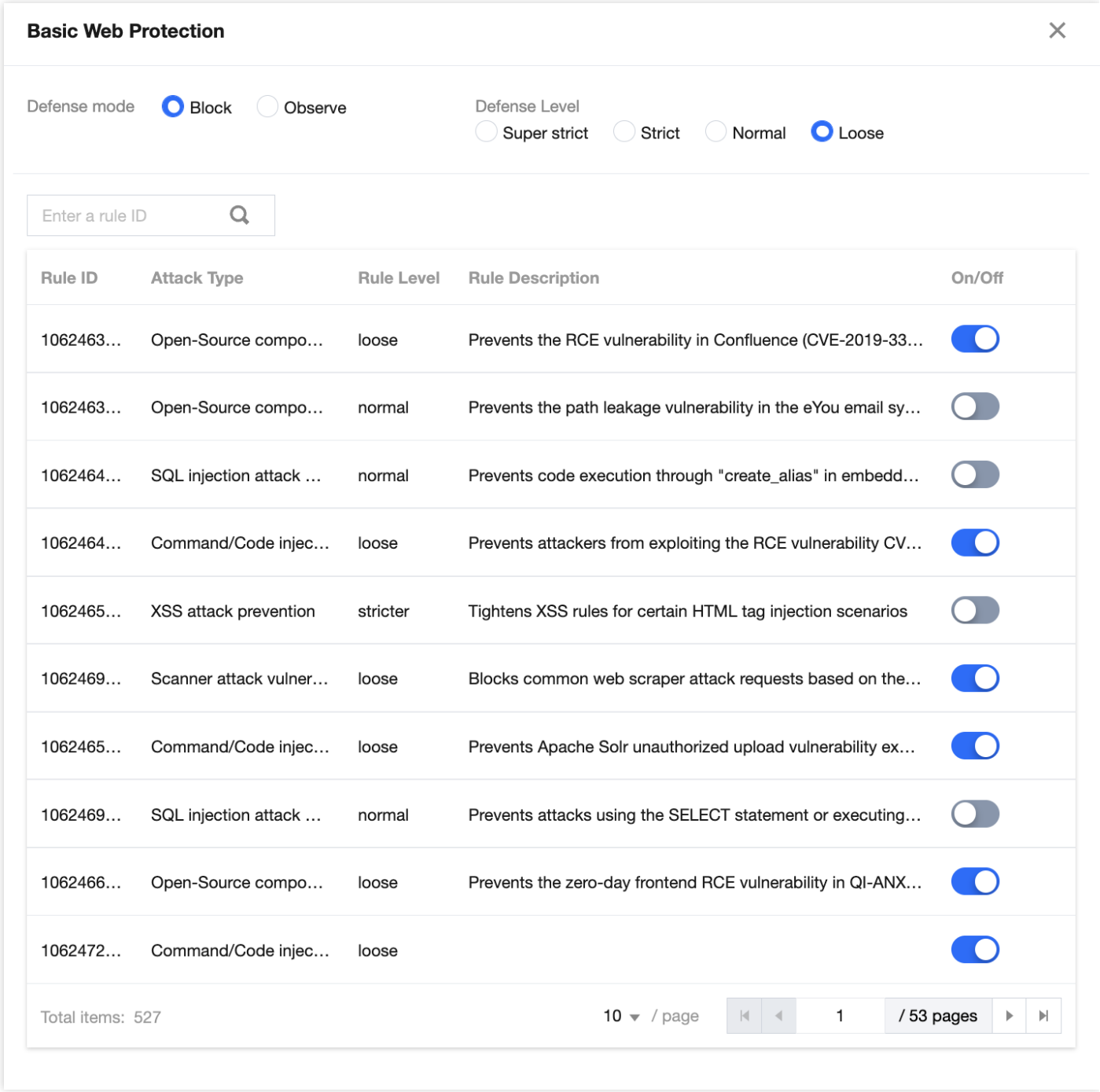
2. Select a site. Turn on/off the switch in the basic web protection module. If it's off, all traffic detected will be allowed, while your configurations will not be deleted.



3. To configure and modify the module, click **Set**.




4. The defense mode, defense level and rule list are editable.



**Parameter description:**

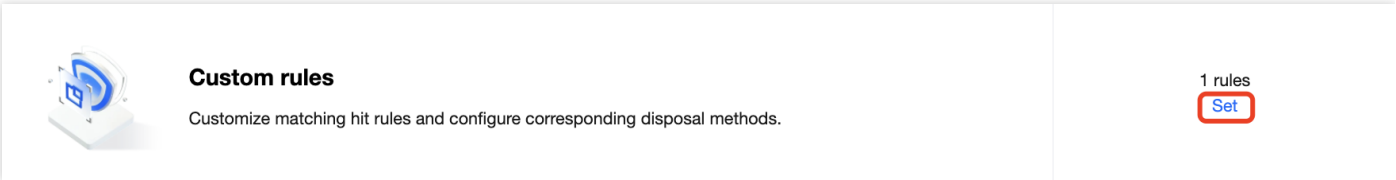
- Defense mode: Select "Block" or "Observe".
  - In the Block mode, attack traffic detected will be blocked and attacks will be recorded. This mode is used by default when basic web protection is enabled.
  - In the Observe mode, attack traffic detected will be allowed and attacks will be recorded, helping observe false positives incurred by your policies. To block the attack traffic, you can switch to the Block mode after your policy tuning.
- Defense level: There are four defense levels, namely, "Super strict", "Strict", "Normal", and "Loose". With a stricter mode enabled, the ability to identify and block suspicious attack traffic is stronger, which may cause false positives more easily. However, in a less strict mode, only obviously suspicious traffic will be identified and blocked with much lower false positives, though it provides lower security.
- A rule list contains the following configuration items:
  - Rule ID: The unique identifier of a rule, which is used to track attack logs for analysis.
  - Attack type: It describes the type of attacks.
  - Rule level: The defense level of a rule. Policies with the same rule level can be enabled/disabled at a time.
  - Rule description: It describes the defense role of a rule.
  - On/Off: Turn the switch on/off to enable/disable a rule.

# Custom Rule

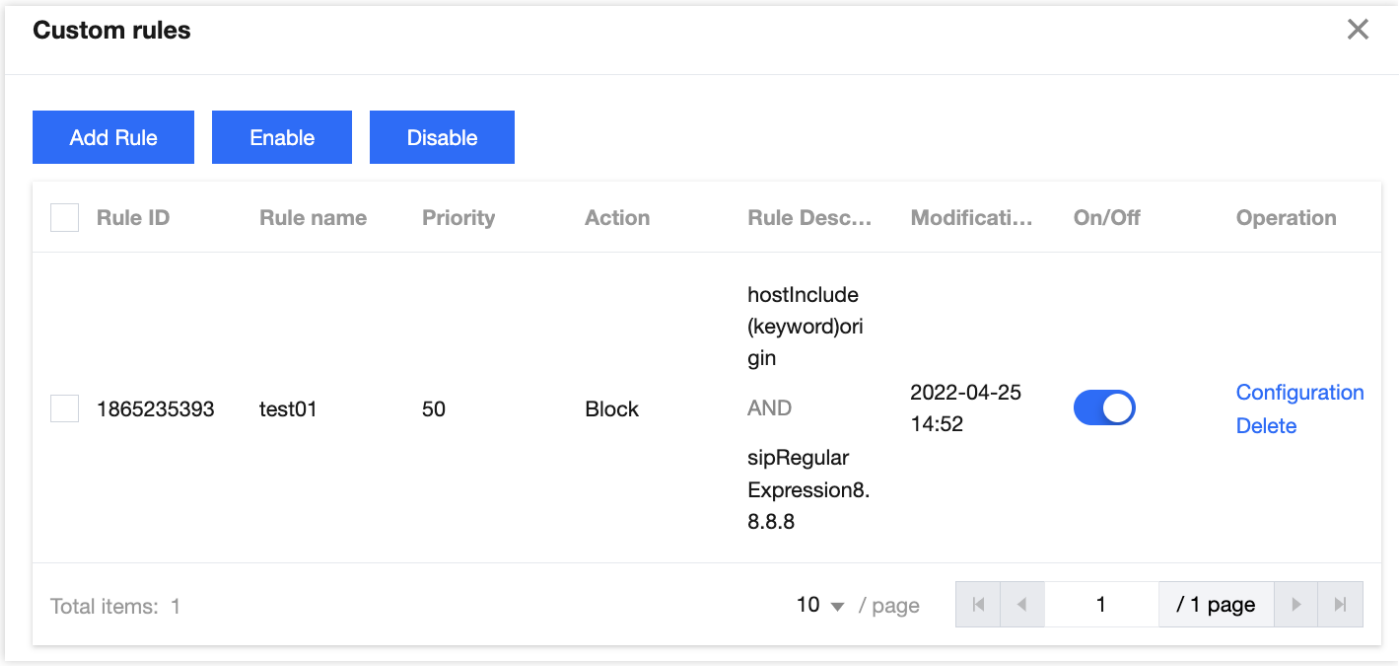
This feature allows you to create custom rules for a number of business use cases, such as allowing/blocking specific traffic.

## Adding a rule

1. On the web protection page, select a site. Click **Set** in the custom rule module.



2. On the custom rule page, click **Add Rule**. Set the rule name, matching method, action, and priority.



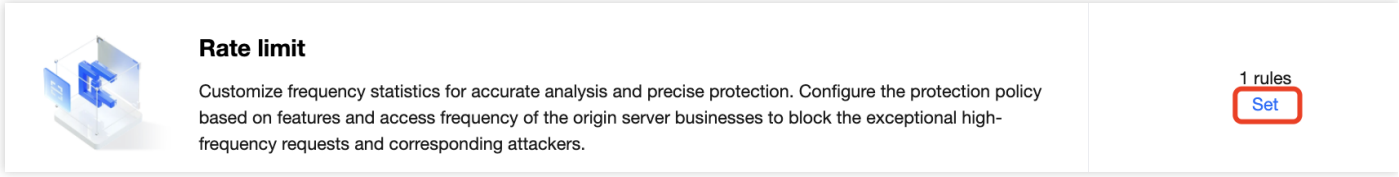

**Parameter description:**

- Rule name: It consists of letters, digits and underscores. A rule name will be generated automatically if this parameter is left empty. Note that a rule name must be unique.
- Matching method: It consists of configuration items such as the protocol field (http/https) and the logical operator (include/equal to). Up to 5 conditions per rule are allowed, and the relation among conditions is "AND". Note that the same field can only be configured once in each rule.
- Actions: It provides three options: Allow, Block and Observe.
  - Allow: Traffic that matches the specified rule will be allowed without any checks.
  - Block: Traffic that matches the specified rule will be blocked. Meanwhile, attacks will be recorded and a block page will be returned.
  - Observe: Traffic that matched the specified rule will be allowed, while attacks will be recorded.
- Priority: Execution order of a rule. Custom rules with higher priority (a larger priority value) take precedence over those with lower priority (a smaller priority value). For custom rules with the same priority, the later-added one will be executed first.

3. Click **OK**.

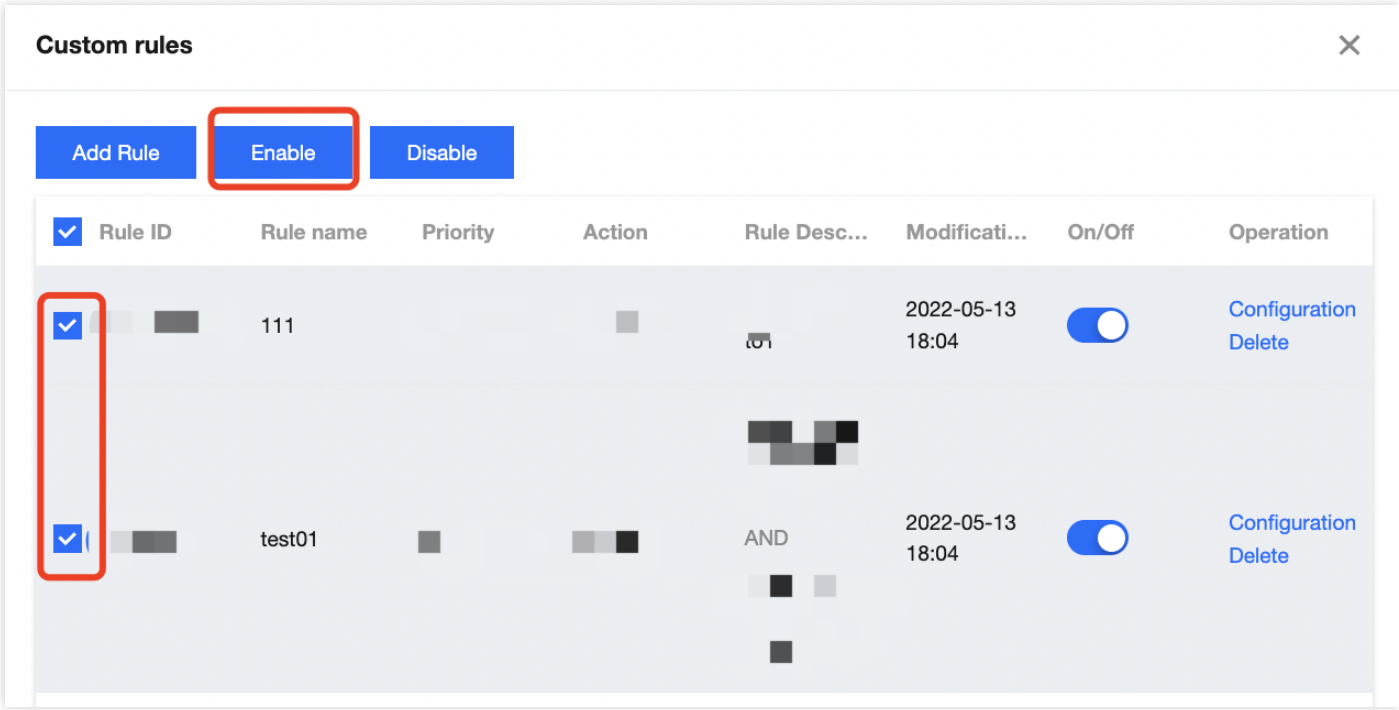
## Enabling a rule

1. On the web protection page, select a site. Click **Set** in the custom rule module.



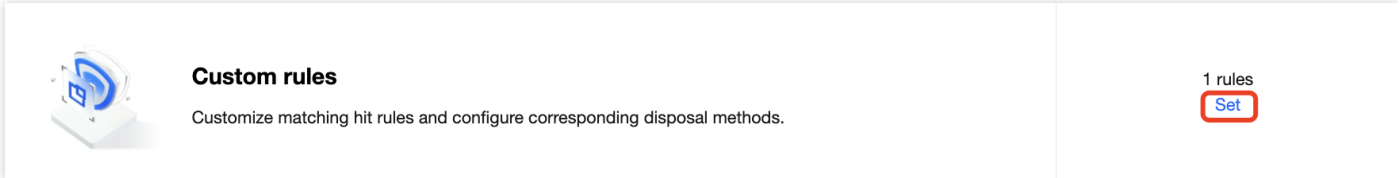

2. On the custom rule page, you can enable one or more rules.

- To enable a single rule, turn on the switch on the right of the rule.
- To enable multiple rules, click **Enable** after you select rules you want to enable.



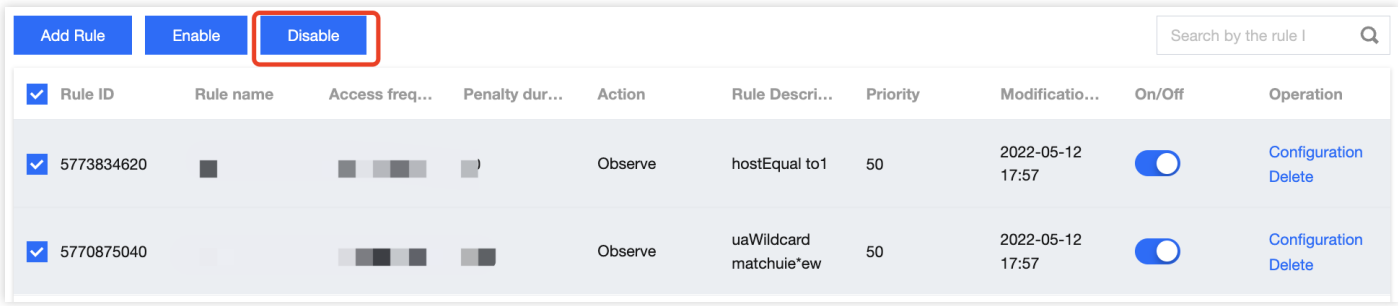

## Disabling a rule

1. On the web protection page, select a site. Click **Set** in the custom rule module.



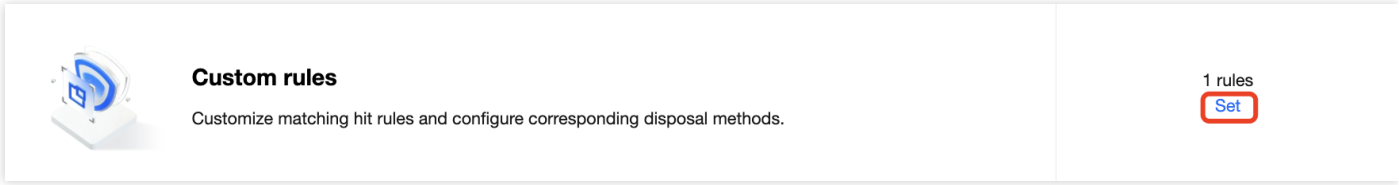

2. On the custom rule page, you can disable one or more rules.

- To disable a single rule, turn off the switch on the right of the rule.
- To disable multiple rules, click **Disable** after you select rules you want to disable.

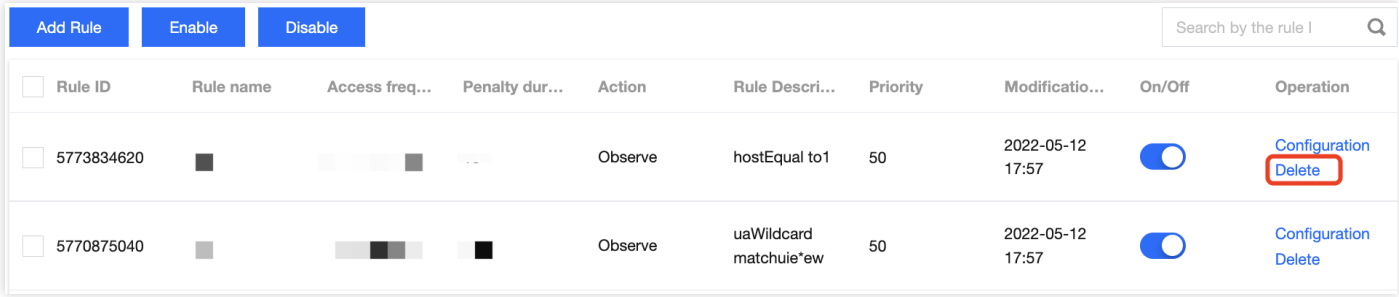



### Deleting a rule

1. On the web protection page, select a site. Click **Set** in the custom rule module.




2. On the custom rule page, select a rule you want to delete, and click **Delete** on the right.



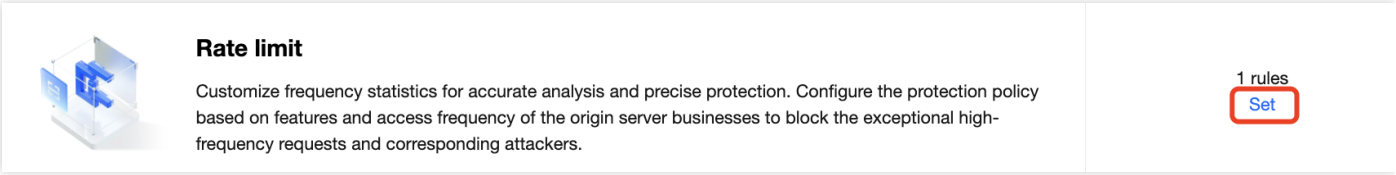

3. In the pop-up window, click **Delete**.

# Rate Limit

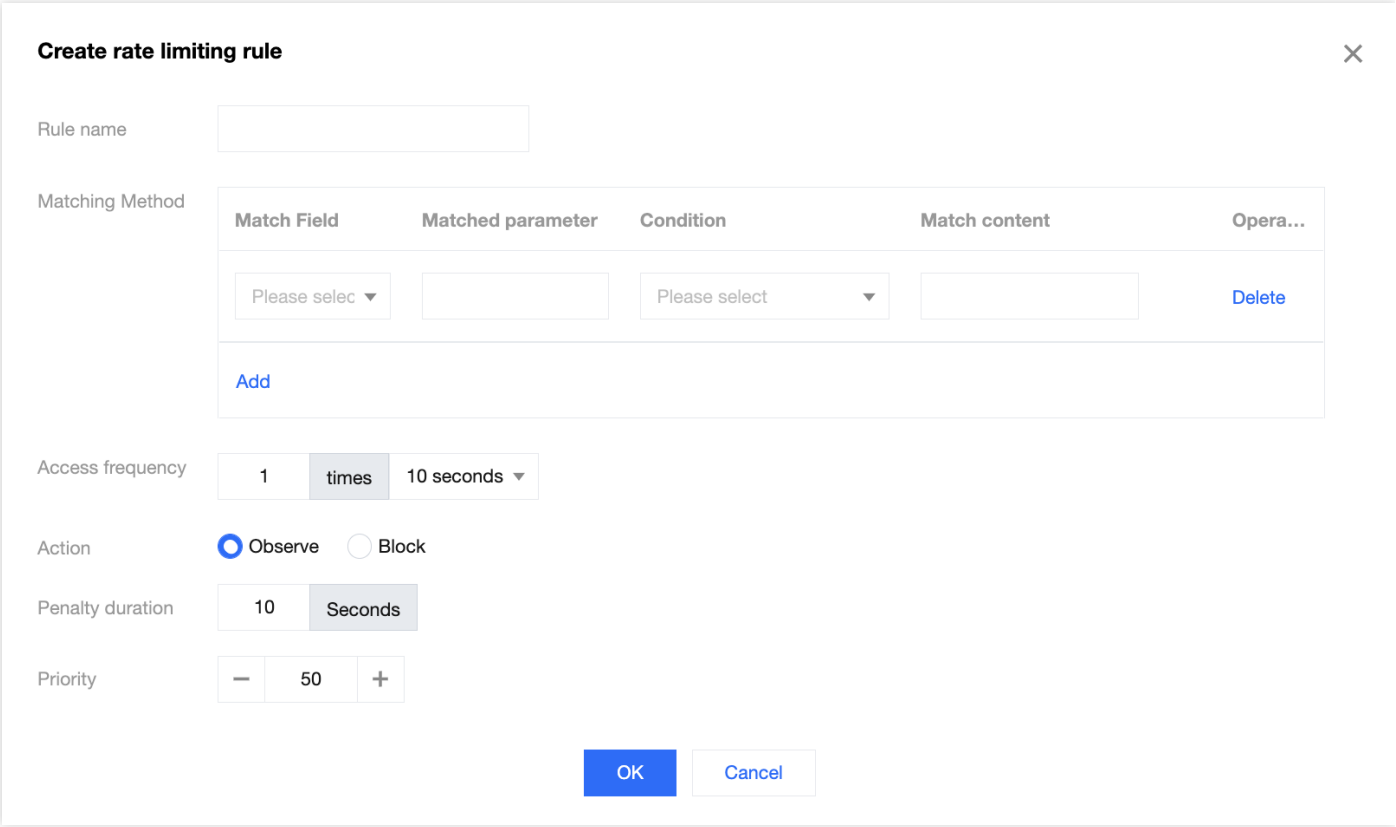
This feature enables you to limit the frequency of a source IP accessing third-level domain names. If the access frequency is exceeded, the source IP will be blocked for a period of time.

### Adding a rule

1. On the web protection page, select a site. Click **Set** in the rate limit module.




2. On the rate limit page, click **Add Rule**. Set the rule name, matching method, access frequency, action, penalty duration, and priority.




**Parameter description:**

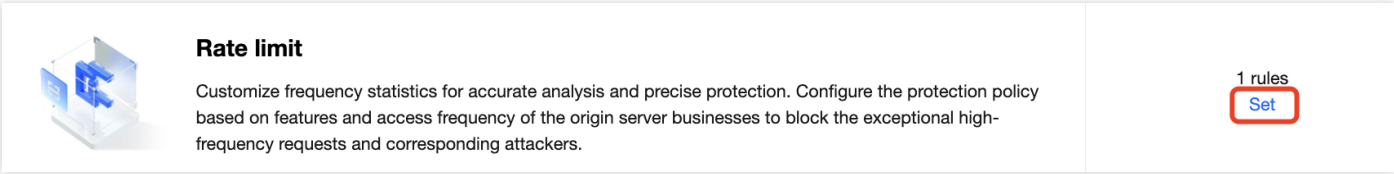
- Rule name: It consists of letters, digits and underscores. A rule name will be generated automatically if this parameter is left empty. Note that a rule name must be unique.
- Matching method: It consists of configuration items such as the protocol field (http/https) and the logical operator (include/equal to). Up to 5 conditions per rule are allowed, and the relation among conditions is "AND". Note that the same field can only be configured once in each rule.
- Access frequency: The frequency of a source IP accessing the current third-level domain name.
- Actions: It provides three options: Allow, Block and Observe.
  - Block: Traffic that matches the specified rule will be blocked. Meanwhile, attacks will be recorded and a block page will be returned.

  - Observe: Traffic that matched the specified rule will be allowed, while attacks will be recorded.
- Penalty duration: The amount of time used to observe/block the source IP when the action is triggered.
- Priority: Execution order of a rule. Custom rules with higher priority (a larger priority value) take precedence over those with lower priority (a smaller priority value). For custom rules with the same priority, the later-added one will be executed first.

3. Click **OK**.

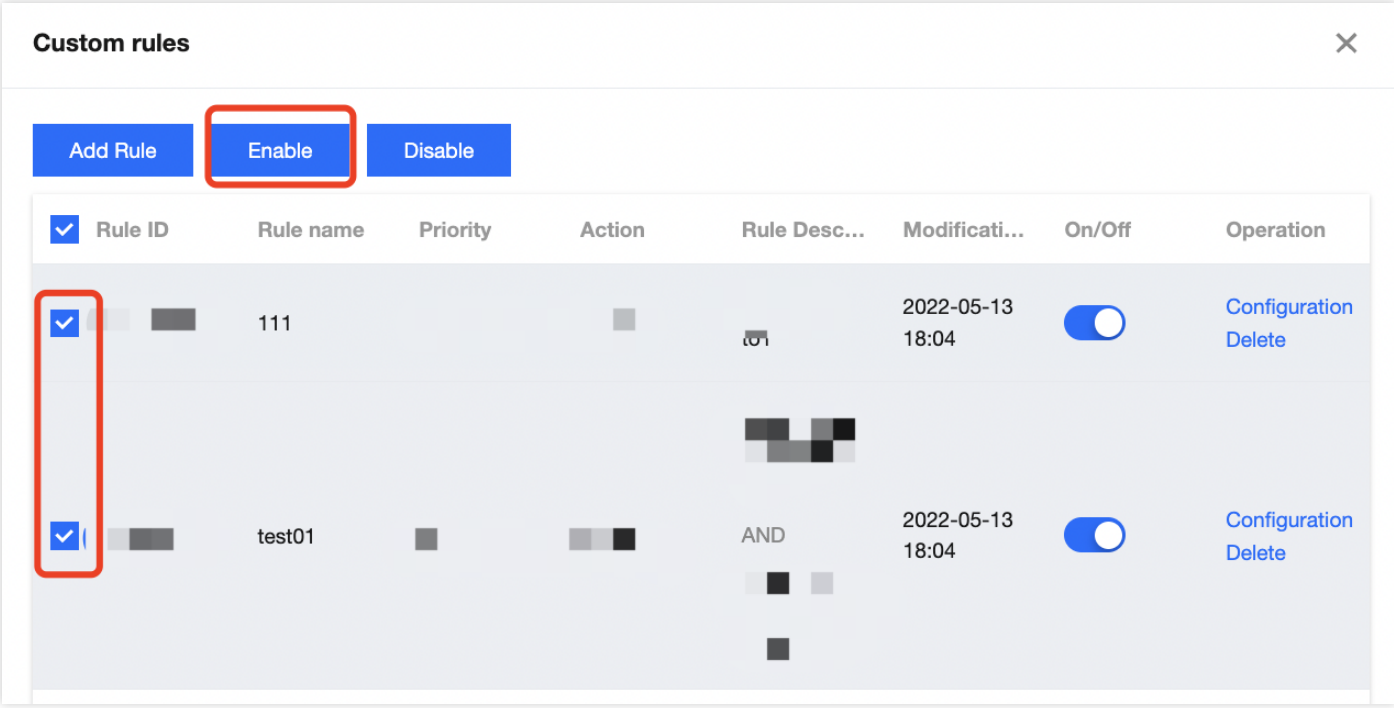
## Enabling a rule

1. On the web protection page, select a site. Click **Set** in the rate limit module.



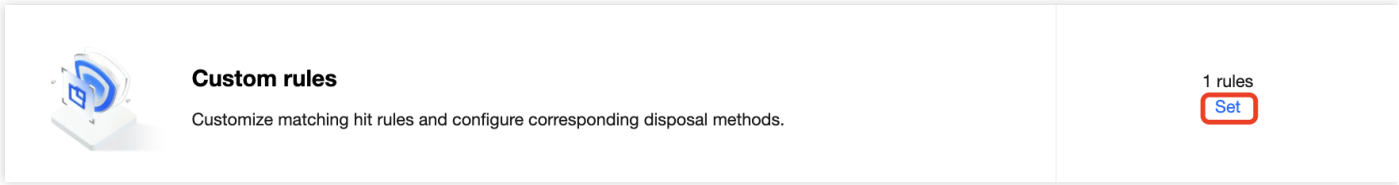

2. On the rate limit page, you can enable one or more rules.

- To enable a single rule, turn on the switch on the right of the rule.
- To enable multiple rules, click **Enable** after you select rules you want to enable.



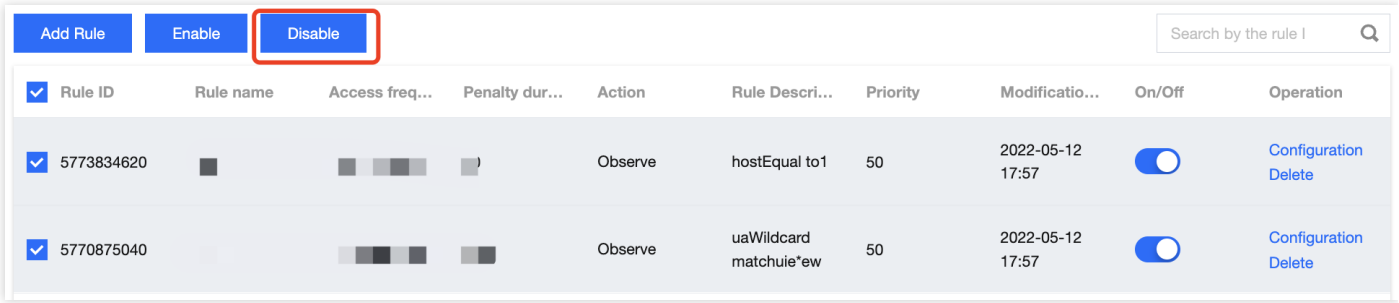
## Disabling a rule

1. On the web protection page, select a site. Click **Set** in the custom rule module.



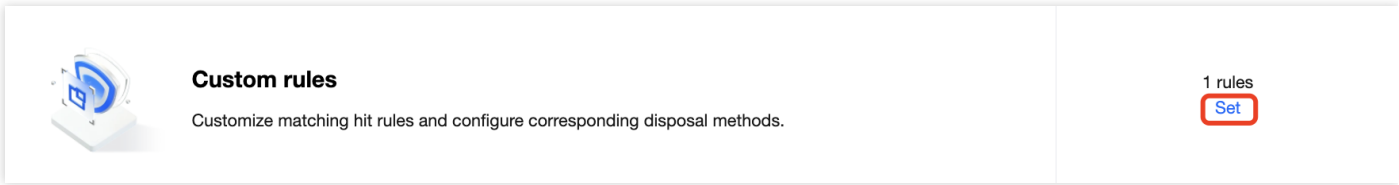

2. On the rate limit page, you can disable one or more rules.

- To disable a single rule, turn off the switch on the right of the rule.
- To disable multiple rules, click **Disable** after you select rules you want to disable.

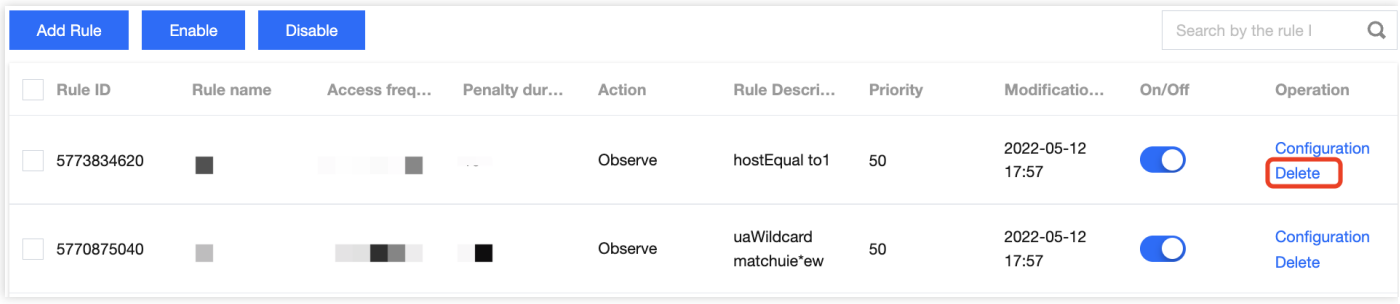



## Deleting a rule

1. On the web protection page, select a site. Click **Set** in the custom rule module.



2. On the rate limit page, select a rule you want to delete, and click **Delete** on the right.




3. In the pop-up window, click **Delete**.

# Bot Management

Last updated：2022-10-09 09:42:57

## Overview

Based on request and session characteristics, client reputation intelligence, and smart behavior analysis, the Bot Management feature identifies and restricts access from bot clients (non-browser clients such as proxies, crawlers, scanners, search engine bots, and API clients), identifies and handles high-risk malicious requests (such as malicious scans, botnets, ATO attack sources, high-risk proxies, and brute force attacks), and reduces false positives and blocking for low-risk crawlers and legitimate APIs.

We recommend you optimize bot management rule configurations in the following steps:

- *1*Change the rule action to **Observe**. In this way, the bot management feature allows matched requests and records a rule match log.
- *2*Send a known normal or need-to-block request.
- *3*Check the bot management rule match log. For normal requests, set the action to **Observe** or **Ignore**; for need-to-block requests, set the action to **CAPTCHA** (**JavaScript challenge** or **Managed challenge**) or **Block**.

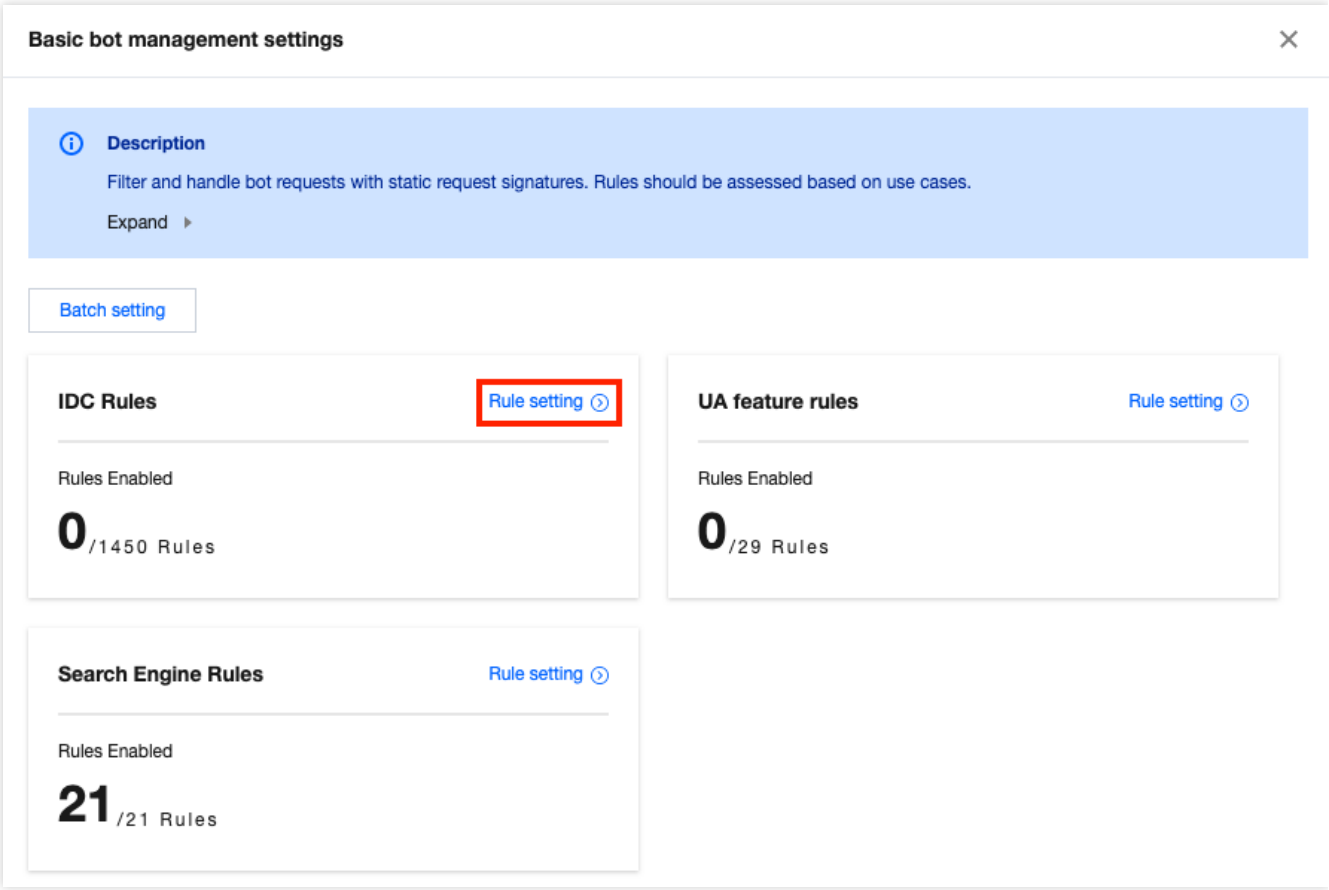
## Basic Bot Protection Settings

EdgeOne can process requests by characteristic, such as UA, search engine, and IDC.

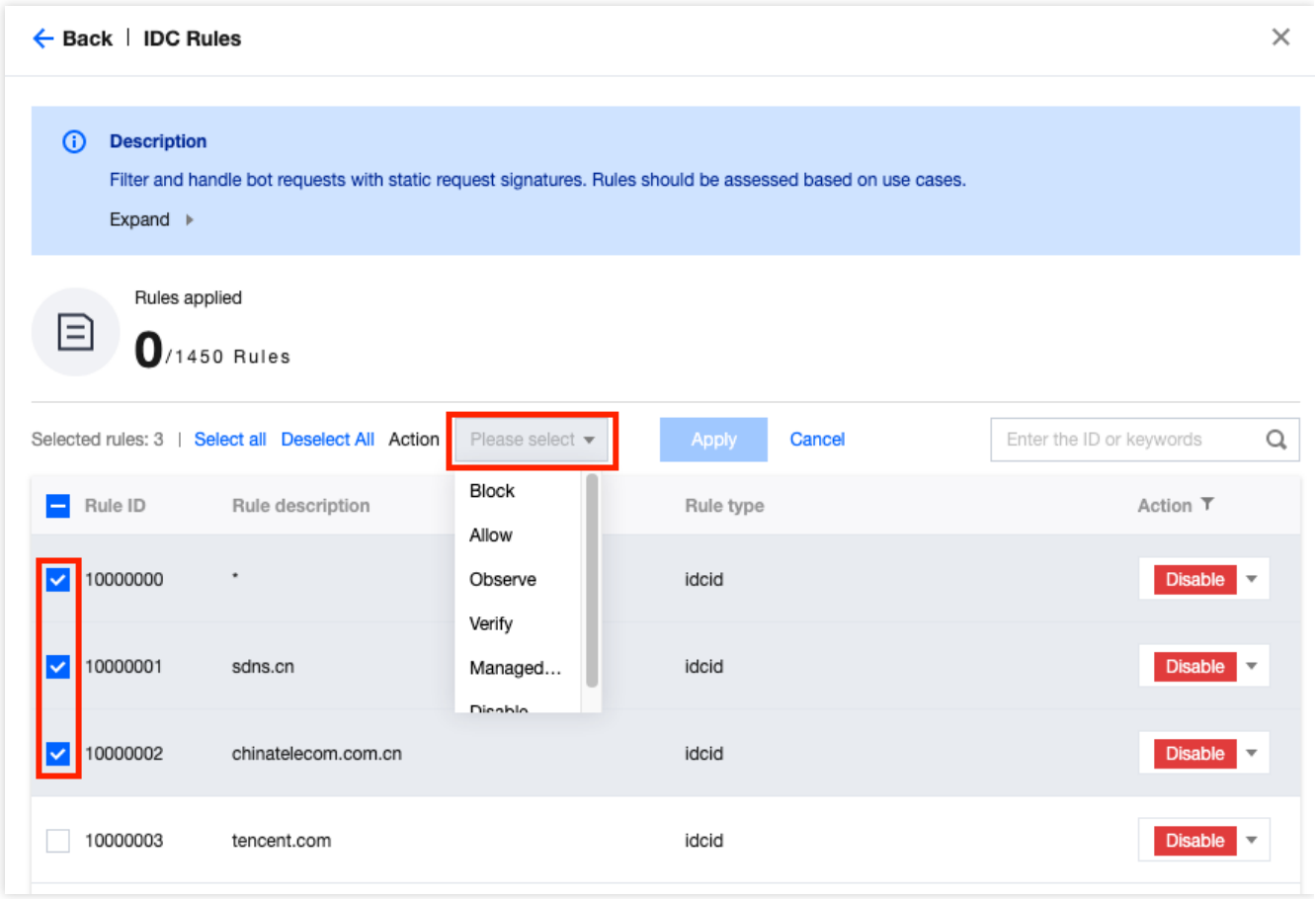
> Note：
> Configuration suggestion: The feature identifies bot requests based on the characteristics of static client requests.
>
> - UA Feature Rules: Identifies clients of a specific type. It's applicable to most general scenarios. Configure the rule, set the Action to **Observe** first and then adjust it according to the result.
> - Search Engine Rules: Identifies bot clients of search engines. It's applicable to non-webpage sites (such as API services). If your business is open to the search engines, we recommend you disable it.
> - IDC Rules: Identifies clients from specified IDCs or ISPs. Configure the rule, set the Action to **Observe** first and then adjust it according to the result.

1. Log in to the EdgeOne console, select **Security** > **Bot Management** on the left sidebar, and select the desired site and subdomain name.

2. In the **Basic bot protection settings** section, click **Set** to adjust the rule configuration.
3. On the **Basic bot protection settings** page, you can set a single rule category or batch set rule categories.
   - Set a single rule category
     a. Click **Rule setting** on the target rule category card to configure its rules.



b. Select a **Rule ID**, click the **Action** drop-down list, and select an action.



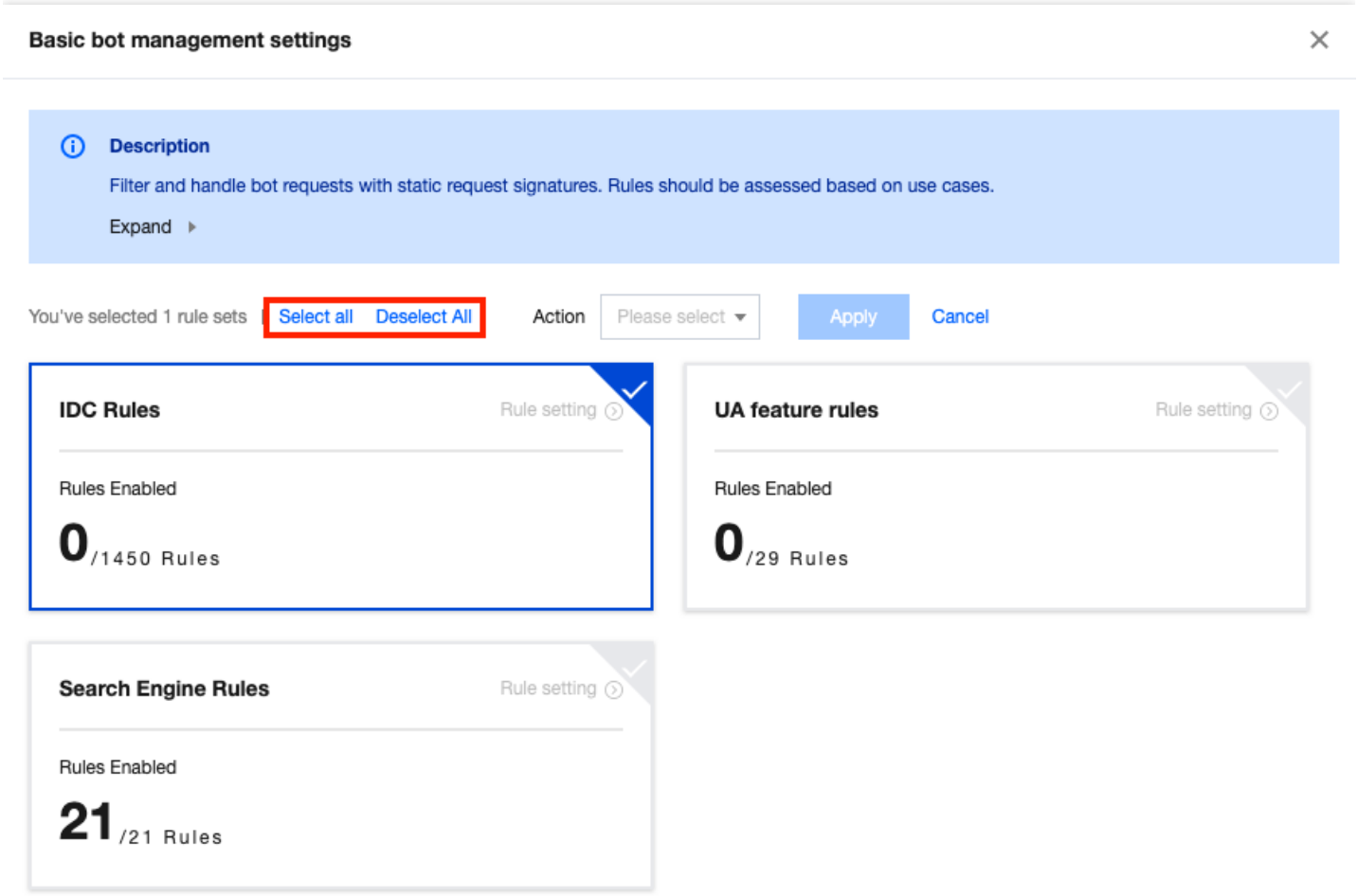

c. Click **Apply**.

- Batch set rule categories

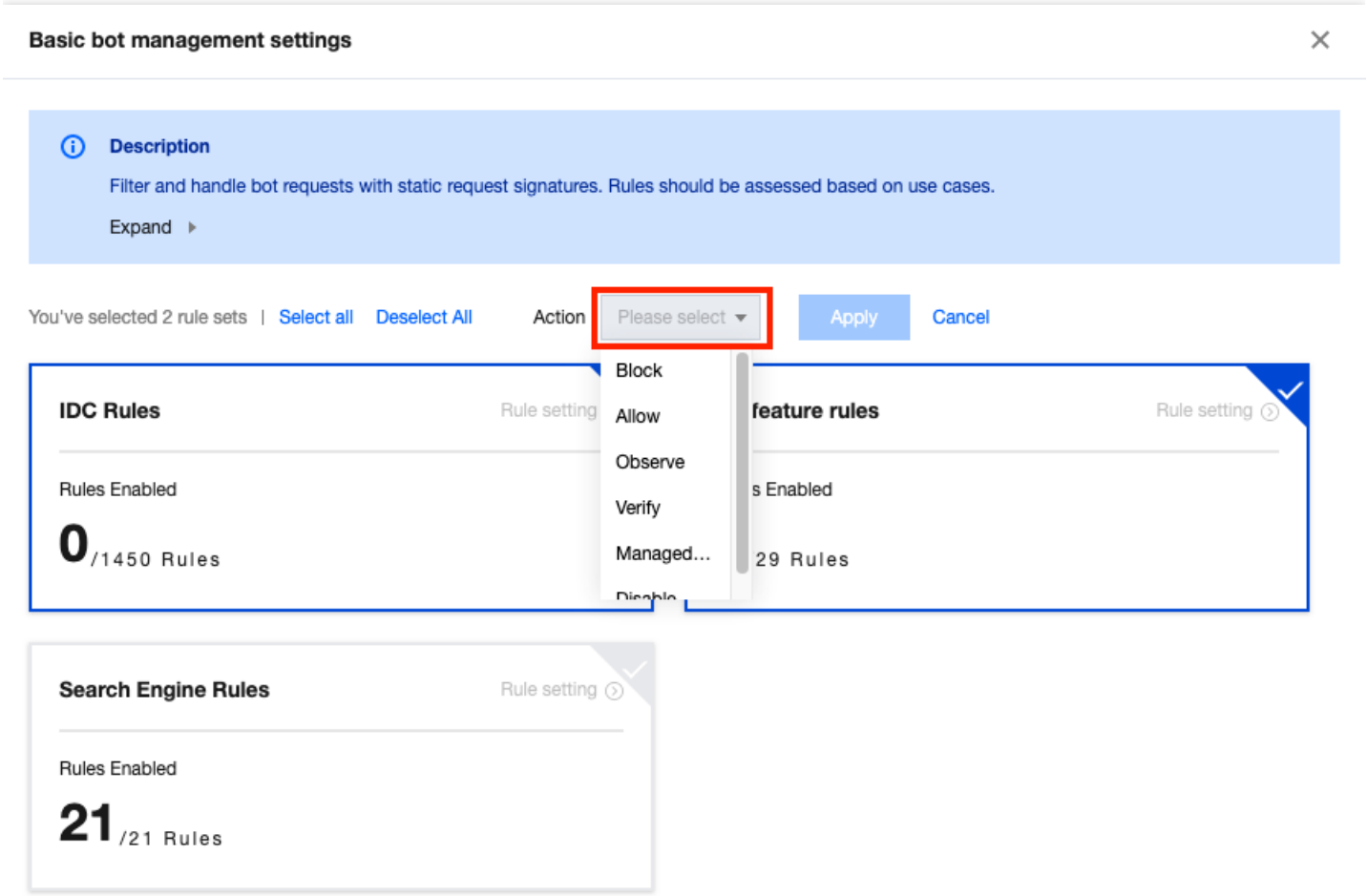
a. On the **Basic bot protection settings** page, click **Batch setting** and select one or more rule categories.

b. In batch setting mode, select all the categories you want.

> Note：
> In batch setting mode, you can **Select all** or **Deselect all** category cards at once.




3. Click the **Action** drop-down list and select an action.




4. Click **Apply**.

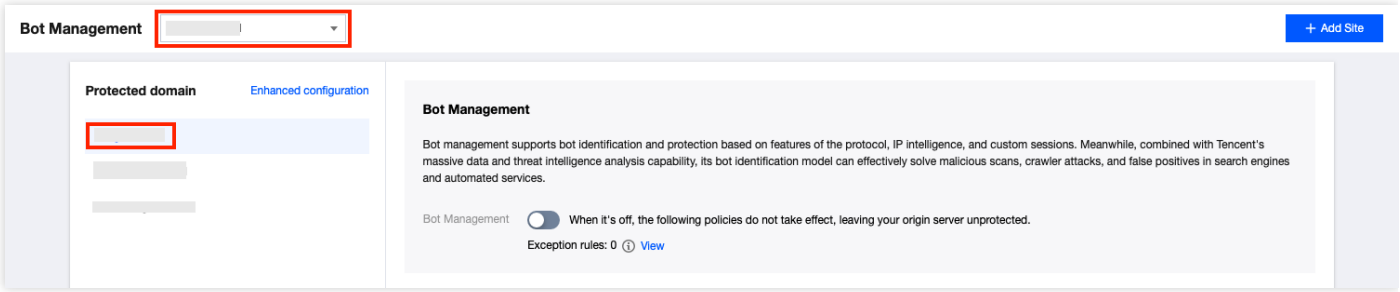
4. Click **OK** at the bottom to complete.

# Custom Rule

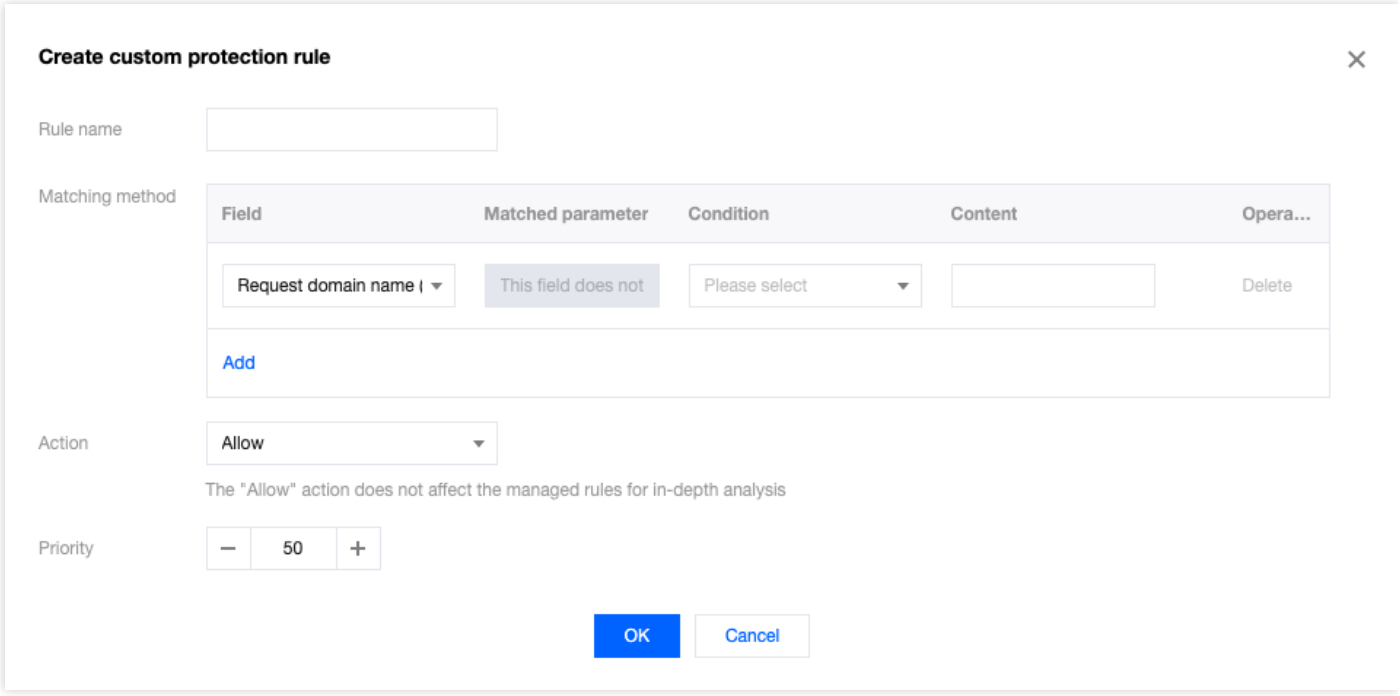
This feature allows you to create custom rules for a number of business use cases, such as allowing/blocking specific traffic.

### Adding a rule

1. Log in to the EdgeOne console, select **Security** > **Bot Management** on the left sidebar, and select the desired site and subdomain name.




2. In the **Custom rules** section, click **Set**.
3. On the custom rule page, click **Add rule**. Set the rule name, matching method, action, and priority.




**Parameter description:**

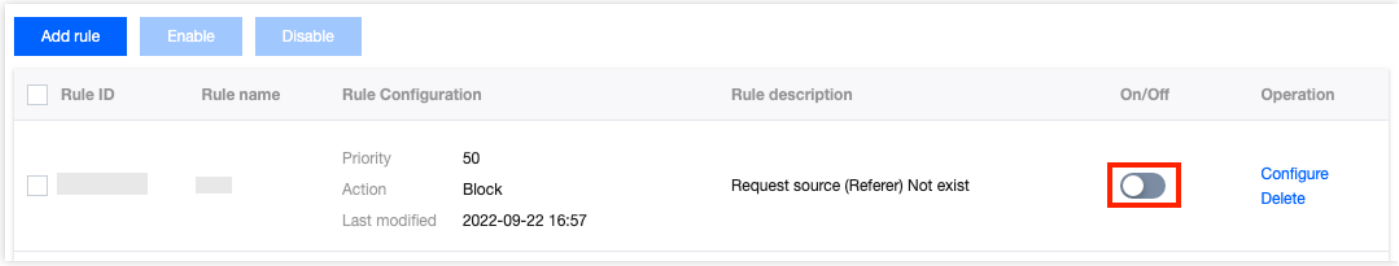
- Rule name: It contains letters, digits, and underscores. A rule name will be generated automatically if this parameter is left empty. Note that a rule name must be unique.
- Matching method: It consists of configuration items such as the protocol field (http/https) and the logical operator (include/equal to). Up to 5 conditions per rule are allowed, and the relation among conditions is "AND". Note that the same field can only be configured once in each rule.
- Action: Select as needed.
- Priority: Execution order of a rule. Custom rules with higher priority (a larger priority value) take precedence over those with lower priority (a smaller priority value). For custom rules with the same priority, the later-added one will be executed first.

3. Click **OK**.

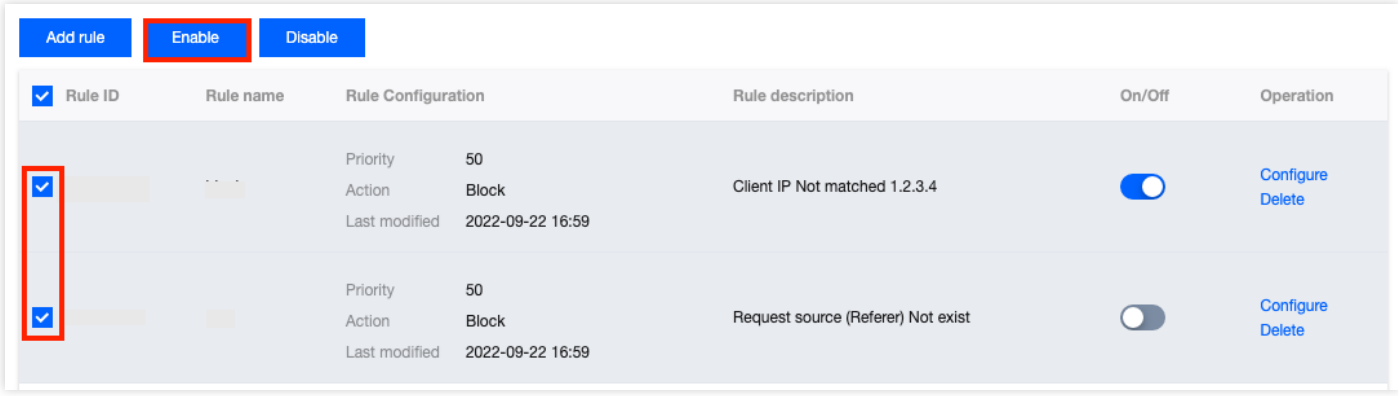
## Enabling a rule

On the **Custom rules** page, you can enable a single rule or multiple rules.

- To enable a single rule, select the target **Rule ID** and toggle on the switch .




- To enable multiple rules, click **Enable** after you select rules you want to enable.




## Disabling a rule

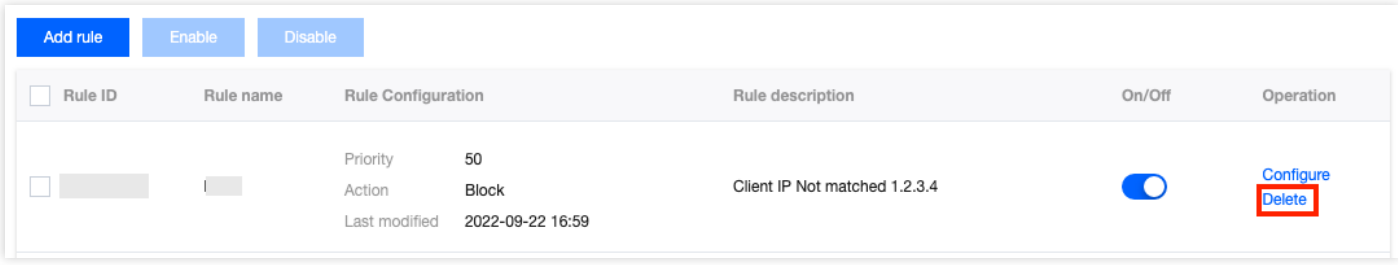
On the **Custom rules** page, you can disable a single rule or multiple rules.

- To disable a single rule, turn off the switch on the right of the rule.

- To disable multiple rules, click **Disable** after you select rules you want to disable.


### Deleting a rule

1. On the custom rule page, select a rule you want to delete, and click **Delete** on the right.




2. In the **Delete rule** pop-up window, click **Delete**.

# Client Reputation

The client IP reputation is profiled based on the malicious access request and intelligence data collected recently. You can configure the action according to the confidence of the malicious client.

Note：
Client reputation confidence: Under each type of client reputation rules, each confidence value corresponds to a client address list and reflects the frequency and consistency of a certain type of malicious behaviors performed from client addresses in the list.

- High confidence: Malicious behaviors are performed constantly and highly frequently from the client address. It is almost certain that requests from this address are malicious. We recommend you configure the rule as **Block**.

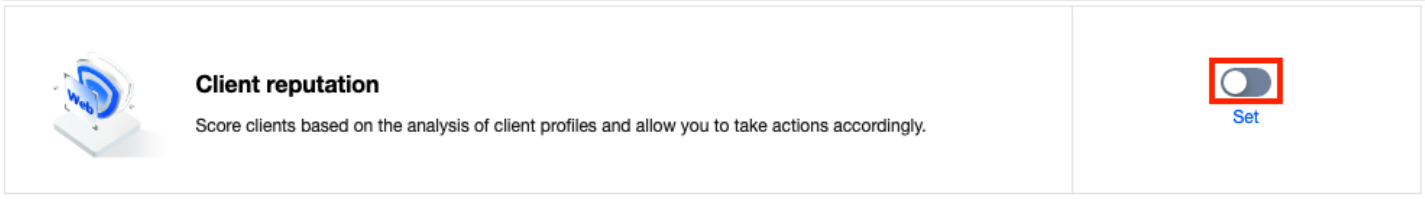
- Medium confidence: Malicious behaviors are performed frequently from the client address. It is highly probable that requests from this address are malicious; however, false positives may occur. We recommend you configure the rule to **JavaScript challenge** or **Managed challenge**.
- General confidence: Malicious behaviors are performed constantly from the client address. This address is more likely to send malicious requests than others; however, false positives may occur. We recommend you configure the rule to **Observe** and change it to **JavaScript challenge** or **Managed challenge** as needed.

1. Log in to the EdgeOne console, select **Security** > **Bot Management** on the left sidebar, and select the desired site and subdomain name.

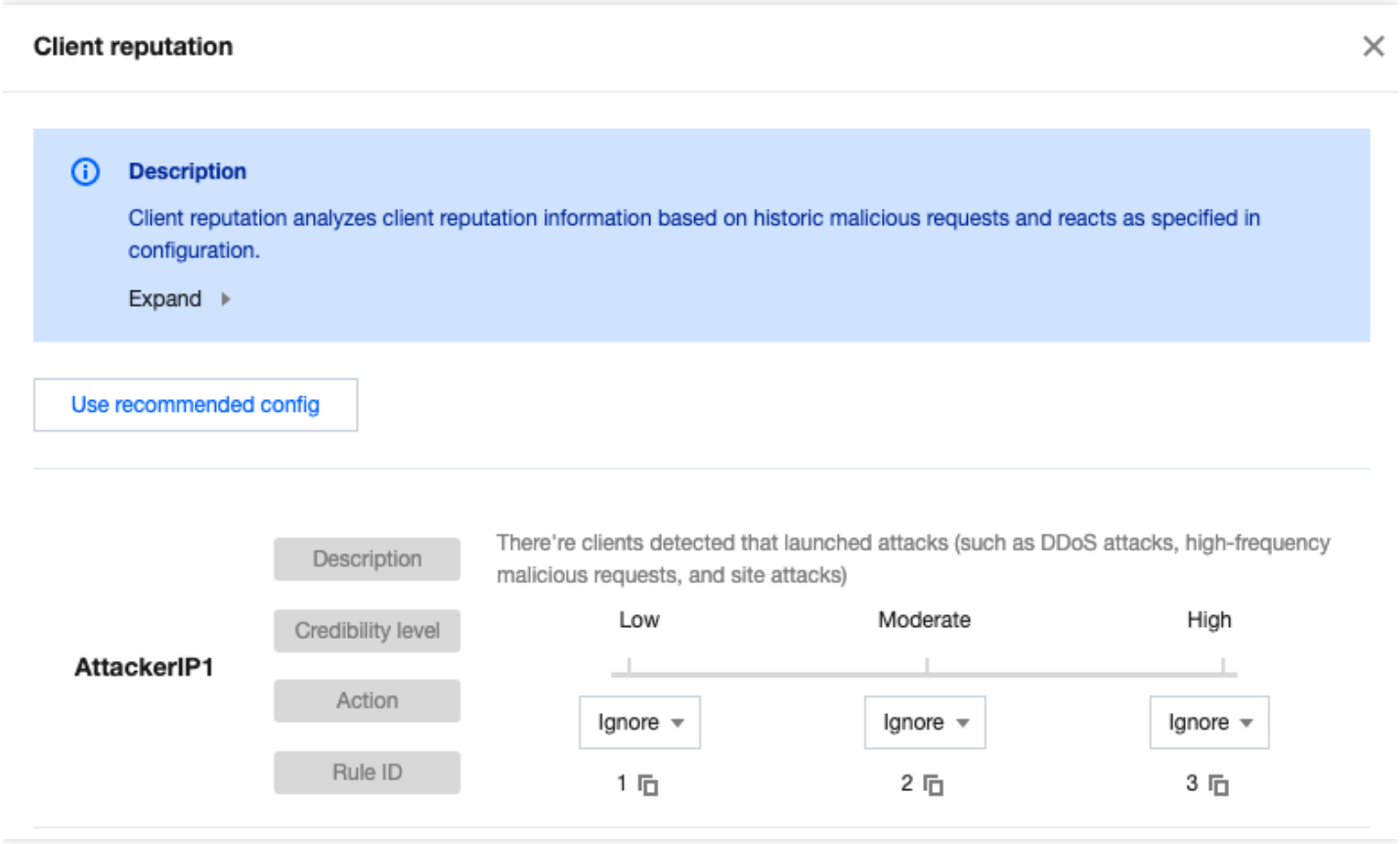

2. In the **Client reputation** section, toggle on or off the switch on the right.

Note：

- After the client reputation feature is disabled, related rules no longer take effect. Requests are allowed by default, and no logs are recorded.
- When the client reputation feature is enabled for the first time, we recommend you configure the detailed rule before enabling the rule. This is to prevent normal business access from being affected.




3. In the **Client reputation** section, click **Set** to configure a rule in the module.
4. On the **Client reputation** page, click the **Action** drop-down list in the target malicious behavior category section and select an action.




5. Click **OK** to complete.

# DDoS Mitigation

Last updated：2022-10-09 09:42:57

This document describes the DDoS mitigation level, IP blocklist/allowlist, regional blocking, and protocol blocking features of DDoS mitigation as well as their configurations.

> Note：
> DDoS mitigation features and their configurations may be different depending on the EdgeOne plan you purchase.

## Prerequisites

You have purchased the EdgeOne Enterprise plan and connected your site to EdgeOne or accessed the layer-4 proxy.

## DDoS Mitigation Level

EdgeOne provides different DDoS mitigation levels in different scenarios. This document describes how to configure the DDoS mitigation level in the console.

### Use cases

EdgeOne allows you to adjust mitigation policies and provides three mitigation levels against DDoS attacks. The mitigation operations at each level are described below:

| Protection Level | Protection Action | Description |
| --- | --- | --- |
| Loose | • Filters SYN and ACK data packets with explicit attack attributes.<br>• Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications.<br>• Filters UDP data packets with explicit attack attributes. | • This cleansing policy is loose and only defends against explicit attack packets.<br>• We recommend choosing this protection level when normal requests are blocked. Complex attack packets may pass through the security system. |

| Protection Level | Protection Action | Description |
| --- | --- | --- |
| Medium | • Filters SYN and ACK data packets with explicit attack attributes.<br>• Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications.<br>• Filters UDP data packets with explicit attack attributes.<br>• Filters common UDP-based attack packets.<br>• Actively verifies the source IPs of some access attempts. | • This cleansing policy is suitable for most businesses and capable of defending against common attacks.<br>• The level Medium is chosen by default. |
| Strict | • Filters SYN and ACK data packets with explicit attack attributes.<br>• Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications.<br>• Strictly checks and filters UDP data packets with explicit attack attributes and UDP-based attack packets.<br>• Actively verifies the source IPs of some access attempts.<br>• Filters ICMP attack packets. | This cleansing policy provides strict traffic cleansing. We recommend choosing this level when attack packets pass through the security system in **Medium** mode. |

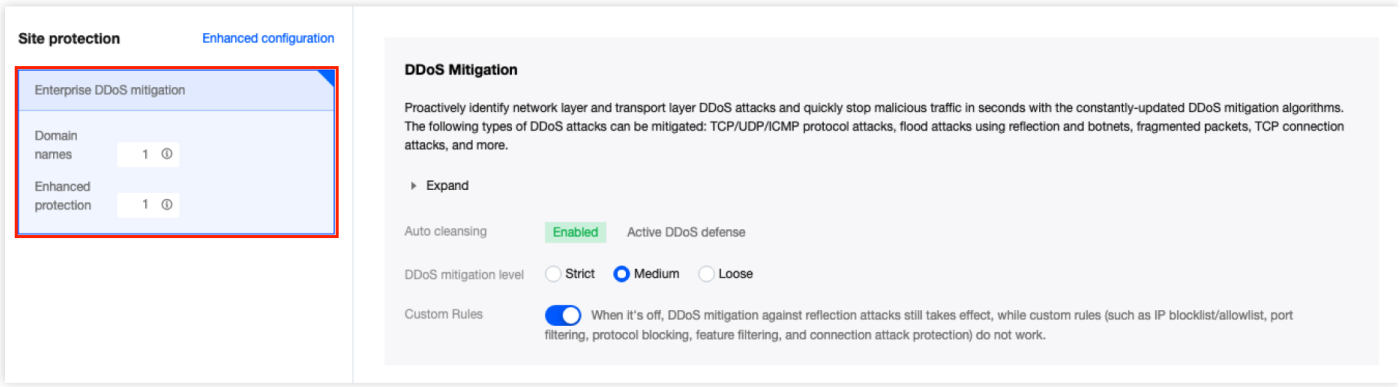
Note：

- If you want to protect your business from massive attacks or use UDP for your business, contact us to customize a policy that can ensure business continuity in **Strict** mode.
- By default, the purchased EdgeOne Enterprise plan uses the **Medium** mitigation level. You can adjust the level based on your actual business conditions.
- By default, the purchased EdgeOne Standard plan uses the **Medium** mitigation level.

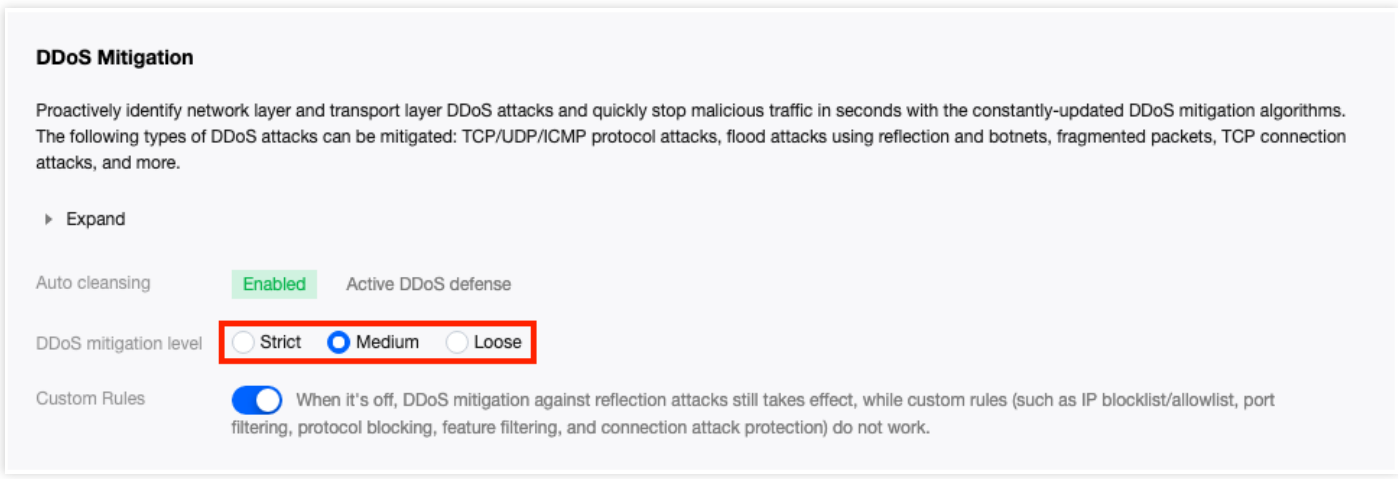
## Directions

1. Log in to the EdgeOne console and select **Security** > **DDoS Mitigation** on the left sidebar.

2. On the left of the **DDoS mitigation** page, select a mitigation business object, such as a **DDoS mitigation Enterprise plan** or **DDoS mitigation Enterprise plan - L4 proxy** instance.




3. In the **DDoS mitigation level** section, the **Medium** mitigation level is applied to your sites in EdgeOne by default when DDoS mitigation is enabled. You can adjust the level based on your actual business needs.




# IP Blocklist/Allowlist

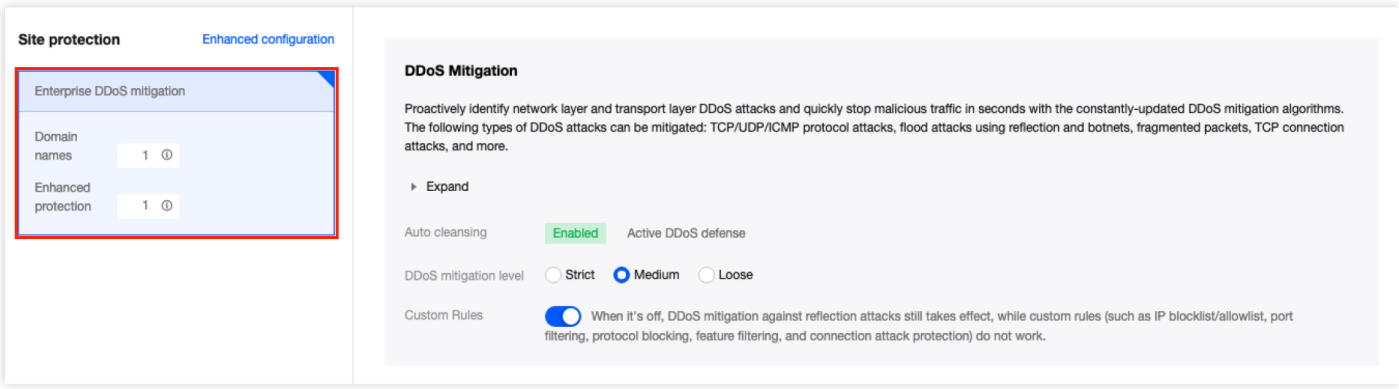
EdgeOne enables you to configure the IP blocklist and allowlist to control access to EdgeOne sites and block or allow access requests based on the client source IP.

Note：

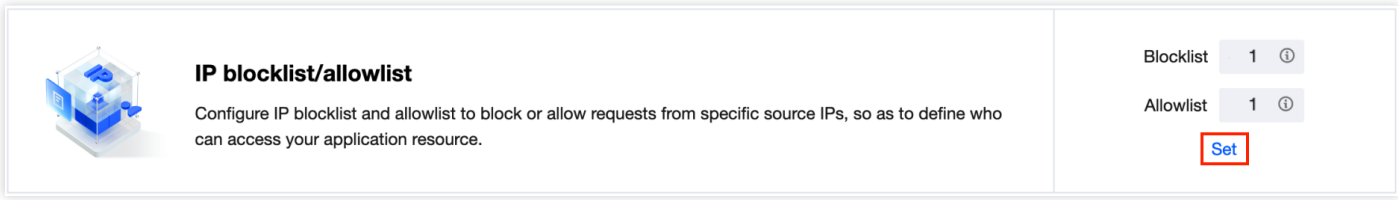
The IP blocklist/allowlist rules take effect in 5 to 10 seconds after being saved.

- The access requests from the IPs on the allowlist will not be filtered by any DDoS mitigation policy.
- The access requests from the IPs on the blocklist will be discarded directly.

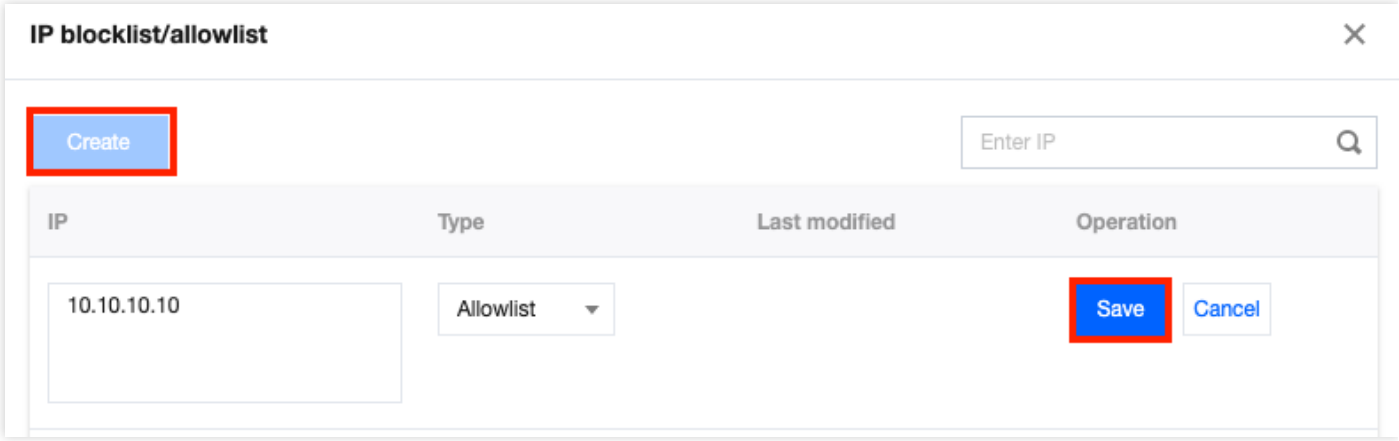
1. Log in to the EdgeOne console and select **Security** > **DDoS Mitigation** on the left sidebar.
2. On the left of the **DDoS mitigation** page, select a mitigation business object, such as a **DDoS mitigation Enterprise plan** or **DDoS mitigation Enterprise plan - L4 proxy** instance.



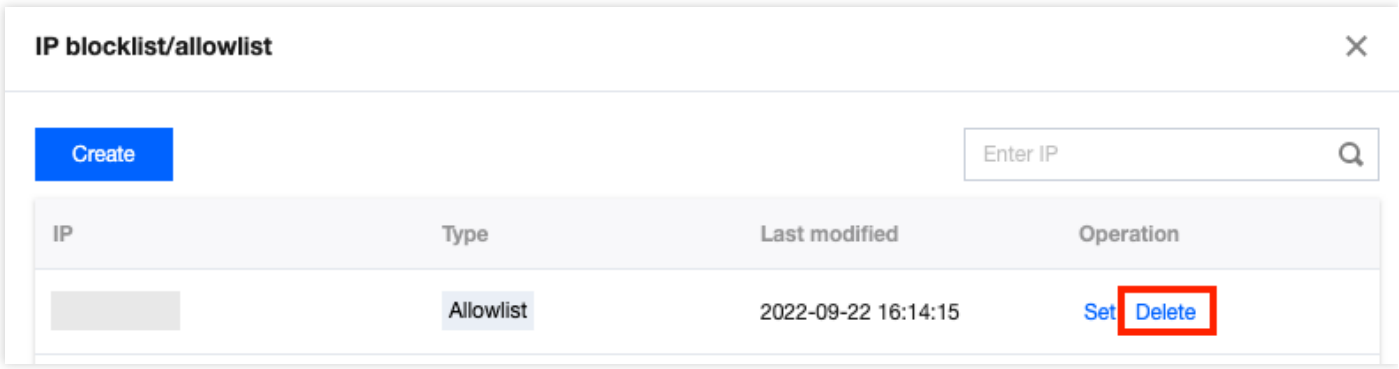

3. Click **Set** in the "IP blocklist/allowlist" section.




4. On the **IP blocklist/allowlist** page, click **Create** to create a rule, enter the target IP, select **Blocklist** or **Allowlist** for the type, and click **Save**.




5. (Optional) After the rule is created, it is added to the rule list. To delete it, click **Delete** in the "Operation" column on the right.

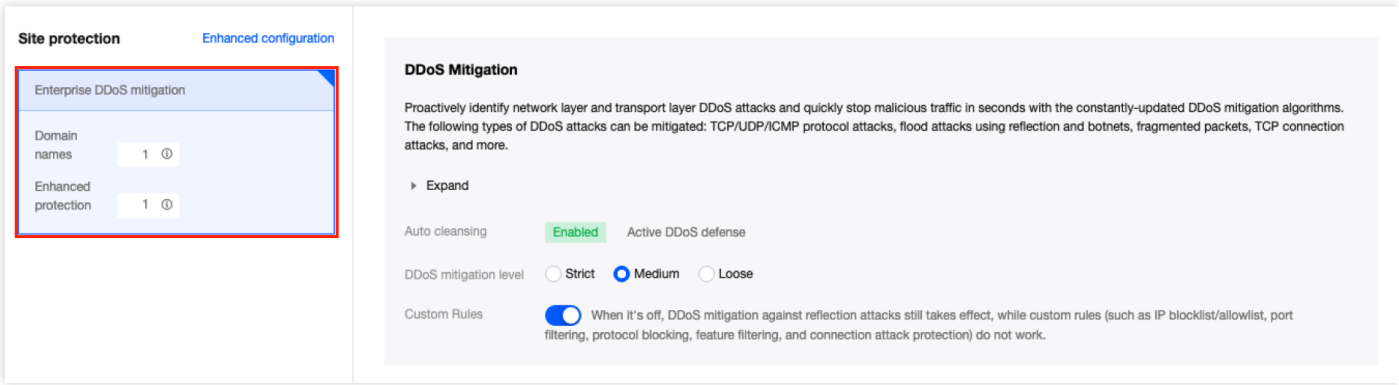



# Regional Blocking

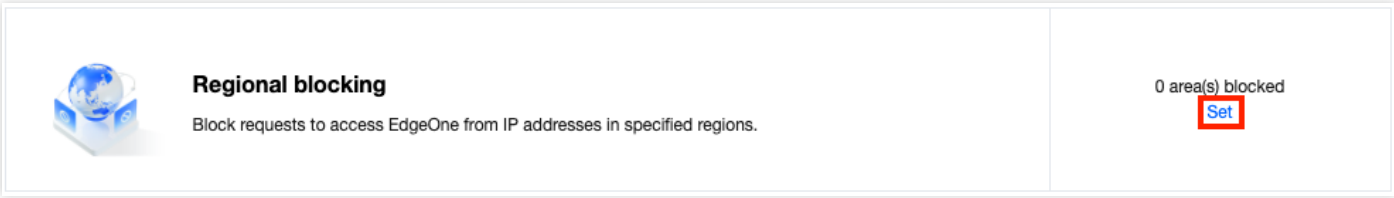
EdgeOne enables you to prevent client IPs in specific regions from accessing your site. It can block traffic from multiple regions/countries.

> Note：
> After you configure the regional blocking setting, attack traffic targeting the region will still be recorded but will not be allowed to your real server.

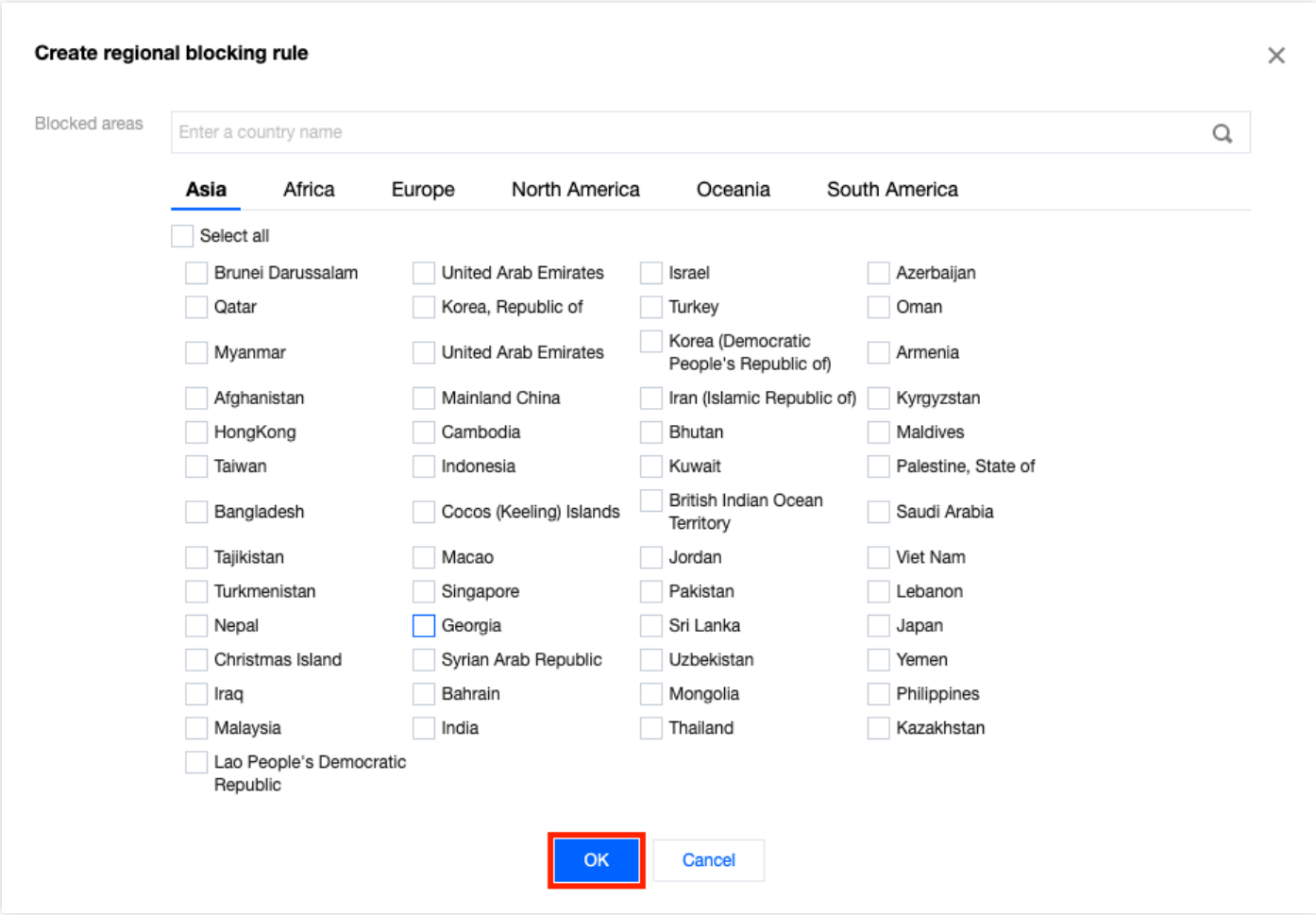
1. Log in to the EdgeOne console and select **Security** > **DDoS Mitigation** on the left sidebar.
2. On the left of the **DDoS mitigation** page, select a mitigation business object, such as a **DDoS mitigation Enterprise plan** or **DDoS mitigation Enterprise plan - L4 proxy** instance.



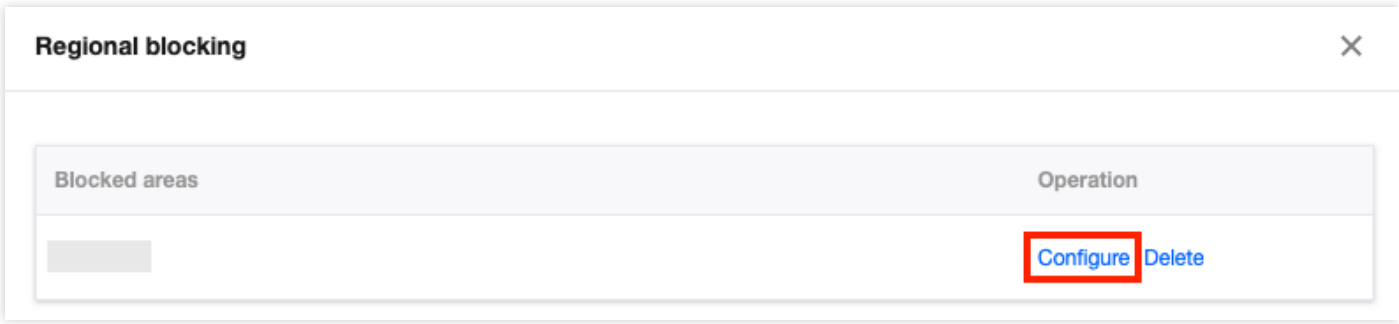
3. Click **Set** in the "Regional blocking" section.




4. On the regional blocking page, click **Create**.
5. In the **Create regional blocking policy** pop-up window, select the target region and click **OK**.



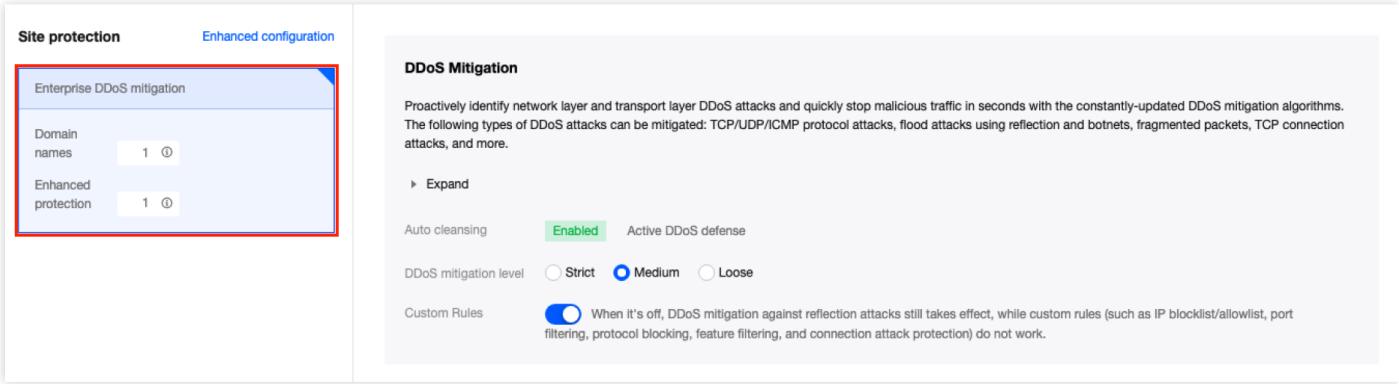

6. (Optional) After the rule is created, it is added to the list. To modify the list of blocked regions, click **Configure** in the "Operation" column on the right.



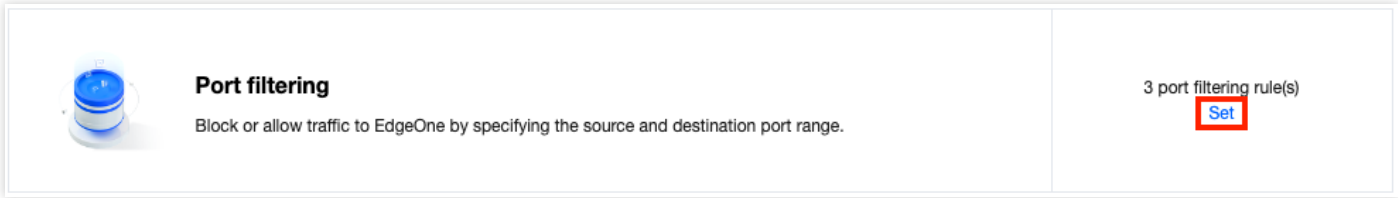

# Port Filtering

Port filtering is a more fine-grained way to restrict client access traffic to your sites in EdgeOne. After it is enabled, you can create a rule by setting the protocol type, source port range, destination port range, and action (**Discard** or **Continue protection**).

1. Log in to the EdgeOne console and select **Security** > **DDoS Mitigation** on the left sidebar.
2. On the left of the **DDoS mitigation** page, select a mitigation business object, such as a **DDoS mitigation Enterprise plan** or **DDoS mitigation Enterprise plan - L4 proxy** instance.



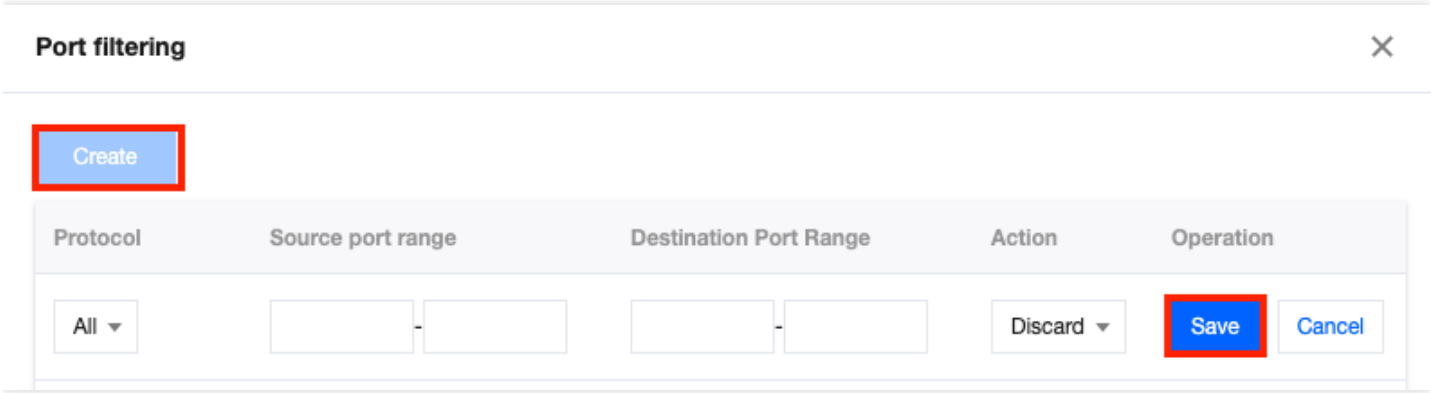

3. Click **Set** in the **Port filtering** section.



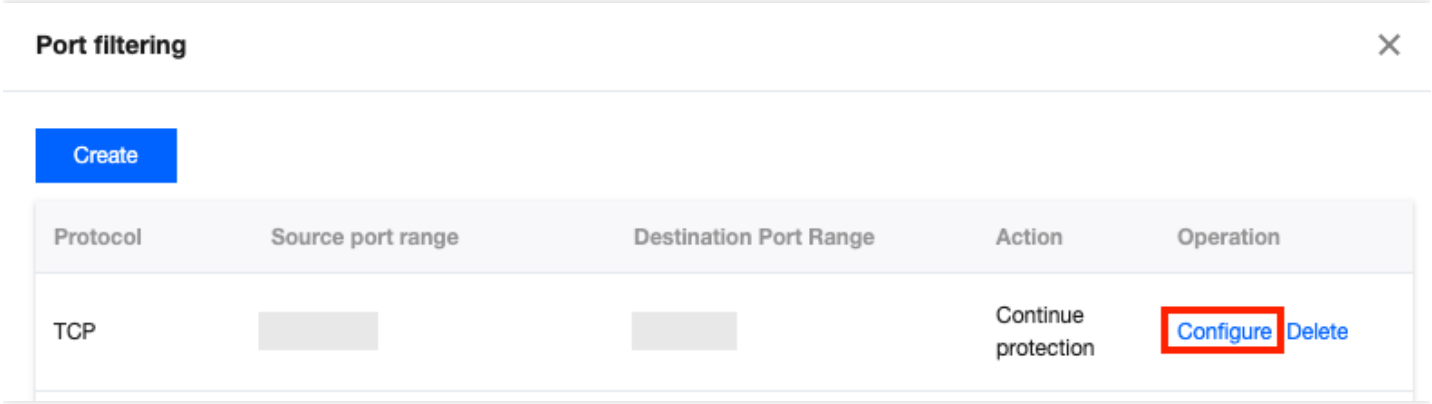

4. On the page that appears, click **Create** to create a rule. Select an action, enter the required fields, and click **Save**.

Note：

- Multiple instances can be created at a time. For instances without protected resources, you cannot create rules.
- For **Priority**, enter an integer between 1 and 1000. A rule with a lower number has higher priority and is listed higher. Default: 10.



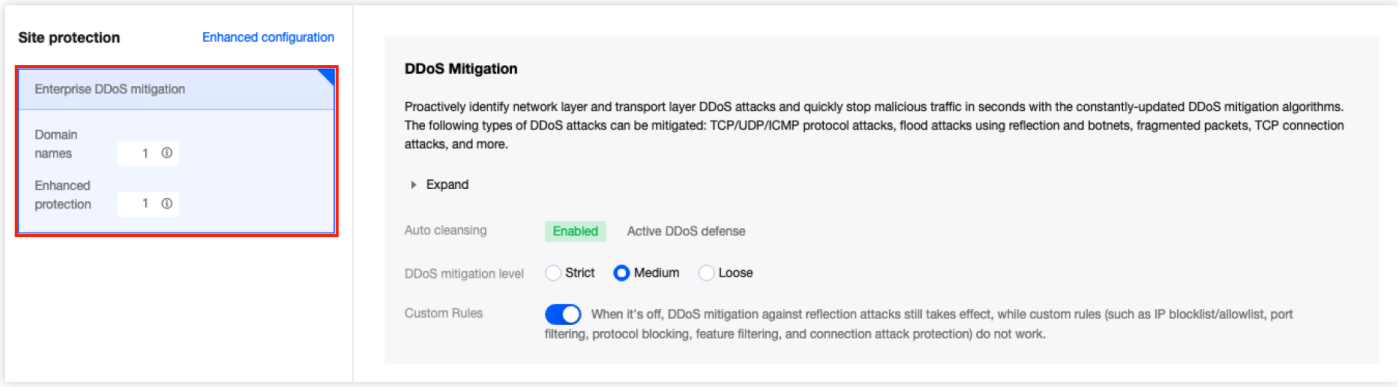

6. (Optional) After the rule is created, it is added to the rule list. To modify it, click **Configure** in the **Operation** column on the right.




# Feature Filtering

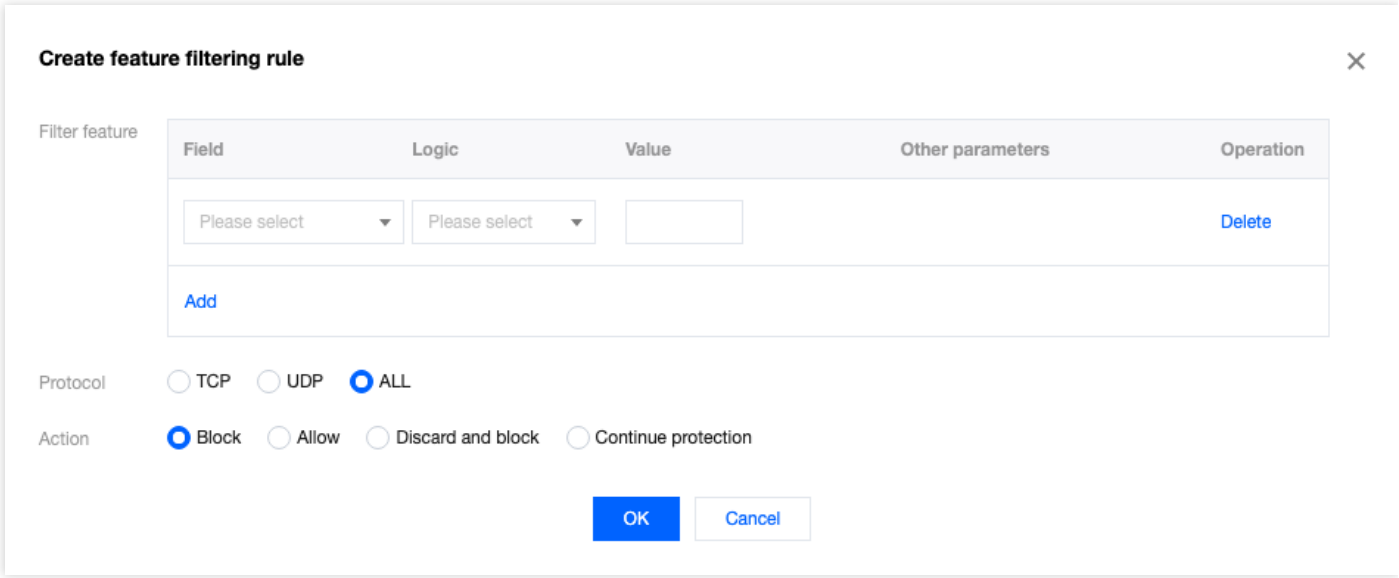
A feature filtering rule allows you to define a number of conditions based on IP, TCP, and UDP headers, payload, source port, destination port, and action (**Discard**, **Allow**, **Discard and block**, or **Continue protection**). After feature filtering is enabled, you can create mitigation rules targeting those specific features.

1. Log in to the EdgeOne console and select **Security** > **DDoS Mitigation** on the left sidebar.
2. On the left of the **DDoS mitigation** page, select a mitigation business object, such as a **DDoS mitigation Enterprise plan** or **DDoS mitigation Enterprise plan - L4 proxy** instance.

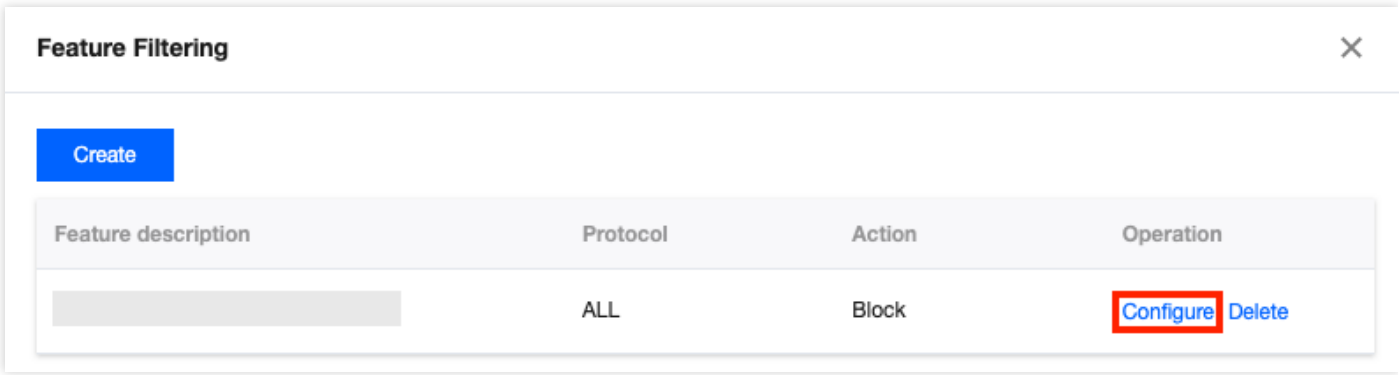



3. Click **Set** in the "Feature filtering" section.


4. On the feature filtering page, click **Create**.
5. In the **Create feature filtering policy** pop-up window, select an action, enter the required fields, and click **OK**.



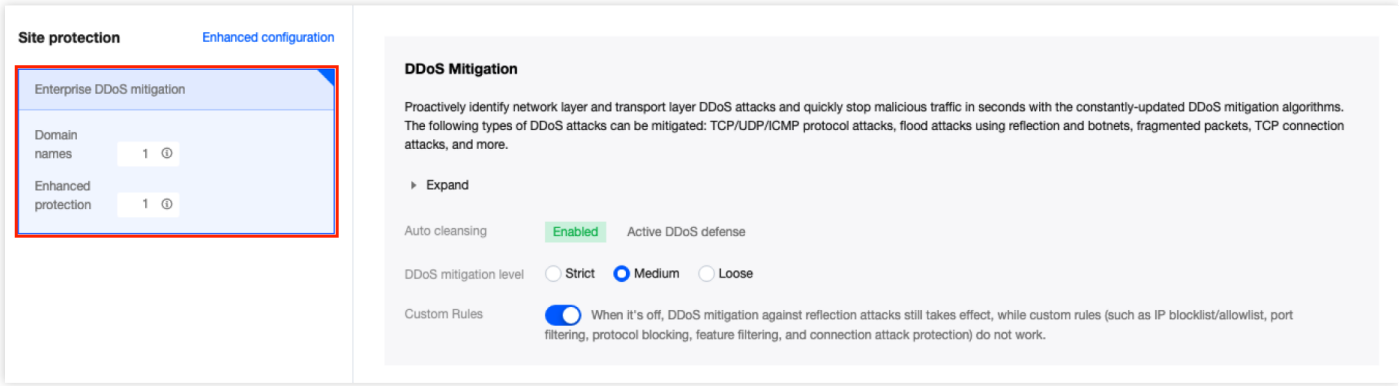

6. (Optional) After the rule is created, it is added to the list. To modify it, click **Configure** in the **Operation** column on the right.




# Protocol Blocking

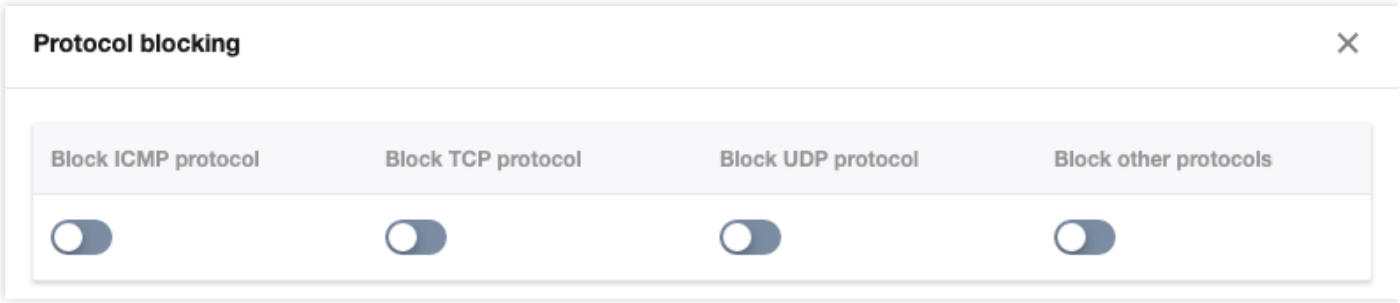
EdgeOne supports blocking inbound traffic based on its protocol type. You can enable **ICMP protocol blocking**, **TCP protocol blocking**, **UDP protocol blocking**, and blocking of other protocols to block their access requests directly. Note that UDP is a connectionless protocol that doesn't provide a three-way handshake process like TCP and thus has security vulnerabilities. We recommend you block UDP if it is not used for your business.

1. Log in to the EdgeOne console and select **Security** > **DDoS Mitigation** on the left sidebar.
2. On the left of the **DDoS mitigation** page, select a mitigation business object, such as a **DDoS mitigation Enterprise plan** or **DDoS mitigation Enterprise plan - L4 proxy** instance.




3. Click **Set** in the "Protocol blocking" section.

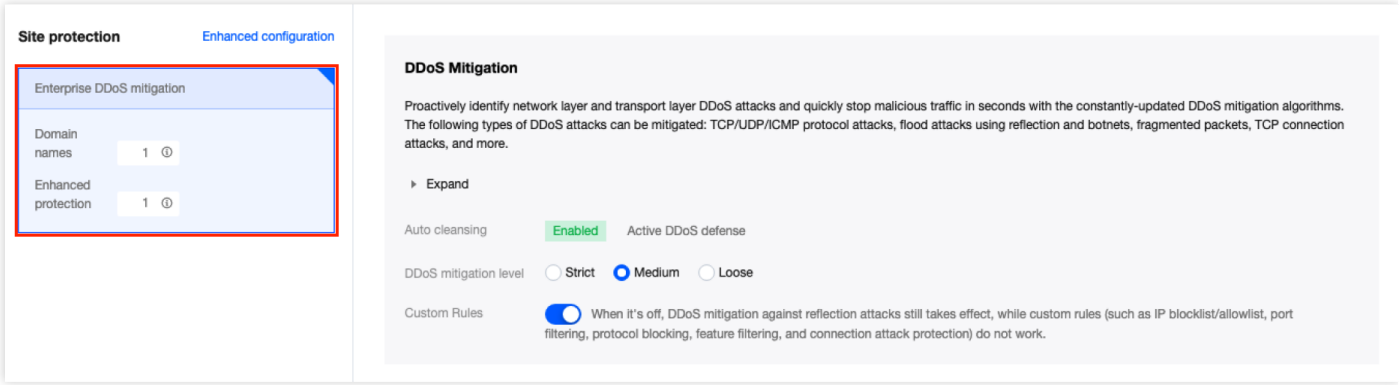
4. On the **Protocol blocking** page, toggle on the target protocol .




# Connection Attack Protection

EdgeOne can provide protection against connection attacks. With **Maximum source IP exceptional connections** enabled, a source IP detected that frequently sends a high number of abnormal connection requests in a short time will be added to the blocklist and be blocked for 15 minutes.

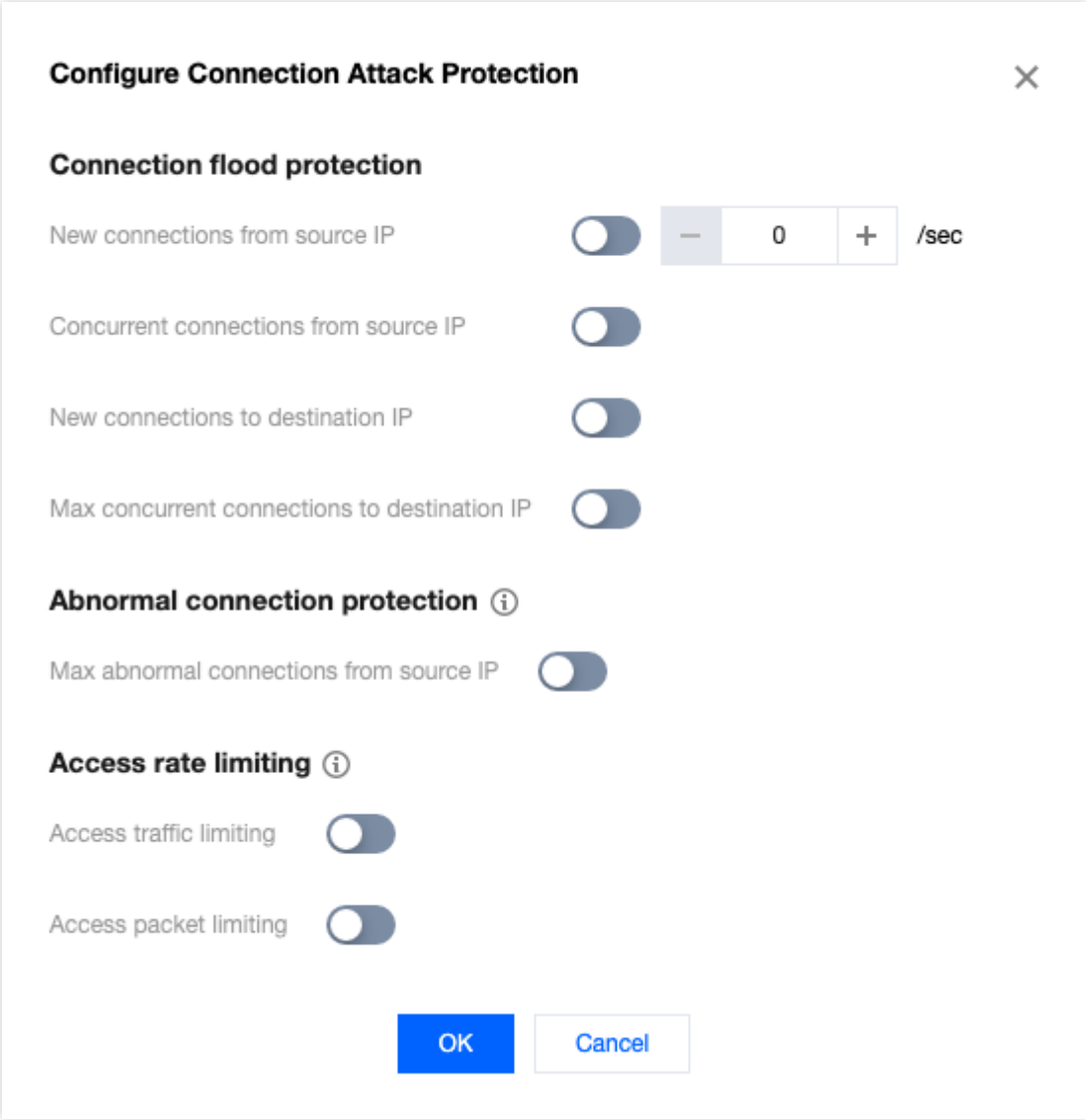
1. Log in to the EdgeOne console and select **Security** > **DDoS Mitigation** on the left sidebar.
2. On the left of the **DDoS mitigation** page, select a mitigation business object, such as a **DDoS mitigation Enterprise plan** or **DDoS mitigation Enterprise plan - L4 proxy** instance.



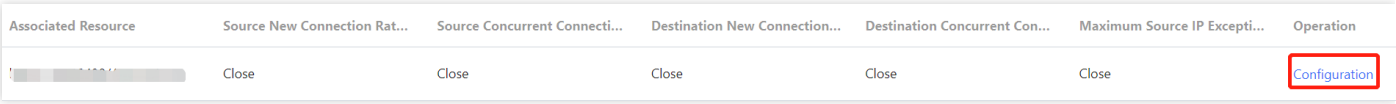

3. Click **Set** in the **Connection attack protection** section to enter the configuration page.


4. On the **Connection attack protection** page, click **Configure**.

5. In the **Configure connection attack protection** pop-up window, enable **Exceptional connection protection** and click **OK**.




6. (Optional) After the rule is created, it is added to the list. To modify the configuration, click **Configure** in the **Operation** column on the right.



# Alarm Notification

Last updated：2022-10-09 09:42:57

## Overview

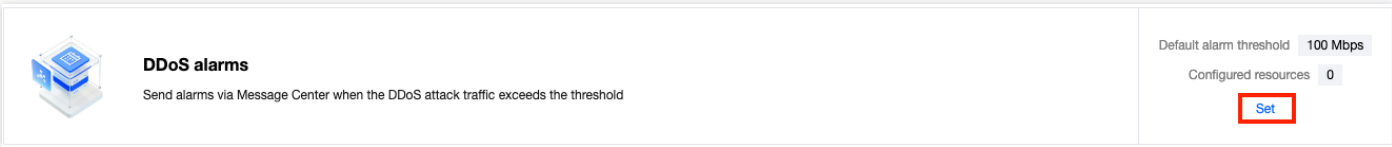
To be notified of DDoS attacks against the DDoS mitigation Enterprise plan (site access and layer-4 proxy services), you can set an alarm threshold based on the minimum DDoS attack rate in the EdgeOne console and configure the corresponding subscription in the Message Center.

Note：

- EdgeOne identifies DDoS attacks by monitoring external access traffic in real time, and automatically cleanses traffic as soon as malicious attack traffic is detected.
- Alarm notifications are pushed only for DDoS attacks against the DDoS mitigation Enterprise plan (site access and layer-4 proxy services). Currently, other businesses don't support the DDoS attack traffic alarming feature.

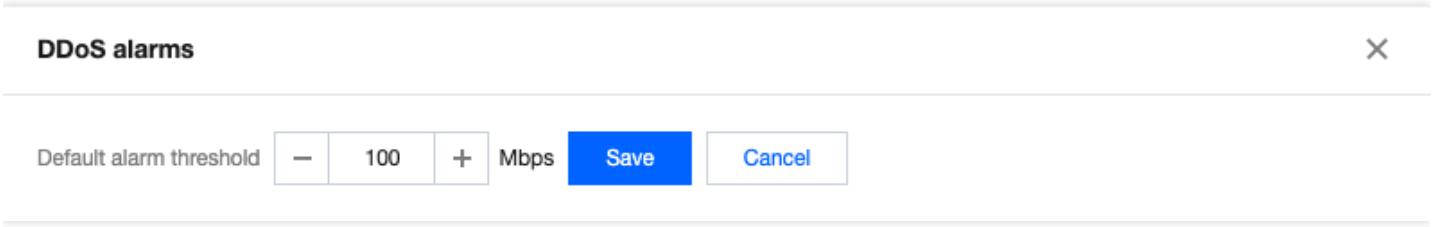
## Directions

1. Log in to the EdgeOne console, select **Security** > **Alarm Notification** on the left sidebar, and select the target site.
2. In the **DDoS attack traffic alarm** section, click **Set**.




3. On the **DDoS attack traffic alarm** page, you can adjust the default global DDoS attack alarm threshold for the current site, and the Message Center will push attack event notifications only when the attack rate exceeds the configured threshold. Click **Edit** of the default alarm threshold, modify the threshold, and click **Save**.

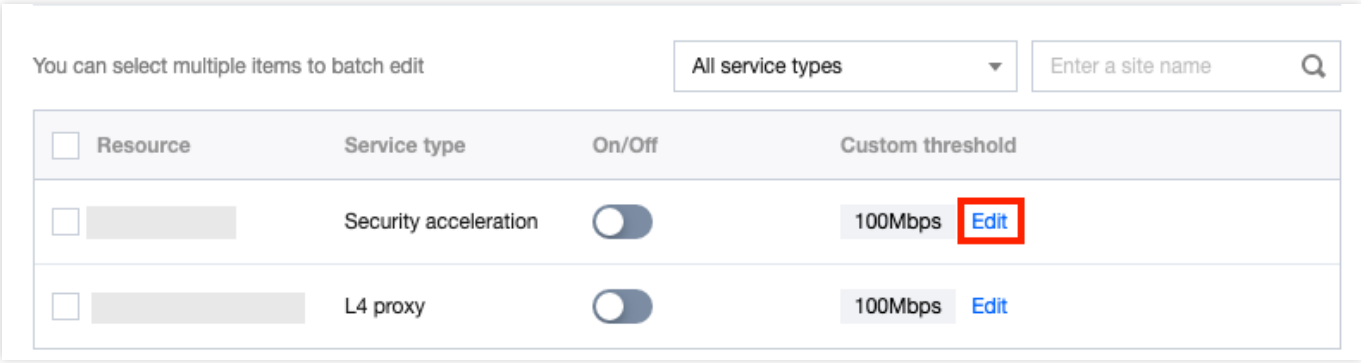
Note：
The **DDoS attack traffic alarm** page displays all objects that can be configured and their custom DDoS alarm thresholds if you have set. For those not configured with custom thresholds, you can modify the **Default alarm threshold**.




4. On the **DDoS attack traffic alarm** page, you can configure the alarm threshold for a security acceleration or layer-4 proxy business project.

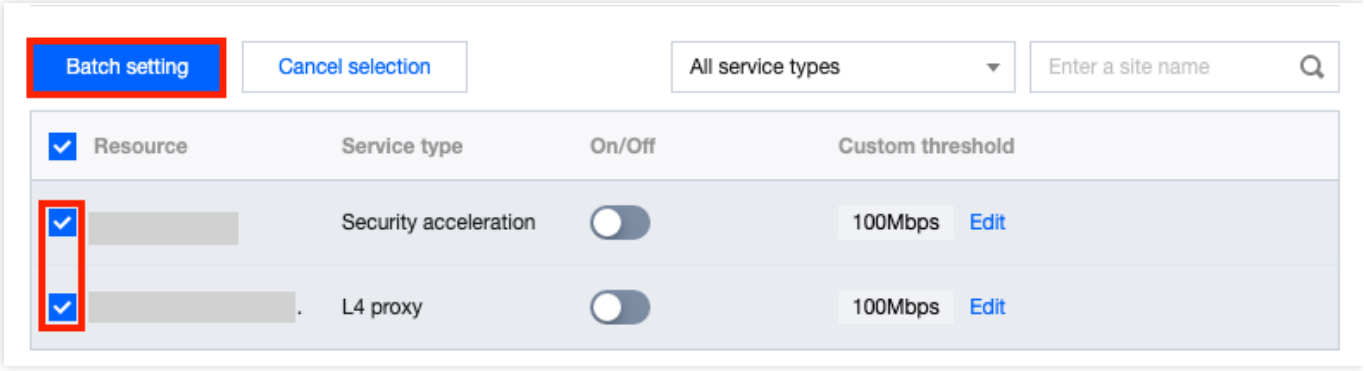
> Note：
> We recommend you adjust the threshold based on the attack frequency and history. It is 100 Mbps by default and can be adjusted to 10 Mbps at the minimum.

- Set a single alarm threshold
  i. Select the target business and click **Edit** in the alarm threshold column to adjust the minimum attack rate above which the business will push DDoS attack notifications.

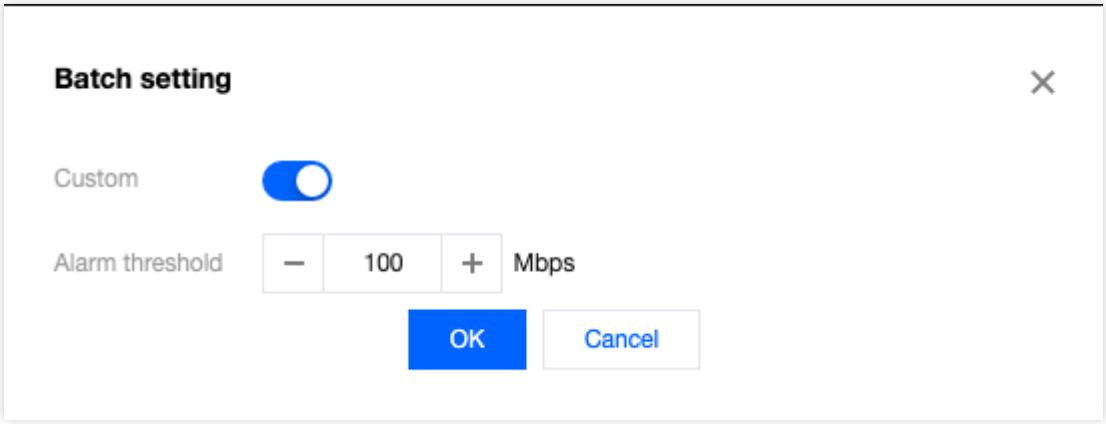



  ii. Modify the alarm threshold, click **Save**, and the custom threshold will be enabled automatically.
- Batch set alarm thresholds

i. Select one or more businesses and click **Batch set**.




ii. Toggle on the custom threshold switch , set the alarm threshold, and click **OK**.



# Origin Protection

Last updated：2022-10-18 10:10:50

## Overview

When Origin Protection is enabled, EdgeOne notifies you of the latest update of intermediate IPs of L4 proxy and site acceleration. You can sync them to the firewall rules of your origin, allowing only traffic from these IPs to your origin.

## Directions

1. Log in to the EdgeOne console. Select **Security Protection** > **Origin Protection** on the left sidebar.

2. On the page that appears, enable **Origin protection**. Select the resources to bind with the intermediate IPs. Click **OK**.

   Note：
   **Select resource**: Select target resources to enable Origin Protection.

3. When origin protection is enabled:

   - You can see the current intermediate IPs. You can update your origin firewall rules accordingly.
   - You will be informed of any updates of the intermediate IPs. Once you confirm the updates and report your update progress, the latest ones will be applied to your associated resources.

## Notes

To ensure the normal running of your business, confirm and update the intermediate IPs in the console as soon as possible after you are notified.

Note：
If the intermediate IPs are not updated, there may be higher latency or instability issues in case of high concurrency.

# FAQs

### Why can't I enable Origin protection for my domain name?

Origin protection only supports domain names with security acceleration enabled.

### How can I enable security acceleration for a domain name?

If your EdgeOne plan supports security acceleration, you can enable advanced protection for a specific domain name in the **Enhanced configuration** card under **DDoS Mitigation**.

### Can I use origin protection for non-security acceleration resources?

No. This feature is not available if your EdgeOne plan does not support security acceleration.

# Certificate Management
# Edge Node Certificate

Last updated：2022-08-01 11:50:08

## Overview

EdgeOne provides a one-stop certificate application, upload, management, and deployment service for site acceleration. This implements centralized management and quick deployment of edge SSL certificates. EdgeOne certificates are divided into the following three types:

- Universal certificate: During NS connection, once a site takes effect, the system will generate a universal certificate for its root domain (example.com) and third-level wildcard domain (*.example.com) and automatically deploy and update it.
- Uploaded custom certificate: It is a certificate you upload in the EdgeOne or SSL Certificates console.
- Tencent Cloud-managed certificate: It is a certificate that you purchase or apply for free of charge in the SSL Certificates console.

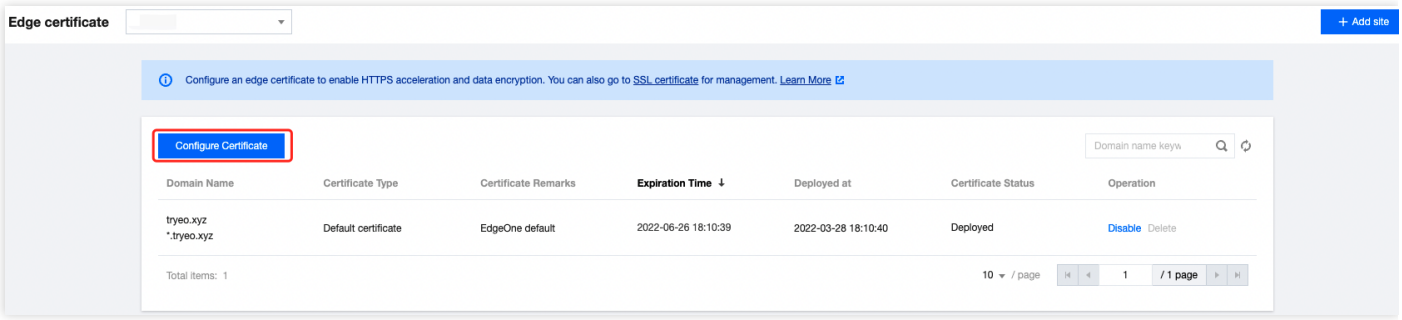
Note：

- Universal certificates are dedicated to the NS connection method and won't be provided by the system during CNAME connection.
- After you switch from NS connection to CNAME connection, the universal certificate will be retained but not updated and will be automatically deleted upon expiration.
- Uploaded custom certificates and Tencent Cloud-managed certificates in EdgeOne are synced with those in the SSL Certificates console.

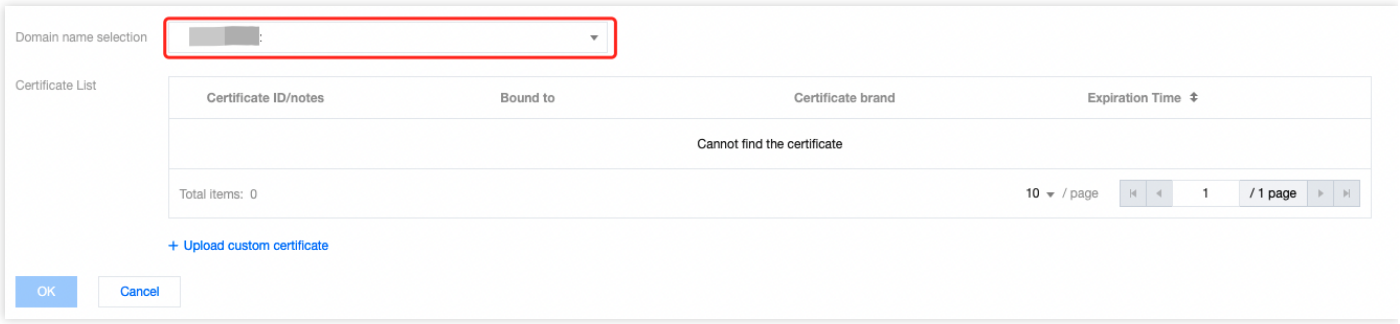
## Directions

1. Log in to the EdgeOne console and click **Certificate management** > **Edge node certificate** on the left sidebar.

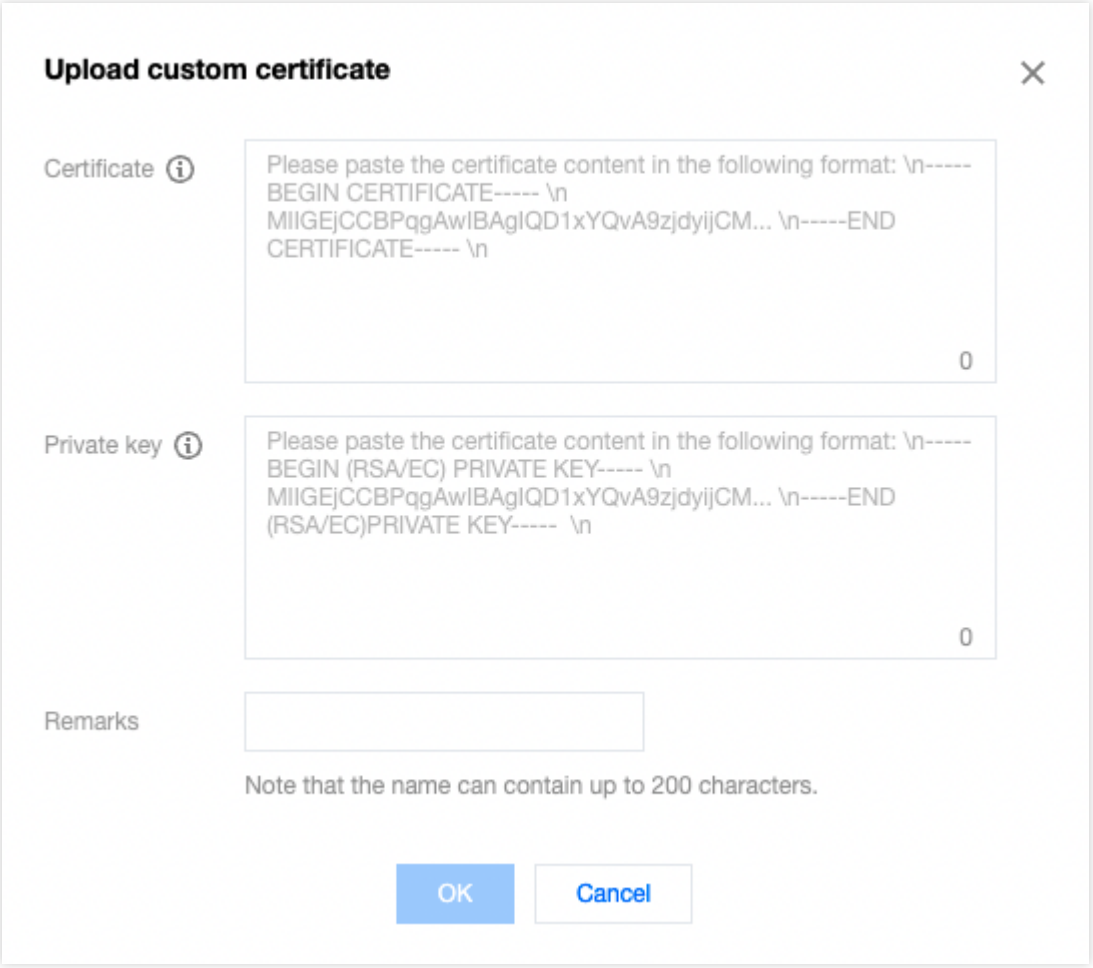
2. On the edge node certificate page, select the target site and click **Configure certificate**.




3. On the certificate configuration page, select the target domain, and certificates in the SSL Certificates console that can be associated with the domain will be automatically displayed in the certificate list.



4. If there are no available certificates, you can click **Upload custom certificate** to upload one.




5. Select the target certificate and click **OK**. Then, the certificate will be automatically deployed to EdgeOne acceleration nodes.

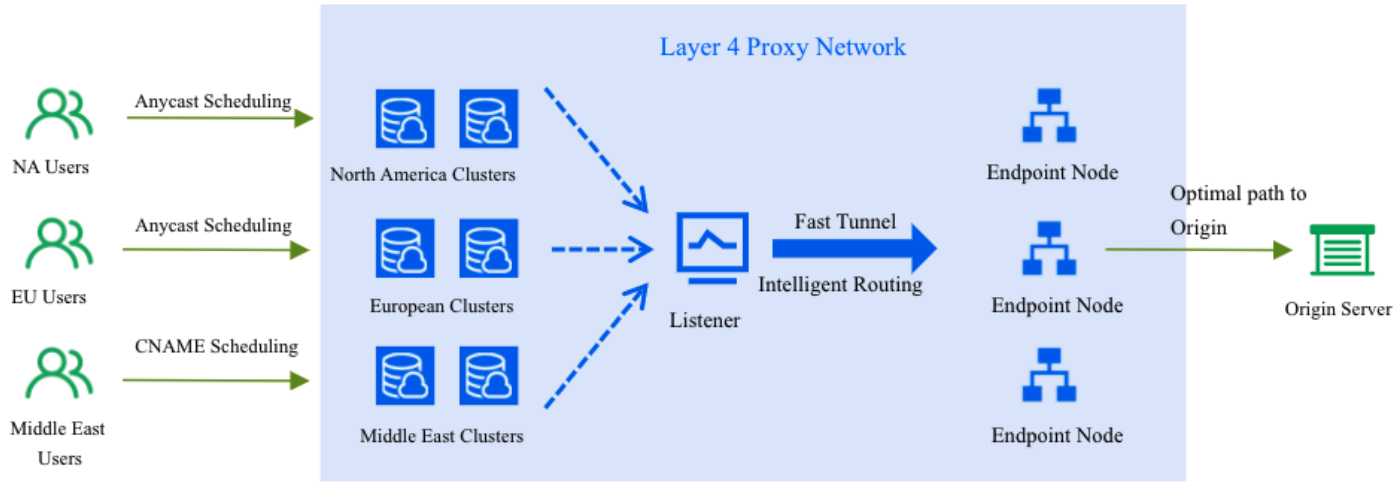
> Note：
> If the domain has been associated with a certificate, reassociation will overwrite the old certificate.

# L4 Proxy

Last updated：2022-08-26 11:45:48

## Overview

L4 proxy provides customer-grade DDoS protection and layer-4 acceleration services for TCP/UDP applications. By leveraging widely distributed layer-4 proxy nodes, unique DDoS module, and smart routing technology, EdgeOne implements nearby access for end users, edge traffic cleansing, and port monitoring and forwarding. It thus offers high-availability and low-latency security and acceleration services for layer-4 applications.



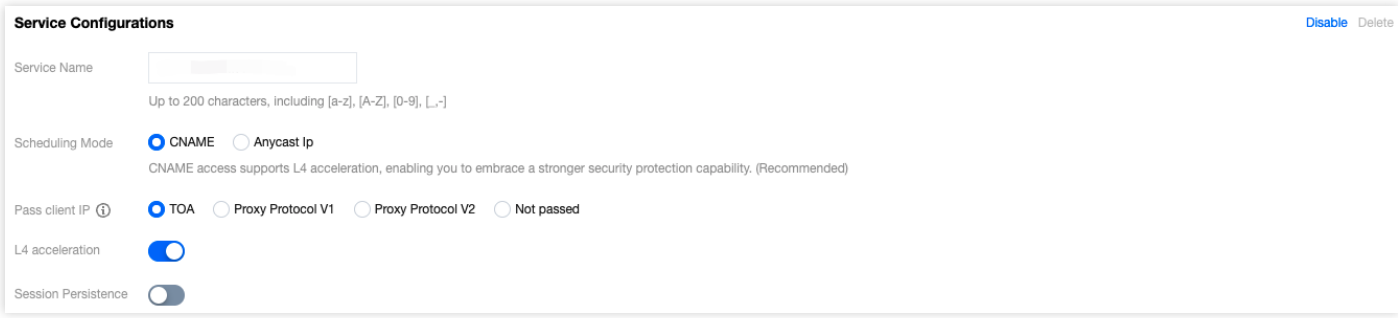

Note：

- The EdgeOne console is not yet fully available. To access the console, please contact us for activation.
- Only one L4 proxy can be created for each site. To create multiple proxies, please contact us.
- L4 proxy provides customer-grade DDoS protection capability by default, which cannot be disabled.
- L4 proxy currently doesn't support IPv6 origin servers.

## Creating a L4 proxy

1. Log in to the EdgeOne console. Click **L4 Proxy** on the left sidebar.
2. On the page that appears, select the target site and click **Create L4 proxy**.

3. On the L4 proxy creation page, set **Service configurations** parameters.




**Parameter description:**

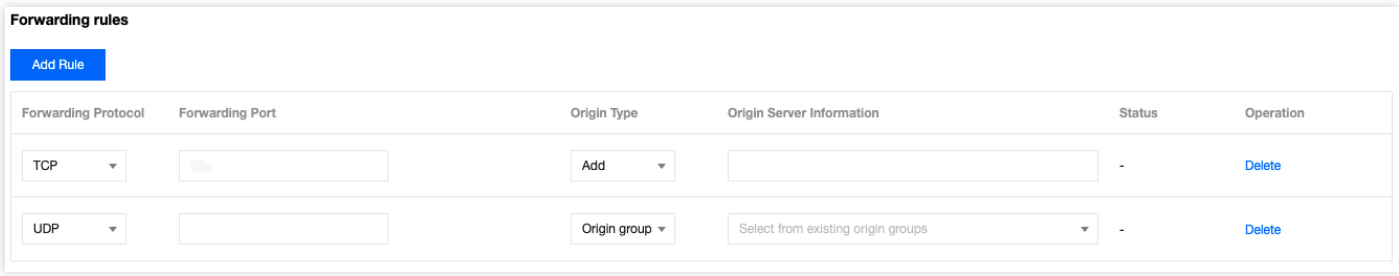
- Service name: Name of the layer-4 proxy instance. The number of instances that can be created is subject to the site package.
- Scheduling mode: Select the method of connecting the layer-4 proxy service.
  - CNAME (recommended): A CNAME record is used as the connection address, which supports stronger DDoS protection, nearby access and acceleration as well as L4 forwarding and acceleration.
  - Anycast IP: An Anycast IP is used as the connection address, which supports DDoS protection and L4 forwarding and acceleration.

> Note：
> If site acceleration is also enabled for the host, the scheduling mode can only be set to "CNAME".

- Proxy mode: Configure the layer-4 proxy mode.
  - DDoS protection: Enable layer-3 and layer-4 DDoS protection by default. To disable it, you can go to DDoS Protection to modify the default DDoS policy.
  - L4 acceleration: Provide L4 acceleration and reduce network transmission delay. You can choose to enable or disable it.

4. On the L4 proxy service creation page, click **Add rule** and configure **Forwarding rules** parameters.

> Note：
> You can add up to 100 forwarding rules for each L4 proxy.




**Parameter description:**

- Forwarding protocol: TCP and UDP are supported.
- Forwarding port: The supported port range is 1–64999, excluding 36000 and 56000. You can enter multiple ports separated with commas or use a hyphen to enter a port range. You can enter up to 20 ports in a forwarding rule.

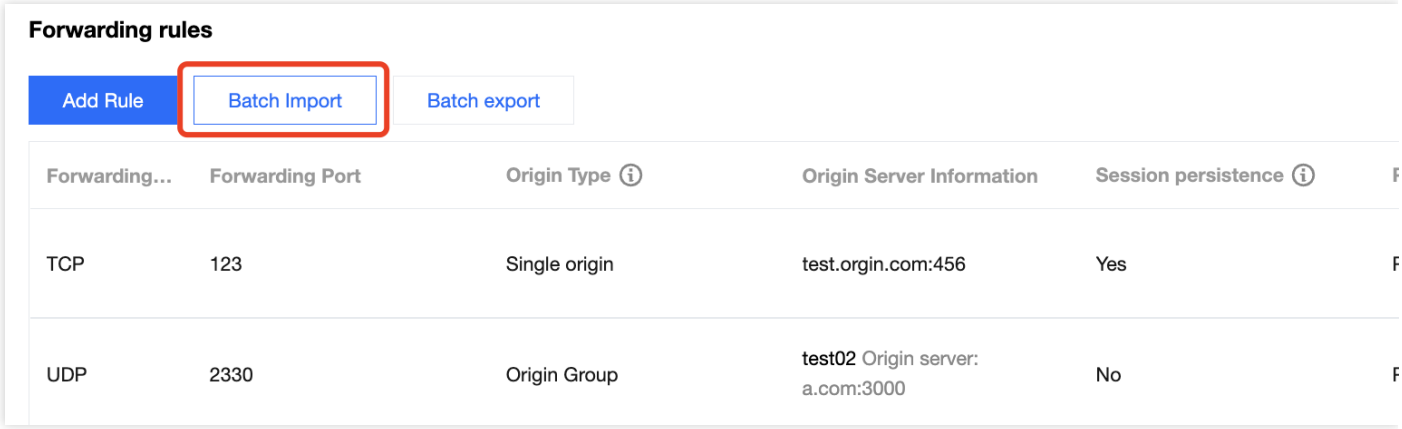
  > Note：
  > If site acceleration is also enabled for the host, forwarding ports 80 and 443 are not supported.

- Origin server type/information:
  - Single origin: You can enter one or more origin servers in the format of **origin server address:port** and separate them with commas.
  - Origin group: Select origin servers from an existing origin group. You can only select an origin group with origin-pull port information or create one here.
- Pass client IP: Specify how real client IPs will be carried when layer-4 proxy nodes are used for origin-pull.
  - TOA: Pass client IPs via TCP Option (type 200), which only supports TCP protocols.
  - Proxy Protocol V1 (recommended): Pass client IPs as plaintext via the TCP header, which only supports TCP protocols.
  - Proxy Protocol V2: Client IPs will be transferred through the header. V2 uses the binary format and supports both TCP and UDP protocols. Each data packet carries a PPv2 header for TCP, while only the first data packet carries the header for UDP.
  - Not passed: Real client IPs will not be transferred.
- Session persistence: As long as an origin server IP remains unchanged, traffic from the same client IP will always be forwarded to it.

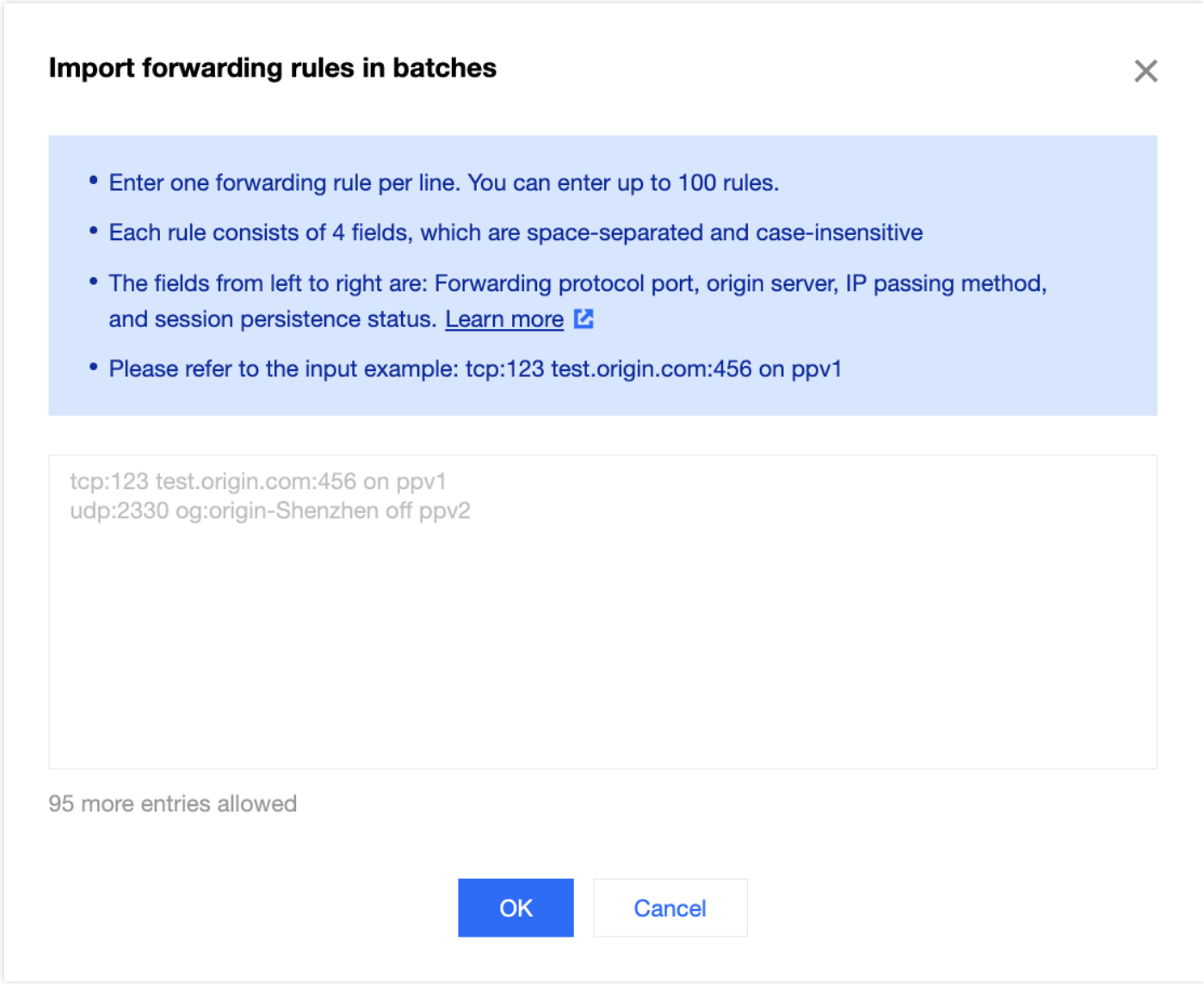
# Importing Forwarding Rules in Batches

When you create or view a L4 proxy, forwarding rules can be imported in batches.

1. Log in to the EdgeOne console. Click **L4 Proxy** on the left sidebar.
2. On the page that appears, select the target site and click **Create L4 proxy**.
3. In the forwarding rules module of the L4 proxy creation page, click **Batch import**.



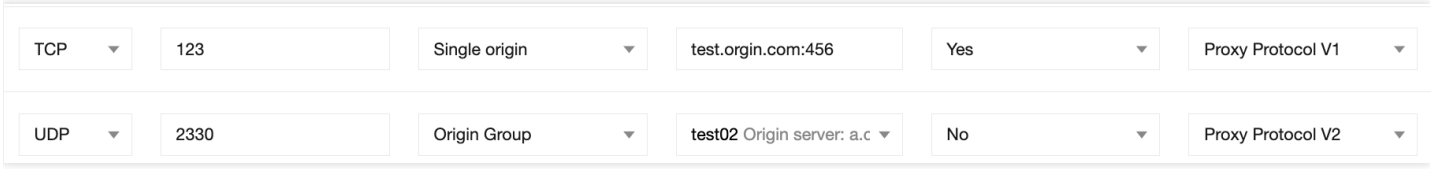
4. In the batch import window, enter the required rules and click **Submit**.




- Batch import format description:
  - Up to 100 forwarding rules can be entered, one rule per line.
  - Each line contains 4 fields that are space-separated and case-insensitive.
  - The fields from left to right are listed as below:
  - Forwarding protocol:Port: For example, `tcp:123` .
  - Origin server: Enter a single origin server in the format of `test.origin.com:456` , or an origin group in the format of `og:OriginGroupName` .
  - Session persistence status: `on` or `off` .
  - IP passing method: `TOA` , `PPv1` , `PPv2` , or `off` .
- Sample request:

```
tcp:123 test.origin.com:456 on ppv1
udp:2330 og:l4testkb off ppv2
```

The configuration is shown as below:



# Site Acceleration
# Access Control
# Token Authentication

Last updated：2023-02-22 17:28:26

## Overview

As an access control policy, token authentication supports creating rules to validate access and filter out unauthorized access requests. This effectively prevents your site resources from being maliciously hotlinked and thus protects your business.

**How does token authentication implement access control?**
An authentication URL is generated based on the request URL and specified rule settings. When the node receives an access request, it does not serve resources until the authentication URL is validated successfully. Otherwise, the request is denied with a 403 error.

## Directions

1. Log in to the EdgeOne console. Click **Rule Engine** on the left sidebar.
2. On the page that displays, select the target site and create rules for token authentication as needed. For more information, see Overview.

| Parameter | Description |
| --- | --- |
| Method | Choose one of four available authentication methods. For more information, see Authentication Methods. |
| Primary key | A primary authentication key must be between 6-40 characters and contains letters and numbers. |
| Secondary key | A secondary authentication key must be between 6-40 characters and contains letters and numbers. |
| Authentication parameter | An authentication parameter must be between 1-100 characters and contains letters, numbers and underscores. The parameter value will be authenticated by nodes. |

| Parameter | Description |
| --- | --- |
| Validity period | Validity period of the authentication URL (1-630720000 seconds). It determines whether a client request is valid:<br>• If the time "timestamp + validity period" is reached, the request is considered expired and a 403 is returned.<br>• If it is not reached, the request is considered valid and will be authenticated. |

# Authentication Methods

## Method A

### Authentication URL format

```
http://Hostname/Filename?sign=timestamp-rand-uid-md5hash
```

### Field description

| Field | Description |
| --- | --- |
| Hostname | Site domain name. |
| Filename | Path to access the resource, which must start with "/". |
| sign | Custom name of the authentication parameter. |
| timestamp | Unix timestamp.<br>Format: A positive decimal integer, indicating the number of seconds elapsed since 00:00:00, January 1, 1970 at UTC. It does not change regardless of your time zone. |
| rand | Random string, which contains letters and digits. Length: 0–100. |
| uid | User ID (not in use), which defaults to 0. |
| md5hash | A fixed-length 32-bit string calculated with the MD5 algorithm:<br>• Authentication algorithm: MD5 (/Filename-timestamp-rand-uid-key)<br>• Authentication logic: When receiving a valid request, the node starts comparing this string value with the `md5hash` value in the request URL. If they match, the node will respond to the request after it is authenticated, otherwise it returns a 403. |

## Method B

#### Authentication URL format

```
http://Hostname/timestamp/md5hash/Filename
```

#### Field description

| Field | Description |
| --- | --- |
| Hostname | Site domain name. |
| Filename | Path to access the resource, which must start with "/". |
| timestamp | Timestamp.<br>Format: YYYYMMDDHHMM (represented in UTC+8), such as 201807301000. |
| md5hash | A fixed-length 32-bit string calculated with the MD5 algorithm:<br>• Authentication algorithm: MD5 (key + timestamp + /Filename)<br>• Authentication logic: When receiving a valid request, the node starts comparing this string value with the `md5hash` value in the request URL. If they match, the node will respond to the request after it is authenticated, otherwise it returns a 403. |

### Method C

#### Authentication URL format

```
http://Hostname/md5hash/timestamp/Filename
```

#### Field description

| Field | Description |
| --- | --- |
| Hostname | Site domain name. |
| Filename | Path to access the resource, which must start with "/". |
| timestamp | Unix timestamp.<br>Format: A positive hex integer, indicating the number of seconds elapsed since 00:00:00, January 1, 1970 at UTC. It does not change regardless of your time zone. |
| md5hash | A fixed-length 32-bit string calculated with the MD5 algorithm:<br>• Authentication algorithm: MD5 (key + /Filename + timestamp). Note that you should remove the identifier 0x from a hex timestamp before calculation.<br>• Authentication logic: When receiving a valid request, the node starts comparing this string value with the `md5hash` value in the request URL. If they match, the node will respond to the request after it is authenticated, otherwise it returns a 403. |

### Method D

#### Authentication URL format

```
http://Hostname/Filename?sign=md5hash&t=timestamp
```

#### Field description

| Field | Description |
| --- | --- |
| Hostname | Site domain name. |
| Filename | Path to access the resource, which must start with "/". |
| sign | Custom name of the authentication parameter. |
| t | Custom name of the timestamp parameter. |
| timestamp | Unix timestamp.<br>Format: A positive decimal/hex integer, indicating the number of seconds elapsed since 00:00:00, January 1, 1970 at UTC. It does not change regardless of your time zone. |
| md5hash | A fixed-length 32-bit string calculated with the MD5 algorithm:<br>• Authentication algorithm: MD5 (key + /Filename + timestamp). Note that you should remove the identifier 0x from a hex timestamp before calculation.<br>• Authentication logic: When receiving a valid request, the node starts comparing this string value with the `md5hash` value in the request URL. If they match, the node will respond to the request after it is authenticated, otherwise it returns a 403. |

## Configuration Sample

The following configuration sample shows how to authenticate a request for `http://www.example.com/test.jpg` with Method A:


#### Getting authentication parameters

- /Filename: `/foo.jpg`

- imestamp: `1647311432` . The timestamp is returned as a 10-digit positive decimal integer indicating that the authentication URL is generated at 10:30:32, March 15, 2022 (UTC+8).
- rand: `J0ehJ1Gegyia2nD2HstLvw`
- uid： `0`
- key: `3C9mxSGzc8ZadmGNzE`
- md5hash: MD5 (/Filename-timestamp-rand-uid-key) = MD5 ( `/foo.jpg` - `1647311432` - `J0ehJ1Gegyia2nD2HstLvw` - `0` - `3C9mxSGzc8ZadmGNzE` ) = ecce3150cbdaac83b116d937777ca77f

#### Generating an authentication URL

`http://www.example.com/foo.jpg?sign=1647311432-J0ehJ1Gegyia2nD2HstLvw-0-ecce3150cbdaac83b116d937777ca77f`

#### Authenticating the request

After the request is initiated via an encrypted URL, the node parses the value of the "timestamp" parameter from the URL to determine whether the request is valid:

- *1*If the time "timestamp + validity period" is reached, the request is considered expired and a 403 is returned.
- *2*If the time "timestamp + validity period" is not reached, the request is considered valid and will be authenticated.
- *3*The node compares the calculated `md5hash` value with the `md5hash` value in the request URL. If they match, the node will respond to the request after it is authenticated, otherwise it returns a 403.

## Must-knows

1. If the authentication succeeds, the authentication parameters in the request URL will be ignored during origin-pull and used as the cache key to increase the cache hit rate.
2. If the authenticated request does not hit the node cache, the request will be forwarded to the origin to retrieve resources. The authentication parameters in the authentication URL (which is identical as the origin-pull URL in this case) can either be used to authenticate again or ignored as needed by setting origin-pull request parameters.
3. The origin-pull request URL cannot contain any Chinese characters.

# Video Dragging

Last updated：2023-02-22 17:28:26

## Overview

Video dragging can be enabled to specify the start point of a video. Only MP4, FLV and TS files are supported.

## Use Cases

Video dragging generally happens in VOD scenarios. When a user drags the video progress bar, a request similar to the one as shown below will be sent to the server:

```
http://www.test.com/test.flv?start=10
```

In this case, data will be returned starting from the 10th byte. VOD files are all cached on nodes, so the nodes can directly respond to such requests once this configuration is enabled.

## Notes

- The origin must support Range requests, or the origin-pull may fail.
- You can optimize node cache with query string. A video URL may carry different query strings. When it's cached with the query strings, even for the same requested resource, multiple cache IDs will be generated (due to different query strings), resulting in multiple origin-pull requests for the same resource. For more information, see Query String.
- Supported file formats: MP4, FLV and TS.

| File Type | Meta Information | Start Parameter | Request Sample |
| --- | --- | --- | --- |
| MP4 | The meta information must be included in the file header, instead of at the end of the file. | The parameter `start` specifies a time point (in seconds) and indicates milliseconds with decimals. For example, "start = 1.01" means that the start time is 1.01s. Nodes will locate the last keyframe before the time specified by `start` if `start` is not a keyframe. | `http://www.test.com/demo.mp4?start=10` indicates that the video plays from the 10th second. |

| File Type | Meta Information | Start Parameter | Request Sample |
| --- | --- | --- | --- |
| FLV | The video on the origin must contain meta information. | The parameter `start` specifies a byte. Nodes will automatically locate the last keyframe before the byte specified by `start` if `start` is not a keyframe. | `http://www.test.com/demo.flv?start=10` indicates that the video plays from the 10th byte. |
| TS | No special requirements | The `start` parameter specifies a start byte. Nodes will automatically locate the byte at the beginning. | `http://www.test.com/demo.ts?start=10` indicates that the video plays from the 10th byte. |

## Directions

1. Log in to the EdgeOne console. Click **Rule Engine** on the left sidebar.
2. On the page that displays, select the target site and create rules for video dragging as needed. For more information, see Overview.

# Smart Acceleration

Last updated：2023-03-08 11:46:26

## Overview

Smart acceleration refers to smart dynamic routing acceleration. After this feature is enabled, it will detect the node network latency in real time and use the smart algorithm to select the optimal transfer path, so as to handle both static and dynamic client requests more quickly, stably, and securely.
Smart dynamic routing minimizes problems such as high network latency, connection errors, and request failures.

#### What are dynamic and static resources?

Static resource: If a user accesses a resource for multiple times and the content returned remains the **same** each time, then the resource is a static resource. For example, images, video, software installation packages, compressed packages, and the following types of files are static resources: HTML, CSS, JS, and APK files.
Dynamic resource: If a user accesses a resource for multiple times and the content returned **changes** each time, then the resource is a dynamic resource. For example, APIs and the following types of files are dynamic resources: JSP, ASP, PHP, PERL, and CGI files.

## Use Cases

#### Dynamic resource acceleration

Smart acceleration can be used for businesses with frequent requests to dynamic resources and a high sensitivity to latency, including online game, ecommerce, finance, payment, and online education.

#### Dynamic/Static hybrid resource acceleration

Dynamic resources are as detailed above. Static resources are cached on edge nodes close to clients for fast response. If a cached static resource expires, it can be updated quickly through smart acceleration.

## Directions

### Global configuration

1. Log in to the EdgeOne console and choose **Site Acceleration** > **Smart Acceleration** on the left sidebar.
2. On the page that appears, select the target site, and enable or disable the feature.

### Differentiated configuration

To create an individual configuration for subdomains, URL paths, or file extensions, you can switch to the rule engine page.

1. Click **Rule Engine** on the left sidebar.
2. For more information, see Rule Engine.

## Billing Overview

As smart acceleration is a value-added service, it incurs additional usage fees. Before enabling the service, read the billing description in Billing Overview.

# Cache Configuration
# Query String

Last updated：2023-03-08 11:46:26

## Overview

You can adjust the query string in resource URLs to optimize the node cache and load requested resources more quickly.

**How does the query string affect the node cache?**

The query string is the string (containing one or multiple parameters separated with `&`) after `?` in the request URL, such as `color=blue&size=large` in `https://www.example.com/images/example.jpg?color=blue&size=large`.

When a node responds to a resource request, it will use the complete request URL as the cache key to match the cached resource. For example, even though the two request URLs of `https://www.example.com/images/example.jpg?time=1` and `https://www.example.com/images/example.jpg?time=2` have the same path, as they carry different query strings, the node will cache the `example.jpg` image twice and match two node caches for the requests respectively. If the resource is not on the node, the request will be forwarded for origin-pull, which increases the origin-pull traffic.

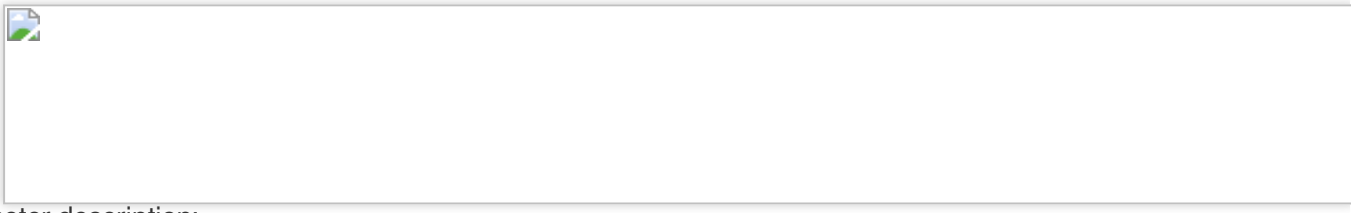
If `example.jpg` does not vary by query string parameters (that is, `example.jpg` will match the same image even if the `time` parameters are different), you can ignore the entire query string in the two request URLs to unify the requests to match the same node cache. For example, both `https://www.example.com/images/example.jpg?time=1` and `https://www.example.com/images/example.jpg?time=2` match the cached resource `https://www.example.com/images/example.jpg`.

Check the impact of the query string on resources in business resource URLs and use the **query string** feature to optimize the cache accordingly.

## Directions

### Global configuration

1. Log in to the EdgeOne console and choose **Site Acceleration** > **Cache Configuration** on the left sidebar.
2. On the page that appears, select the target site and click **Settings** in the query string module. In the pop-up window, select a mode.



Parameter description:

Retain all (default configuration): The complete query string will be retained, and once the query string changes, the request URL will be considered different.

**Note**

In which cases are query strings considered different?

They have a different parameter value, such as `?sign=x;time=y` and `?sign=z;time=y`.

They have the same parameter values but their parameters are in different orders, such as `?sign=x;time=y` and `?time=y;sign=x`.

They have the same parameter values in different letter cases, such as `?sign=A` and `?sign=a`. If you want to identify them as the same query string, you can enable the case ignoring feature.

Ignore all: The entire query string will be ignored.

Retain specified parameters: Only specified parameters in the query string will be retained.

You can specify only parameter names and must separate them with semicolons (;), such as sign;time.

You can enter up to 10 parameters.

Ignore specified parameters: Only specified parameters in the query string will be ignored.

You can specify only parameter names and must separate them with semicolons (;), such as sign;time.

You can enter up to 10 parameters.

### Differentiated configuration

To create an individual configuration for subdomains, URL paths, or file extensions, you can switch to the rule engine page.

1. Click **Rule Engine** on the left sidebar.
2. For more information, see Rule Engine.

## Must-Knows

1. This feature doesn't affect origin-pull request URLs and only changes the cache key of request on nodes. The origin-pull request URLs are the same as the URLs of original requests initiated by clients.

2. If different parameters in the query string in request URLs are separated with characters other than ampersands (&), they cannot be identified normally.

## Sample Configuration

1. If the resources requested from the site `example.com` do not vary by the `time` parameter in query strings, you need to ignore the `time` parameter. The configuration is as follows:

In this case, the `time` parameter is ignored when resources are obtained from the cache for the `https://www.example.com/images/example.jpg?time=1` and `https://www.example.com/images/example.jpg?time=2` requests. That is, the cached resource `https://www.example.com/images/example.jpg` will be returned for both requests.

2. If the resources requested from the site `example.com` vary by only the `size` parameter in query strings, you need to retain the `size` parameter. The configuration is as follows:

In this case, the `size` parameter is retained when resources are obtained from the cache for the `https://www.example.com/images/example.jpg?size=small&color=blue` and `https://www.example.com/images/example.jpg?size=large&color=blue` requests. That is, the cached resources `https://www.example.com/images/example.jpg?size=small` and `https://www.example.com/images/example.jpg?size=large` will be respectively returned for the two requests.

# Case Ignoring

Last updated：2023-03-08 11:46:26

## Overview

You can choose to or not to ignore the letter case of client request URLs as needed to optimize the node cache and load requested resources more quickly.

**How does the letter case affect node cache?**

When a node responds to a resource request, it will use the complete request URL as the cache key to match the cached resource and follow the letter case of the original request URL. Even if URLs in different letter cases have the same content, they will match different node caches. For example, `https://www.example.com/images/demo.JPG` and `https://www.example.com/images/demo.jpg` will be identified as different resource requests. If the resource is not on the node, the request will be forwarded for origin-pull, which increases the origin-pull traffic.

If `demo.jpg` does not vary by letter case (that is, even if in different letter cases, `demo.jpg` indicates the same image), then you can ignore the letter case to unify the requests to match the same node cache. For example, both `https://www.example.com/images/demo.jpg` and `https://www.example.com/images/demo.JPG` match the cached resource `https://www.example.com/images/demo.jpg`.

Check the impact of the letter case on resources in business resource URLs and use the **case ignoring** feature to optimize the cache accordingly.

## Directions

### Global configuration

1. Log in to the EdgeOne console and choose **Site Acceleration** > **Cache Configuration** on the left sidebar.
2. On the page that appears, select the target site and toggle the case ignoring feature on or off.

**Parameter description:**

Off (default): Request URLs are case-sensitive. Even if URLs in different letter cases have the same content, they will still be considered different resources.

On: Request URLs are case-insensitive. URLs with the same content but in different letter cases will be considered the same resource.

### Differentiated configuration

To create an individual configuration for subdomains, URL paths, or file extensions, you can switch to the rule engine page.

1. Click **Rule Engine** on the left sidebar.
2. For more information, see Rule Engine.

## Must-Knows

This feature doesn't affect origin-pull request URLs and only changes the cache key of request on nodes. The origin-pull request URLs are the same as the URLs of original requests initiated by clients.

# Custom Cache Key

Last updated：2023-02-22 17:28:26

## Overview

A cache key can be customized to suit your needs by setting the query string, HTTP header and URL case, so that requested resources can be loaded faster.

**Cache key**

A cache key identifies a resource cached on the node. When a resource is requested from the node, it searches for a match in the cache using the complete request URL as the cache key. For example, resources of the URLs `https://www.example.com/images/example.jpg?key1=value1` and `https://www.example.com/images/example.jpg?key2=value2` are identified by their respective query strings and cache keys.

## Use Cases

Use custom cache keys when you want the resources to be served based on the characteristics of client requests, such as the URL query string, URL case, HTTP headers and request protocol.

## Directions

1. Log in to the EdgeOne console. Click **Rule Engine** on the left sidebar.
2. On the page that displays, select the target site and create rules to configure custom cache keys as needed. For more information, see Overview.

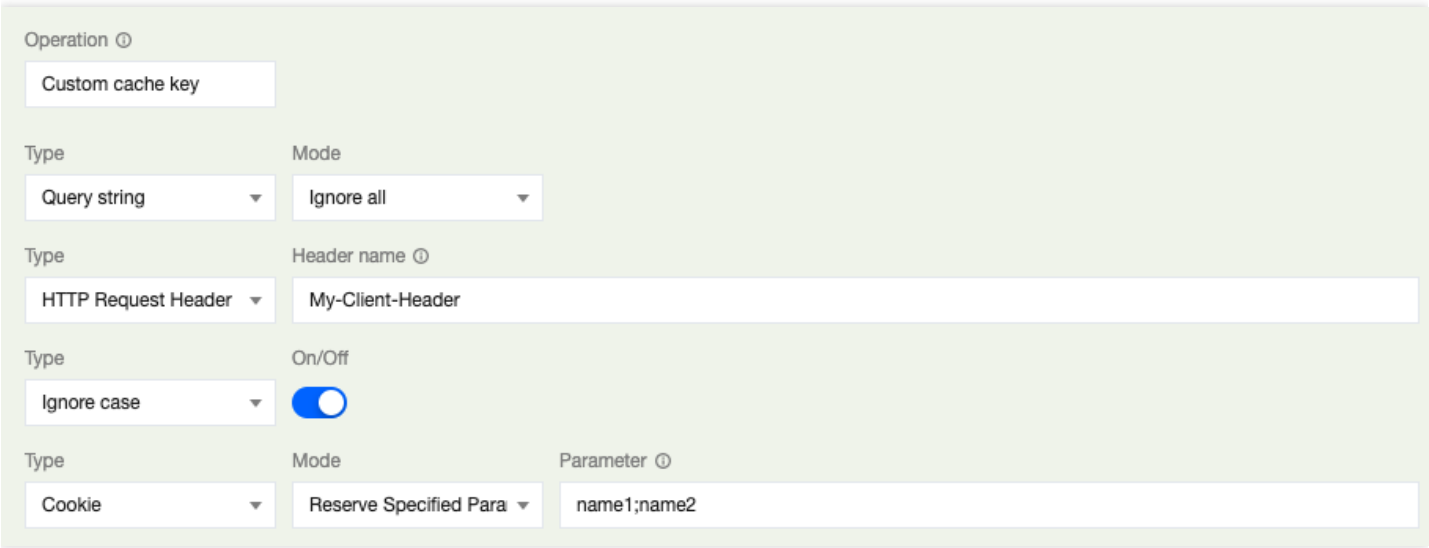
Description of configuration items:

| Configuration Item | Description |
| --- | --- |
| Query string | The query string in the URL can be adjusted to generate a cache key. By default, all query parameters of the original request are retained. For more information, see Query String. |
| Ignore case | Whether to ignore the case of the URL. For more information, see Case Ignoring. |

| Configuration Item | Description |
| --- | --- |
| HTTP request header | Resources to be requested differ according to HTTP request headers. You can specify the HTTP request headers to be concatenated in the URL as part of the cache key.<br>• Custom header: Allow to define custom headers, such as `X-Client-Header`.<br>• Preset header: Allow to specify preset headers that provide information about the `User-Agent` and client IP (such as the device/browser type).<br>◦ `EO-Client-Device`: The device type.<br>Values: `Mobile`, `Desktop`, `SmartTV`, `Tablet`, `Others`.<br>◦ `EO-Client-OS`: The client OS.<br>Values: `Android`, `iOS`, `Windows`, `MacOS`, `Linux`, `Others`.<br>◦ `EO-Client-Browser`: Type of the client browser.<br>Values: `Chrome`, `Safari`, Firefox`, `IE`, `Others`.<br>◦ `EO-Client-IPCountry`: Location of the client IP.<br>Values: ISO 3166-1 alpha-2 codes, representing two-letter country/region codes defined in ISO 3166-1. |
| Cookie | The `Cookie` parameter can be adjusted and concatenated in the URL to generate the cache key. |
| Request protocol | Whether to distinguish between caches by request protocol (HTTP/HTTPS). By default, they are not distinguished between. |

# Configuration Samples

The following configuration samples shows how to create a custom cache key for the domain name `www.example.com` :




The cache key is formed by concatenating the URL (which doesn't differentiate the request protocol by default and ignores the case and query string), My-Client-Header, and specified Cookie.

Request A from the client:

URL: `https://www.example.com/path/demo.jpg?key1=value1&key2=value2` .

HTTP request header: Includes `My-Client-Header:fruit` .

Cookie: name1=yummy;name2=tasty;name3=strawberry.

Request B from the client:

URL: `http://www.example.com/path/demo.JPG?key1=value1&key2=value2&key3=value3` .

HTTP request header: Includes `My-Client-Header:fruit` .

Cookie: name1=yummy;name2=tasty;name3=blueberry.

Request C from the client:

URL: `http://www.example.com/path/demo.JPG?key1=value1&key2=value2&key3=value3&key4=value4` .

HTTP request header: Includes `My-Client-Header:sea` .

Cookie: name1=yummy;name2=tasty;name3=fish.

Requests A and B will hit the same cached resource, and request C will hit another.

# Node Cache TTL

Last updated：2022-12-13 16:25:41

## Overview

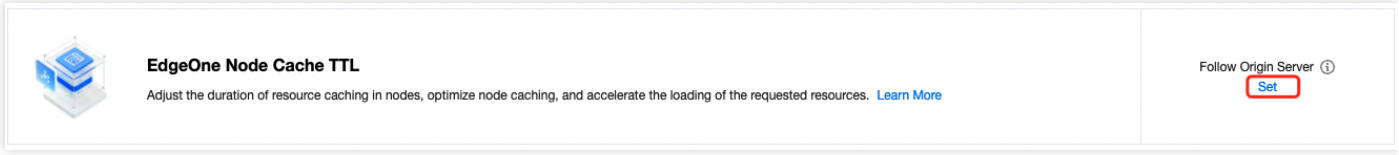
You can adjust the cache period of resources on nodes to optimize the node cache, load requested resources more quickly, and remove old resources timely.

Note：

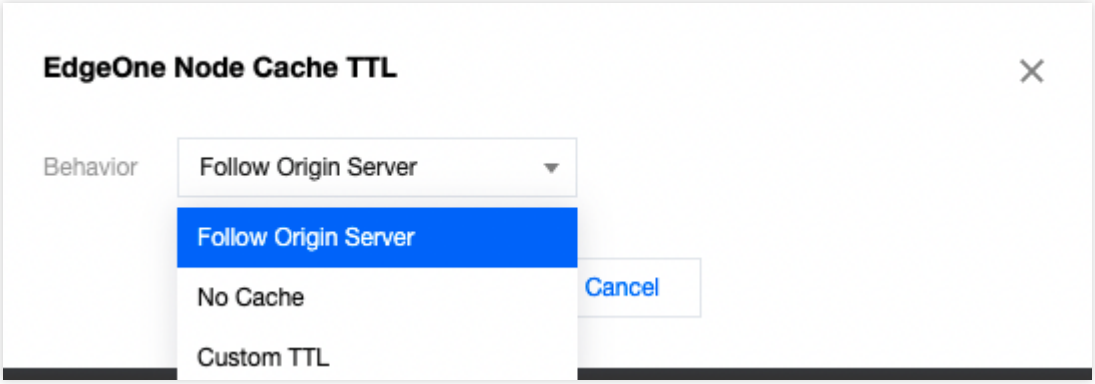
- EdgeOne will determine whether a resource cached on a node expires based on the cache validity period configured in **EdgeOne Node Cache TTL**.
- If the cache of a resource accessed by a client doesn't expire on the node, the node will directly return the cached resource to the client.
- If a resource accessed by a client is not cached, or the resource cache has expired on the node, the node will pull the latest resource from the origin server to cache it and return it to the client.
- After a resource on the origin server is updated, its cache on the node needs to be updated immediately. You can use the cache purge feature to clear historical caches that haven't expired on the node, so that the latest resources can be requested from the origin server.

## Directions

1. Log in to the EdgeOne console and click **Site Acceleration** > **Cache configuration** on the left sidebar.
2. On the **Cache configuration** page, select the target site and click **Set** in the **EdgeOne Node Cache TTL** module.



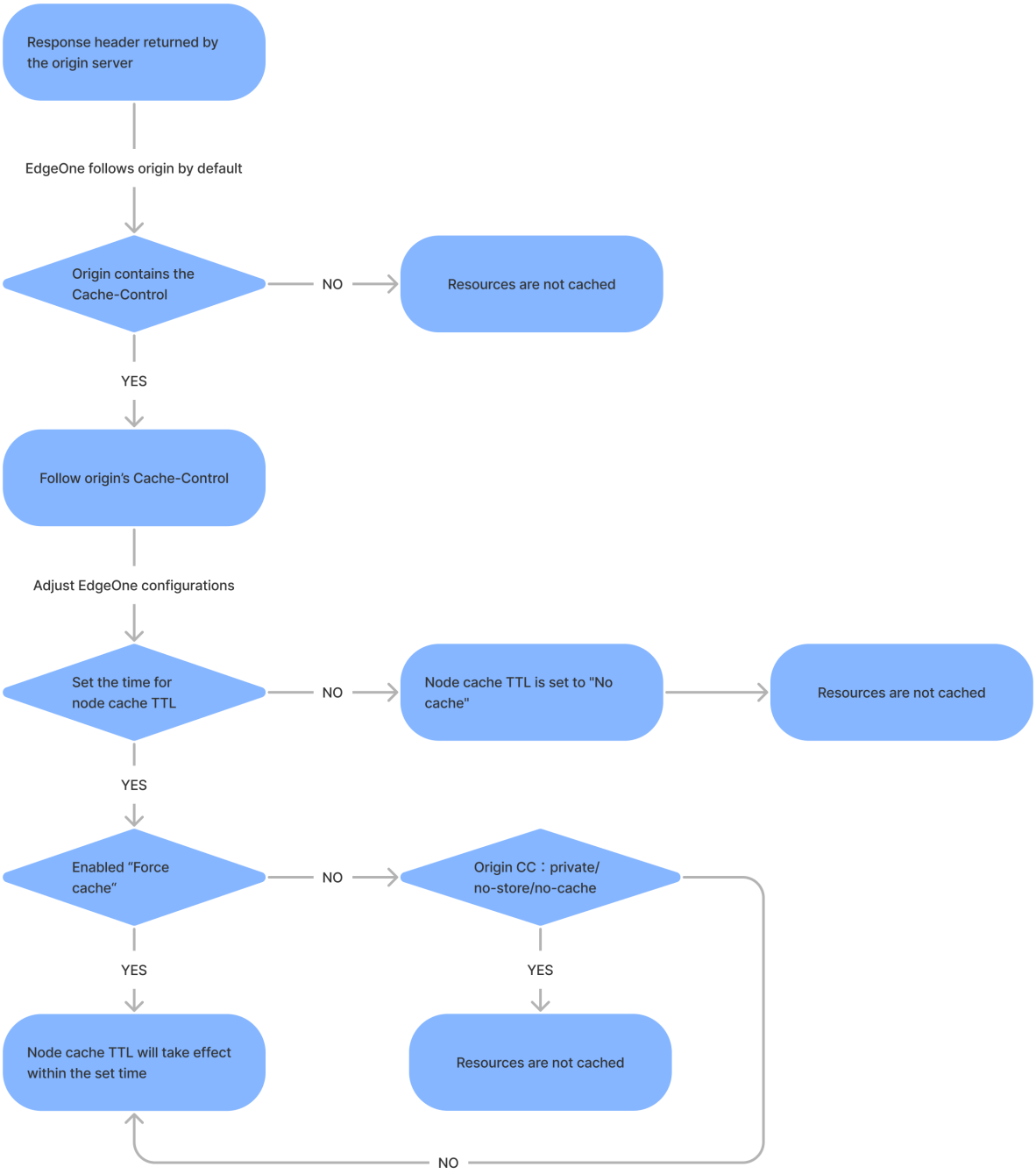
3. In the pop-up window, select a behavior and click **Save**.




**Parameter description:**

- Follow origin server (default configuration): The `Cache-Control` header of the origin server will be followed. If the origin server has no CC headers, there will be no cache. You can also set a default cache time for overwriting.
- No cache: Resources won't be cached on nodes.
- Custom time: Customize the resource cache period.

Note: The overall cache policy is as shown below:




Note：

Force cache: It is enabled by default. When it's enabled, node cache TTL will take effect within the cache period you configure, even if the origin server's `Cache-Control` is `no-cache/no-store/private`. When it's disabled, the nodes will not cache resources and follow the no-cache header, even if the origin server's `Cache-Control` is `no-cache/no-store/private`. To disable force cache, you can go to Rule Engine to customize node cache TTL rules.

# Cache Prefresh

Last updated：2023-03-08 11:46:26

## Overview

Cached resources are validated via origin-pull before expiration, so that your site can respond to requests more rapidly.

## Directions

### Global configuration

1. Log in to the EdgeOne console and choose **Site Acceleration** > **Cache Configuration** on the left sidebar.
2. On the page that appears, select the target site, and then toggle on the switch in the **Cache prefresh** card. The switch is on by default.

| Configuration Item | Description |
| --- | --- |
| Configuration Status | Enabled by default |
| Prefresh interval | A percentage of node cache TTL. Enter an integer from 1 to 99. Default value: 90%.<br>Suppose a resource has a 10-second node cache TTL:<br>If the resource is valid, its TTL will be reset to 10 seconds.<br>If the resource expires, the latest resource will be fetched from the origin and the TTL will be reset to 10 seconds. |

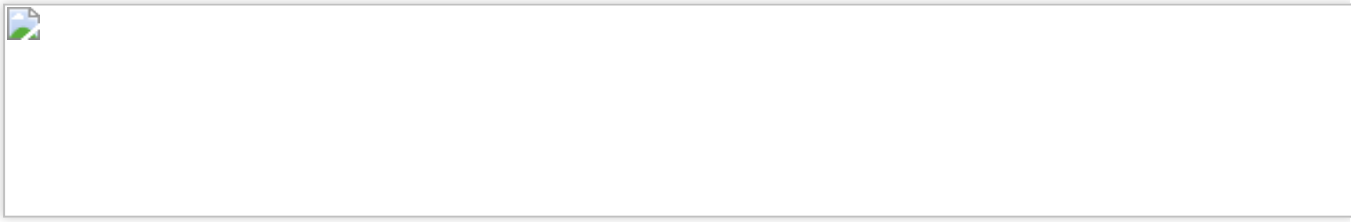
### Differentiated configuration

To create an individual configuration for subdomains, URL paths, or file extensions, you can switch to the rule engine page.

1. Click **Rule Engine** on the left sidebar.
2. For more information, see Rule Engine.

## Sample Configuration

To accelerate the response speed of `example.com`, the node cache TTL is set to 10 seconds, and the prefresh interval is set to 60% of the TTL. The configuration is as follows:



In this case, you can validate the cached resource via origin-pull from the 6th to 10th second before the resource expires.
If the resource is valid, its TTL will be reset to 10 seconds.
If the resource expires, the latest resource will be fetched from the origin and the TTL will be reset to 10 seconds.

# Browser Cache TTL

Last updated：2022-08-01 14:32:16

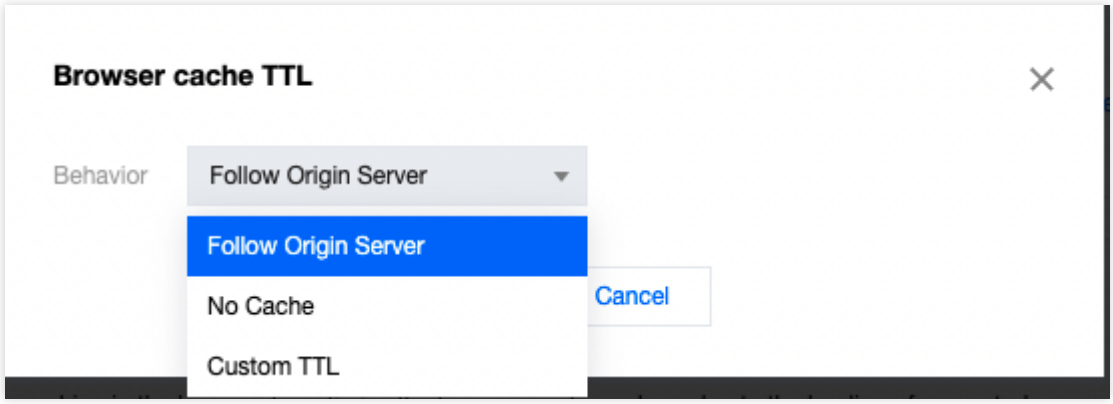
## Overview

You can adjust the cache period of resources in browsers to optimize the browser cache and load requested resources more quickly.

## Directions

1. Log in to the EdgeOne console. Select **Site Acceleration** > **Cache Configuration** on the left sidebar.
2. On the cache configuration page, select the target site and click **Set** in the browser cache TTL module.


3. In the browser cache TTL pop-up window, select a mode and click **Save**.




Parameter description:

- Follow origin server (default configuration): The `Cache-Control` or `Last-Modified` header of the origin server will be followed.
- No cache: Resources won't be cached in browsers.
- Custom time: Customize the resource cache period.

Note: The overall cache policy is as shown below:

# Status Code Cache TTL

Last updated：2023-02-22 17:28:26

## Overview

You can specify a TTL period for origin response status codes, allowing the node to directly respond with non-2XX codes.

Currently supported status codes are as follows:

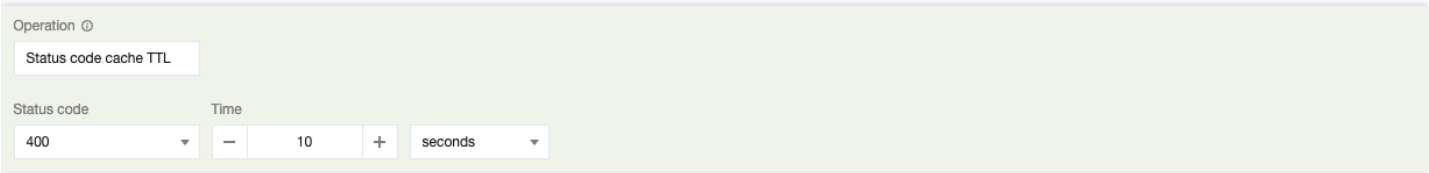
- 4XX: 400, 401, 403, 404, 405, 407, 414
- 5XX: 500, 501, 502, 503, 504, 509, 514

## Directions

1. Log in to the EdgeOne console. Click **Rule Engine** on the left sidebar.
2. On the page that displays, select the target site and create TTL cache rules for status codes as needed. For more information, see Overview.

## Configuration Sample

The following configuration sample shows how to configure the node to return the 404 status code within the specified TTL (10 seconds) for each failed request:



# Offline Caching

Last updated：2023-03-08 11:46:26

## Overview

After offline caching is enabled, when your origin fails, and resources cannot be pulled through origin-pull normally, resources cached on nodes (even expired resources) can be used until the origin recovers.
If there is cached content on nodes, it will be returned. Even if the hit content has expired, it will still be returned until the origin recovers to resume normal origin-pull.
If there is no cached content on nodes, an error message indicating that the origin fails will be returned.

## Directions

### Global configuration

1. Log in to the EdgeOne console and choose **Site Acceleration** > **Cache Configuration** on the left sidebar.
2. On the page that appears, select the target site and toggle the offline caching feature on or off.

On (default): Offline caching is enabled.
Off: Offline caching is disabled.

### Differentiated configuration

To create an individual configuration for subdomains, URL paths, or file extensions, you can switch to the rule engine page.
1. Click **Rule Engine** on the left sidebar.
2. For more information, see Rule Engine.

# File Optimization
# Smart Compression

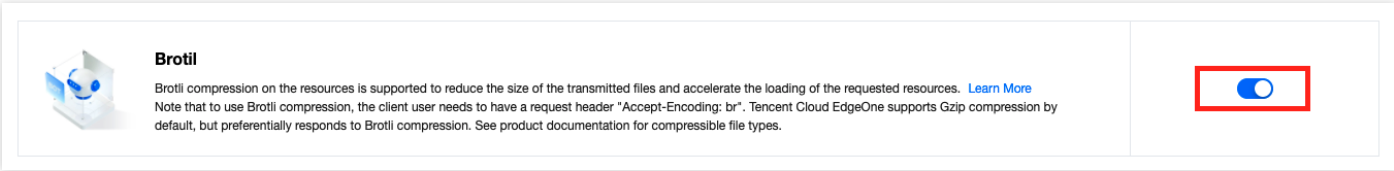
Last updated：2022-12-13 16:25:41

## Overview

Smart Compression can automatically compress the resources to Gzip/Brotli files to reduce the files size and shorten the resource loading time.

## Directions

1. Log in to the EdgeOne console. Click **Site Acceleration** > **File Optimization** on the left sidebar.
2. On the page that appears, select a site, and toggle on/off Smart Compression.




**Parameter description:**

- **On** (default): Smart compression is enabled.
- **Off**: Smart compression is disabled.

## Notes

1. Smart compression supports files of 256 B to 30 MB.

2. By default, smart compression compresses resources by `Content-Type` and supports the following types:

```
text/html
text/xml
text/plain
text/css
text/javascript
```

```
application/json
application/javascript
application/x-javascript
application/rss+xml
application/xmltext
image/svg+xml
image/tiff
text/richtext
text/x-script
text/x-component
text/x-java-source
text/x-markdown
text/js
image/x-icon
image/vnd.microsoft.icon
application/x-perl
application/x-httpd-cgi
application/xml
application/xml+rss
application/vnd.api+json
application/x-protobuf
multipart/bag
multipart/mixed
application/xhtml+xml
font/ttf
font/otf
font/x-woff
application/vnd.ms-fontobject
application/ttf
application/x-ttf
application/otf
application/x-otf
application/truetype
application/opentype
application/x-opentype
application/font-woff
application/eot
application/font
application/font-sfnt
application/wasm
application/javascript-binast
application/manifest+json
application/ld+json
```

3. If both Gzip compression and Brotli compression are enabled, and the client request header `Accept-Encoding` carries both `br` and `gzip` :

- If the node has cached resources compressed in Brotli and Gzip, Brotli compressed resources are returned first.
- If the node has cached resources compressed only in Brotli, Brotli compressed resources are returned first.
- If the node has cached resources compressed only in Gzip, Gzip compressed resources are returned first.

4. If only Brotli compression or Gzip compression is enabled and the request header carries `gzip` or `br` , the compression will not take effect, and the original resource will be returned.
5. If the origin server has the compression feature enabled, and the server carries the response header `Content-Encoding` , the smart compression feature will no longer take effect.

# Media processing
# Resizing and Converting Images

Last updated：2023-02-01 15:35:45

## Overview

EdgeOne can respond to the client with images in the specified size and format, and cache the processed images. The whole process is taken place on EdgeOne nodes.

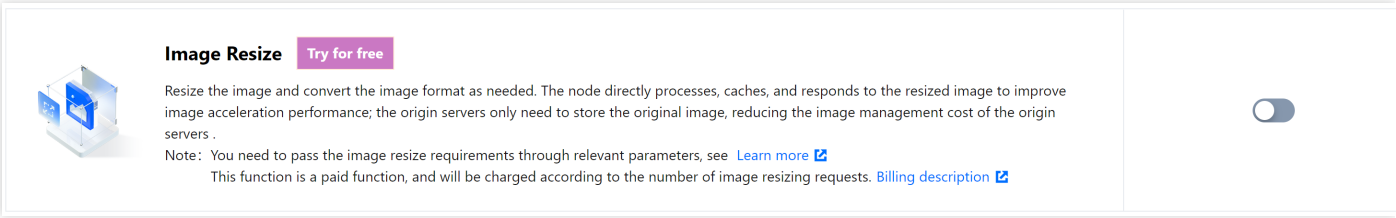
## Use Cases

- Responds to the client with resized images. Only the original image is stored on the origin server, which reduces the image management costs.
- Compresses an image on the premise that the image quality is not visually degraded, which improves the page/image loading speed.

## Directions

1. Log in to the EdgeOne console. Click **Site Acceleration** > **Media Processing** on the left sidebar.

2. On the page that appears, toggle **Image Resize** on.




3. Concatenate `eo-img` parameters to the client request URL. Example:
`https://www.example.com/foo.png?eo-img.resize=w/100` .
The parameters are described as follows:

| Feature | Parameter | Value (type/pixel) | Description |
| --- | --- | --- | --- |

| Feature | Parameter | Value (type/pixel) | Description |
| --- | --- | --- | --- |
| Resize | eo-img.resize | w/100 | Changes the width to the specified value. The height is automatically adjusted based on the aspect ratio. |
| | | h/100 | Changes the height to the specified value. The width is automatically adjusted based on the aspect ratio. |
| | | w/100/h/100 | Changes the width and height to the specified values. |
| | | l/100 | Changes the long side of an image to the specified value. The short side is automatically adjusted based on the aspect ratio. |
| | | s/100 | Changes the short side of an image to the specified value. The long side is automatically adjusted based on the aspect ratio. |
| Format conversion | eo-img.format | webp, heif, avif, guetzli, tpg, svg, jpg2000, or jpg-xr | Converts an image to the specified format. |

## Limits

1. The original image cannot exceed 20 MB. For images over the limit, the original image is returned.
2. `eo-img.resize` and `eo-img.format` can be used at the same time. For example, `eo-img.resize=w/100&eo-img.format=webp` means to resize the image and convert the format.
3. The same parameter can only be specified once in a request URL. For example, `eo-img.resize=w/100&eo-img.resize=w/200` and `eo-img.resize=w/100&eo-img.format=webp&eo-img.resize=w/200` are not allowed. In this case, the parameter settings are invalid, and the original image is returned.
4. `width` / `height` and `long` / `short` parameters cannot be specified at the same time. For example, `w/300/s/200` is not allowed. In this case, the parameter settings are invalid, and the original image is returned.
5. If parameters are specified in an incorrect syntax, such as `eo-img.resize=w=100` , or are misspelled, the parameter settings are invalid, and the original image is returned.
6. If the **image resize** feature is disabled, `eo-img` parameters are processed as a common query string, and the original image is returned.

## Pricing and Billing

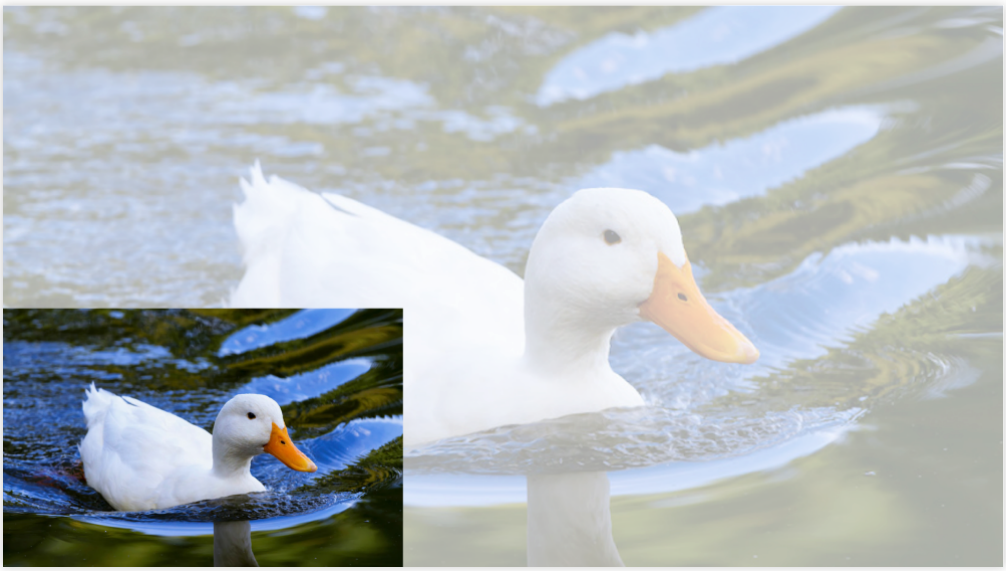
The image resize feature is billed based on the number of image resizing requests. For more information, see Billing Overview.

Note：
The image resize feature is currently free for a limited time. An announcement will be released when the free trial ends.

## Sample Configuration

In the following examples, the original image is 500 × 280 pixels in resolution and 500 KB in size.

1. Change the width to 200 pixels, and the height is automatically adjusted based on the aspect ratio.
   Request URL: `http://www.example.com/foo.png?eo-img.resize=w/200`



2. Change the height to 200 pixels, and the width is automatically adjusted based on the aspect ratio.
   Request URL: `http://www.example.com/foo.png?eo-img.resize=h/200`

3. Change the width to 300 pixels and the height to 200 pixels.
   Request URL: `http://www.example.com/foo.png?eo-img.resize=w/300/h/200`

> Note：
> If both the width and height are specified, the aspect ratio of the original image may not be retained.

4. Change the long side to 400 pixels, and the short side is automatically adjusted based on the aspect ratio.
   Request URL: `http://www.example.com/foo.png?eo-img.resize=l/400`

5. Change the short side to 200 pixels, and the long side is automatically adjusted based on the aspect ratio.
   Request URL: `http://www.example.com/foo.png?eo-img.resize=l/200`

6. Convert the image to WebP format.
   Request URL: `http://www.example.com/foo.png?eo-img.format=webp`
   Output image format: WebP

7. Change the width to 200 pixels, with the height automatically adjusted based on the aspect ratio, and convert the format to WebP.
   Request URL: `http://www.example.com/foo.png?eo-img.resize=w/200&eo-img.format=webp`

# Cache Purge

Last updated：2022-12-13 16:25:41

## Overview

Cache purge is to clear resources cached on nodes. After purge, when a user accesses a resource, the latest resource will be obtained through origin-pull for response.

> Note：
> After cache purge, as there is no cache of the resource on nodes, the resource can be obtained only through origin-pull, and the number of origin-pull requests will increase for a short period, which will compromise the acceleration effect. If many cached resources are purged, a large number of origin-pull requests will be generated, bringing pressure on the origin server.

## Use Cases

**New resource release**

When a resource is updated on the business origin server, you need to purge the old resource cached on nodes to prevent users from getting the old resource. After the cache is purged in the entire network, users can get the latest resource.

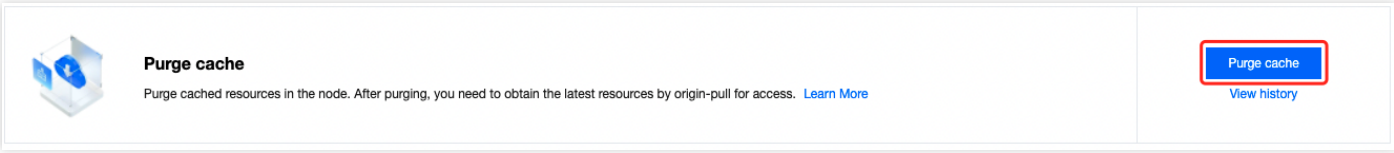
**Non-compliant resource clearing**

If there are non-compliant resources at your business site, you need to clear them and rectify your site promptly. As such resources may still be cached on nodes, you need to purge them from nodes.

## Directions

1. Log in to the EdgeOne console and click **Site Acceleration** > **Cache configuration** on the left sidebar.

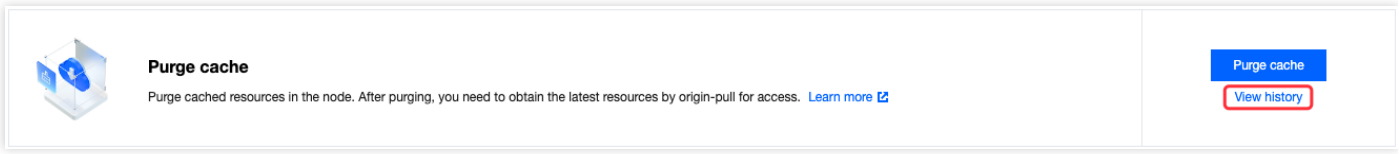
2. On the cache configuration page, select the target site and click **Purge cache** in the cache purge module.




3. In the pop-up window, enter the target resource content and click **Clear**.

| Supported Type | Details |
| --- | --- |
| URL | The URL(s) matched by the resource cached on the node, for example, `https://www.example.com/path/foo.jpg` . |
| Prefix | The prefix path matched by the resource cached on the node, for example, `https://www.example.com/path` . |
| Hostname | The hostname(s) matched by the resource cached on the node, for example, `www.example.com` .<br>Note: You cannot submit URLs in the format of `http://*.test.com/` , i.e., domain names cannot contain `*` . You need to specify the corresponding subdomain names. |
| Cache-Tag | Cache purge with matched tag(s) of the `Cache-Tag` response header in the HTTP response packet, for example, `Cache-Tag: tag1,tag2,tag3` .<br>◦ It applies only to the Enterprise plan.<br>◦ EdgeOne can identify the `Cache-Tag` response header of the origin server. You need to add tag(s) to the header.<br>▪ A header can be up to 6 KB in size.<br>▪ Separate tags by comma. A tag can contain up to 128 characters. There can be up to 1,000 tags.<br>▪ Tags are case-insensitive, which means `Tag1` and `tag1` are the same. |
| Cache all | All cached resources of the site on nodes.<br>Note: If a wildcard domain name under the current site (example.com) such as `*.foo.example.com` is connected, this option cannot take effect, and you need to submit the cache purge task for each subdomain name separately. |

4. Click **View history** to view the history in a specified time period and of a specified purge type.




# Notes

## Content specifications

Check whether the submitted content meets the following specifications:

- Do not submit the content of a site that is disabled, locked, or not connected to the current account.
- If you submit tasks by file upload, make sure that the file is in .txt format and doesn't exceed 10 MB in size.
- If the content contains non-ASCII characters, toggle **URL-encoding** on to convert the encoding.
- The encoding rules must comply with RFC 3986.
- Spaces must be encoded to `%20` no matter where they are.
- If encoding conversion is involved, only resources matched after encoding conversion will be purged.

## Submission limit

- Different plans have different quotas. For billing details, see Billing Overview.
- If you select file upload as the URL submission method, there is no limit on the number of URLs that can be submitted each time, but the number of submitted URLs will be deducted from the daily quota.

# URL Pre-Warming

Last updated：2022-12-13 16:25:41

## Overview

URL pre-warming caches the resource at the matched URL from the origin server to a node in advance, so that users' resource requests can be responded to directly on the node. This enhances the acceleration effect and mitigates the pressure on the origin server.

Note：

- During resource pre-warming, a request will be simulated to pull the corresponding resource from the origin server. If there are many submitted pre-warming tasks, a large number of origin-pull requests will be generated, increasing the origin server bandwidth usage.
- If a pre-warmed resource conflicts with a resource cached on the node (that is, the node already cached a resource with the same name that hasn't expired), the cached resource will remain effective and won't be overwritten by the pre-warmed resource. If the cached resource changes, you can purge the corresponding node cache before pre-warming.
- Resources are pre-warmed to edge nodes by default, and traffic generated at the edge layer is billed as normal traffic.

## Use Cases

**Installation package release**

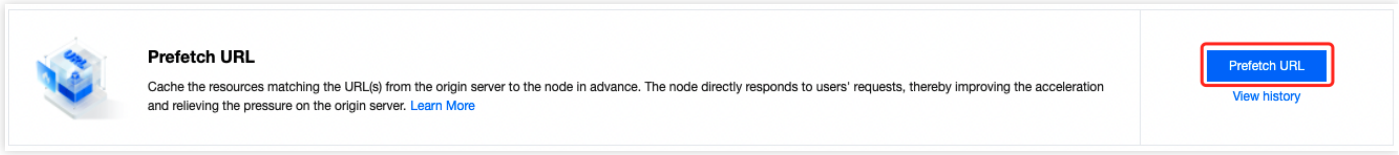
Before formally releasing the installation or upgrade package of a new version, you can pre-warm the installation package resources to nodes. After formal release, when users request to download the package, they can directly get it from the nodes, which speeds up download and alleviates the pressure on the origin server.

**Operational event**

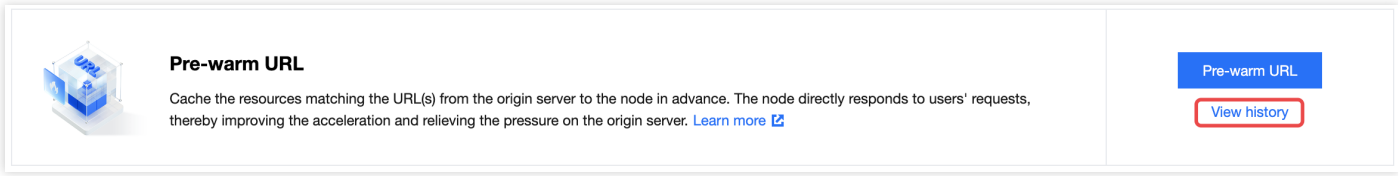
Before holding an operational event formally, you can pre-warm static resources including webpages and images used on event webpages to nodes. After the event formally starts, static resources requested by users will be directly returned by nodes to accelerate the page access and improve the user experience.

# Directions

1. Log in to the EdgeOne console and click **Site Acceleration** > **Cache configuration** on the left sidebar.
2. On the **Cache configuration** page, select the target site and click **Pre-warm resource** in the **Pre-warm URL** module.




3. In the pop-up window, enter or upload URLs and click **OK**.
4. Click **View history** to view the history in a specified time period.




# Notes

## Content specifications

Check whether the submitted content meets the following specifications:

- Do not submit the content of a site that is disabled, locked, or not connected to the current account.
- You cannot submit URLs in the format of `http://*.test.com/` ; that is, domains cannot contain `*` . You need to specify the corresponding subdomains.
- If you submit tasks by file upload, make sure that the file is in .txt format and doesn't exceed 10 MB in size.
- If the content contains non-ASCII characters, toggle **URL-encoding** on to convert the encoding.
- The encoding rules must comply with RFC 3986.
- Spaces must be encoded to `%20` no matter where they are.
- If encoding conversion is involved, only resources matched after encoding conversion will be pre-warmed.

## Submission limit

- Different plans have different quotas. For billing details, see Billing Overview.
- If you select file upload as the URL submission method, there is no limit on the number of URLs that can be submitted each time, but the number of submitted URLs will be deducted from the daily quota.

# HTTPS Configuration

Last updated：2022-10-18 10:30:12

1. Log in to the EdgeOne console and click **Site Acceleration** > **HTTPS configuration** on the left sidebar.

2. On the HTTPS configuration page, select the target site and configure the following HTTPS items for site acceleration:

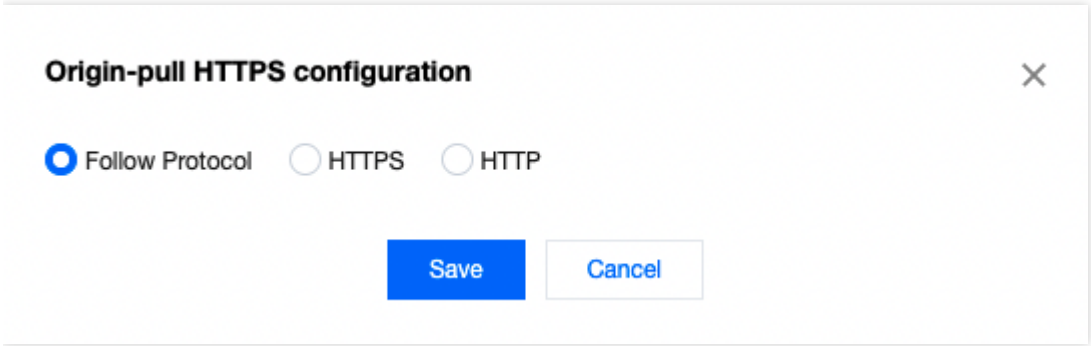
### Forced HTTPS

In the forced HTTPS module, click  to forcibly redirect all edge HTTP requests to HTTPS through 301/302. It is disabled by default.

> Note：
> After this feature is enabled, all requests will be transferred over HTTPS. Make sure that certificates of service-providing subdomains have been deployed in EdgeOne.

### Origin-Pull HTTPS

In the origin-pull HTTPS module, click **Edit**, select the origin-pull encryption mode (i.e., protocol used for origin-pull), and click **Save**.

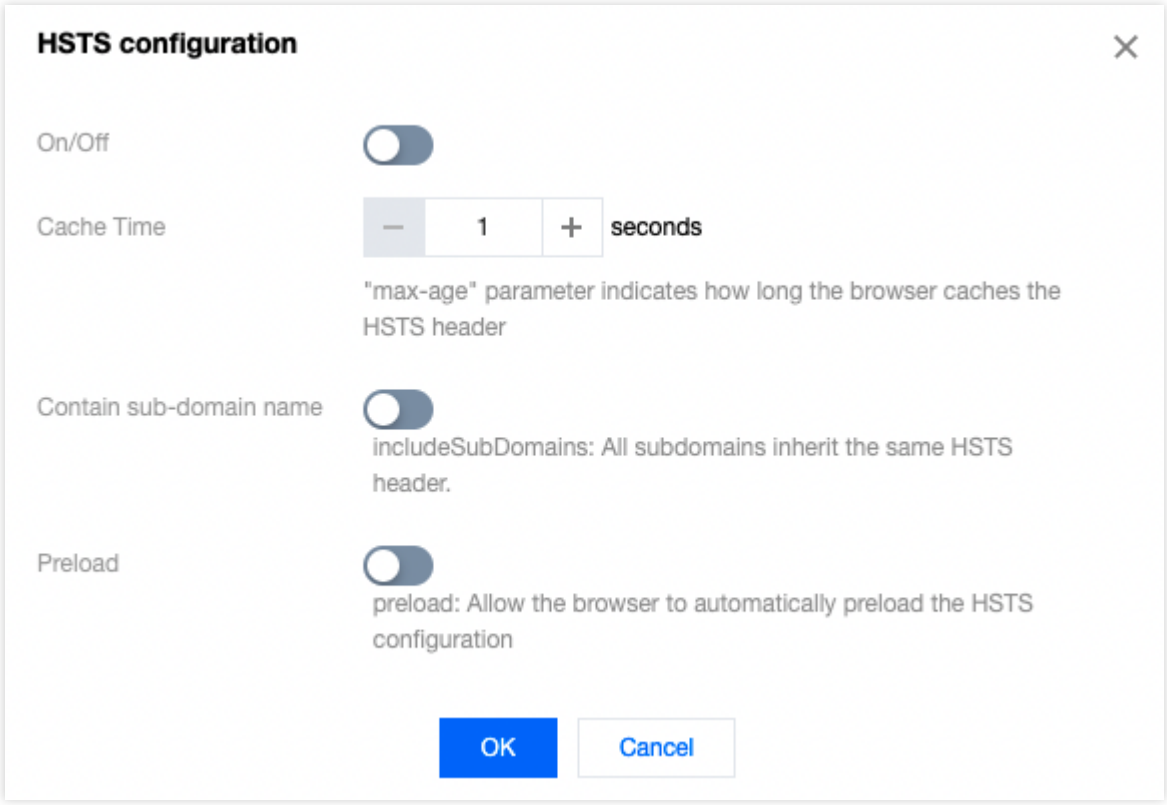



**Parameter description:**

- Follow protocol (default): The origin-pull protocol follows the request protocol. For example, if the request uses HTTP, origin-pull will also use HTTP.
- HTTP: All origin-pull requests use the HTTP protocol.
- HTTPS: All origin-pull requests use the HTTPS protocol.

### HTTP Strict Transport Security (HSTS)

1. In the HSTS module, click **Enable HSTS**, configure relevant parameters, and click **OK**.




**Parameter description:**

- Default status: It is disabled by default. To use the HSTS feature, you need to enable it.
- Cache time: Set the HSTS header validity period in seconds, during which browsers always initiate requests over HTTPS. The value range is 1–31536000.
- Include subdomain: If it is enabled, HSTS will take effect for the current domain and its subdomains.
- Preload: If it is enabled, browsers will automatically load the HSTS configuration in advance to avoid the attack risks of the first HTTP request. This feature can take effect only if you add the domain to the HSTS preload list in browsers first.

2. After HSTS is configured, the `Strict-Transport-Security` header will be added to the EdgeOne cache node responses to force clients such as browsers to establish connections to edge nodes over HTTPS for global website encryption.

- HTTPS header format

```
Strict-Transport-Security: max-age=expireTime [; includeSubDomains] [; preload]
```

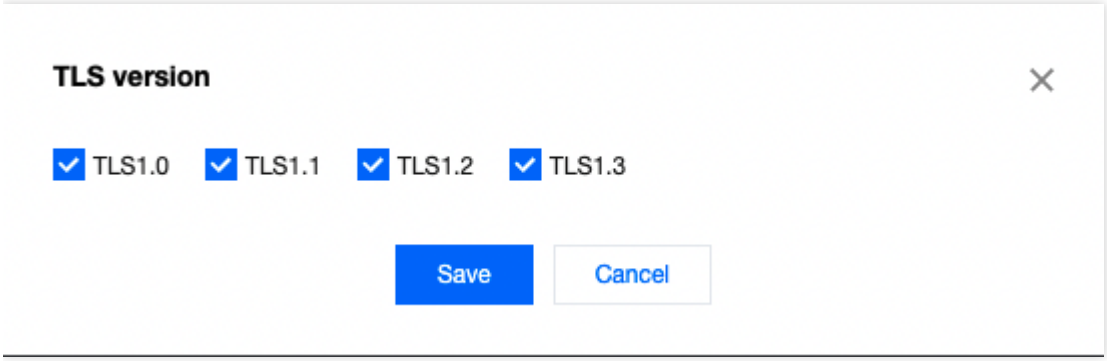
- Field description
  - max-age: HSTS header validity period in seconds, during which browsers always initiate requests over HTTPS.
  - includeSubDomains: It is an optional field. If it is enabled, HSTS will take effect for the current domain and its subdomains.
  - preload: It is an optional field. If it is enabled, browsers will automatically load the HSTS configuration in advance to avoid the attack risks of the first HTTP request. This feature can take effect only if you add the domain to the HSTS preload list in browsers first.

> Note：
>
> - Before enabling HSTS, make sure that domain certificates have been deployed to respond to HTTPS requests normally.
> - We recommend you also enable forced HTTPS when enabling HSTS; otherwise, if requests use HTTP, browsers won't execute the HSTS configuration.
> - The value range of `max-age` is 1–31536000 seconds.

### TLS version

In the TLS version module, click **Edit**, select the target version, and click **Save**.

> Note：
> Only HTTPS links on enabled TLS versions are allowed. Available TLS versions are 1.0–1.3. You can enable a single version or a series of consecutive versions.




### OCSP stapling

In the OCSP stapling module, the cached OCSP response will be sent during TLS handshake to improve the handshake efficiency. After you click  to enable OCSP stapling, cache nodes will cache the OCSP response for clients to verify it, and clients won't need to send query requests to certificate authorities (CAs), which accelerates TLS handshakes.

# Network Optimization
# HTTP/2

Last updated：2023-03-08 11:46:26

## Overview

HTTP/2 (HTTP 2.0) requests are supported to accelerate sites and improve the web performance.

**What is HTTP/2?**

Hypertext Transfer Protocol Version 2 (HTTP/2 or HTTP 2.0) is the second major version of the HTTP protocol. It can effectively reduce the network latency and accelerate site page loading.

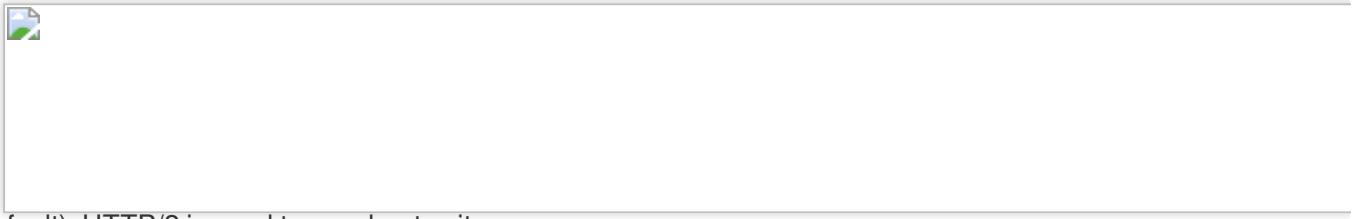
## Prerequisites

This feature takes effect only after an HTTPS certificate is configured.

## Directions

### Global configuration

1. Log in to the EdgeOne console and choose **Site Acceleration** > **Network Optimization** on the left sidebar.
2. On the page that appears, select the target site and toggle the HTTP/2 feature on or off.



On (default): HTTP/2 is used to accelerate sites.
Off: HTTP/2 is not used to accelerate sites.

### Differentiated configuration

To create an individual configuration for a subdomain of the target site, you can switch to the rule engine page.
1. Click **Rule Engine** on the left sidebar.
2. For more information, see Rule Engine.

# Must-Knows

1. If a client does not support HTTP/2, HTTP 1.x will be used.
2. Only HTTP/2 access requests rather than origin-pull requests are supported here. You can configure HTTP/2 origin-pull by referring to Rule Engine.

# HTTP/3 (QUIC)

Last updated：2023-03-09 09:39:50

## Overview

HTTP/3 (QUIC) requests are supported. HTTP/3 (QUIC) is used to accelerate site requests and improve data transfer efficiency and security.

**What is QUIC?**

Quick UDP Internet Connections (QUIC) is a general-purpose network protocol. It not only provides reliability comparable to that of TCP connections, but also greatly reduces the latency in transfer and connections to prevent network congestion while guaranteeing the network security.
EdgeOne currently supports the following QUIC versions: h3-29, h3-Q050, h3-Q046, h3-Q043, Q046, and Q043.

## Directions

### Global configuration

1. Log in to the EdgeOne console and choose **Site Acceleration** > **Network Optimization** on the left sidebar.
2. On the page that appears, select the target site and toggle the HTTP/3 (QUIC) feature on or off.

Off (default): HTTP/3 (QUIC) requests are not supported.
On: HTTP/3 (QUIC) requests are supported, and HTTP/3 (QUIC) is used to accelerate site requests.

**Note**

This feature takes effect only after an HTTPS certificate is configured.
HTTP/3 (QUIC) requests in excess of the package quota will be billed in pay-as-you-go mode separately.

### Differentiated configuration

To create an individual configuration for a subdomain of the target site, you can switch to the rule engine page.

1. Click **Rule Engine** on the left sidebar.
2. For more information, see Rule Engine.

# Must-Knows

1. If both HTTP/2 and HTTP/3 (QUIC) are enabled, HTTP/2 or HTTP/3 (QUIC) will be used based on the actual client request conditions.
2. Only HTTP/3 (QUIC) access requests rather than origin-pull requests are supported here.

# IPv6 Access

Last updated：2022-10-09 09:42:57

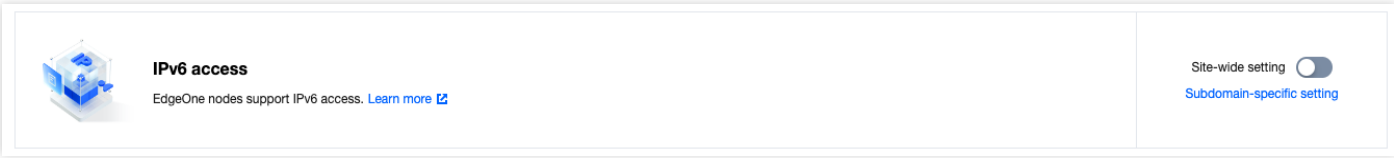
## Overview

You can quickly enable IPv6 access to allow IPv6 clients to access nodes over the IPv6 protocol.

> Note：
> This feature is currently unavailable in the Chinese mainland.

## Directions

1. Log in to the EdgeOne console. Click **Site Acceleration** > **Network Optimization** on the left sidebar.
2. On the **Network optimization** page, select the target site and toggle on or off the IPv6 access feature.



# Maximum Upload Size

Last updated：2023-03-08 11:46:26

## Overview

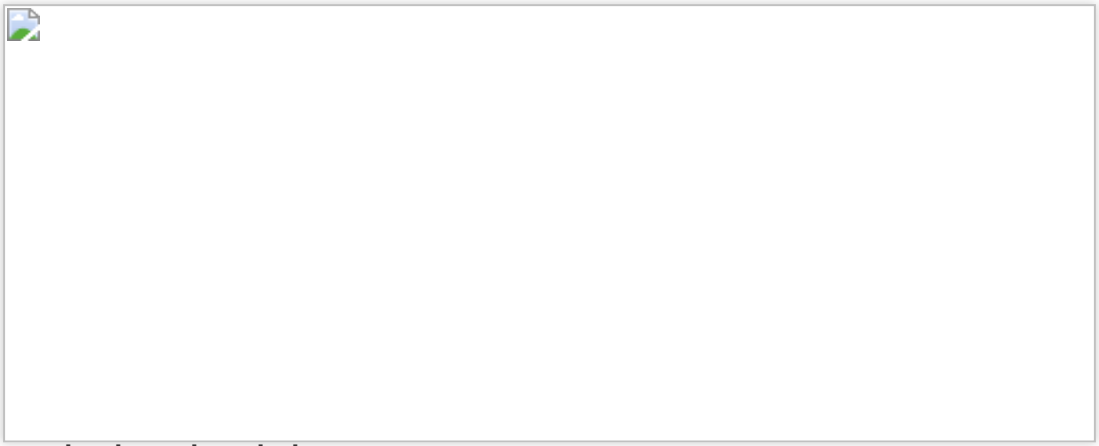
The maximum upload size is the maximum data volume that can be uploaded in a single client request. You can restrict it to improve the data transfer efficiency and optimize the network transfer.

## Directions

### Global configuration

1. Log in to the EdgeOne console and choose **Site Acceleration** > **Network Optimization** on the left sidebar.
2. On the page that appears, select the target site and click **Settings** in the maximum upload size module.

3. In the pop-up window for configuring the maximum upload size, enable **Size limit**, enter an upper limit value, and click **Save**.



**Configuration item description:**

Size limit: It is enabled by default. In the Enterprise edition, you can disable this feature, and then you can upload data in any size (the platform uses streaming transfer).

Upper limit: After the size limit is enabled, you can set an upper limit from 1-500 MB. Default value: 500 MB.

### Differentiated configuration

To create an individual configuration for subdomains, URL paths, or file extensions, you can switch to the rule engine page.

1. Click **Rule Engine** on the left sidebar.
2. For more information, see Rule Engine.

## Must-Knows

The configuration here takes effect before the origin configuration.

# WebSocket

Last updated：2023-03-08 11:46:26

## Overview

EdgeOne supports the WebSocket protocol that allows the server to proactively send data to the client.

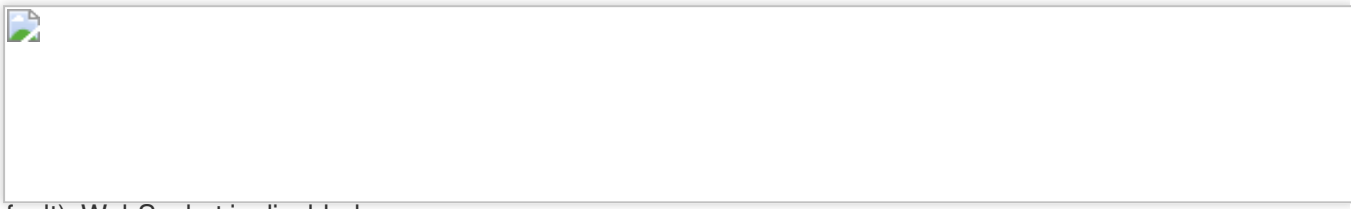
**What is WebSocket?**

WebSocket is a TCP-based persistent protocol that implements full-duplex communication between the client and server and allows the server to proactively send information to the client. Before the emergence of WebSocket, to implement such duplex communication, web applications needed to consistently send HTTP request calls for inquiry, which increased service costs and reduced the efficiency.
Thanks to full-duplex, WebSocket is widely used in scenarios such as social networking subscription, online collaboration, market quotation push, interactive live streaming, online education, and Internet of Things. It can better save server resources and bandwidth and implement communication with higher real-timeliness.

## Directions

### Global configuration

1. Log in to the EdgeOne console and choose **Site Acceleration** > **Network Optimization** on the left sidebar.
2. On the page that appears, select the target site, and toggle the switch of the WebSocket module on/off.



Off (default): WebSocket is disabled.
On: WebSocket is enabled.
3. In the WebSocket maximum connection time window, set the maximum duration and click **Save**.

**Note**

Maximum connection time: If there is no data transmissions within the period, the connection will be terminated.
The maximum connection duration varies with the following editions:
Enterprise: 300s
Standard: 120s

### Differentiated configuration

To create an individual configuration for a subdomain of the target site, you can switch to the rule engine page.

1. Click **Rule Engine** on the left sidebar.
2. For more information, see Rule Engine.

# Real Client IP Header

Last updated：2022-12-07 16:15:58

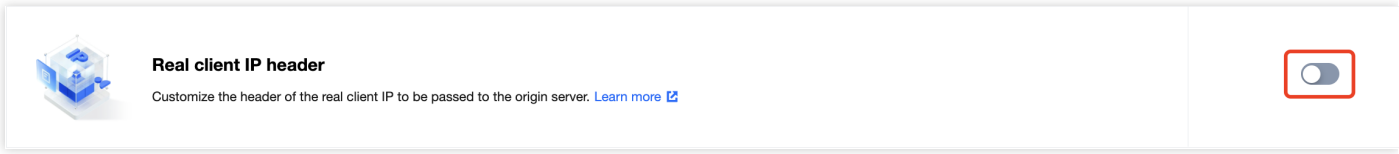
## Overview

Real client IP header allows you to create a custom origin-pull HTTP request header that carries the real client IP information.

## Directions

1. Log in to the EdgeOne console. Click **Site acceleration** > **Network optimization** on the left sidebar.

2. On the network optimization page, select a site and click  to enable the "Real client IP header" feature.




3. In the pop-up window, enter a header name, such as Tencent-Client-IP, and click **Save**.

# Client IP Geographical Location

Last updated：2022-12-07 16:18:00

## Overview

The custom header can carry the geographical location information of the client IP to the origin.

Note：

- The country/region value is represented by an ISO 3166-1 alpha-2 code (a two-letter country/region code).
- Currently, IPv6 is not supported.

## Directions

1. Log in to the EdgeOne console. Click **Site Acceleration** > **Network optimization** on the left sidebar.
2. On the **Network optimization** page, select the target site and click  to enable **Client IP Geographical Location**.


3. In the pop-up window, customize the header name or directly use the default name `EO-Client-IPCountry` and click **Save**.

# gRPC

Last updated：2023-02-07 17:59:18

## Overview

Tencent Cloud EdgeOne supports the HTTP, HTTPS, and gRPC protocols at the same time, and automatically uses a protocol based on your requests. In other words, the HTTP protocol is used for HTTP requests and the gRPC protocol for gRPC requests.

## What Is gRPC?

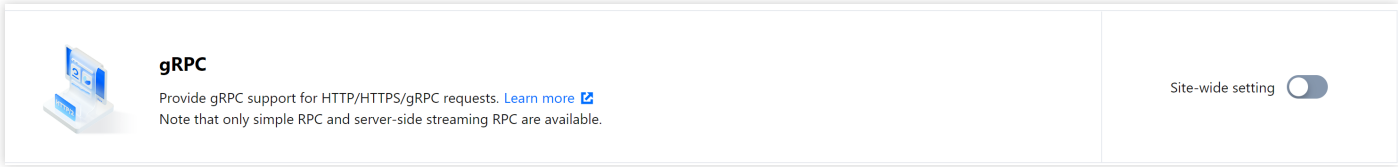
Google Remote Procedure Call (gRPC) is an open source remote procedure call system developed by Google based on the HTTP/2 specification. It provides many features, such as bidirectional streams, stream throttling, header compression, and multiplexing requests over a single TCP connection.

## Prerequisites

gRPC runs over the HTTP/2 protocol. To send requests and forward them to the origin by using gRPC, you must enable HTTP/2. For more information, see HTTP/2.

## Directions

1. Log in to the EdgeOne console and choose **Site Acceleration** > **Network Optimization** on the left sidebar.
2. On the **Network Optimization** page, select a site and toggle the switch of the gRPC module on to enable gRPC.




**Parameter description:**
Disabled status (default): gRPC requests are not supported.
Enabled status: gRPC requests are supported. Only Simple RPC and Server-side streaming RPC requests are supported.

# URL Rewrite
# Access URL Redirection

Last updated：2022-12-13 16:25:41

## Overview

A node redirects the URL requested by the client to the destination URL based on the response status code.

## Use cases

The URL redirect used to be generated and returned by the origin server, which can now be constructed and returned by EdgeOne nodes. This reduces the network latency and load consumed to generate the URL redirect, thereby improving the client access performance.

## Directions

1. Log in to the EdgeOne console and click **Rule engine** on the left sidebar.
2. On the **Rule engine** page, select the target site and configure the URL redirect rule as needed. For more information, see Overview.
   Configuration item description:

| Configuration Item | Description |
| --- | --- |
| Destination URL | Destination URL after redirection, such as `https://www.example.com/images/foo.jpg` and `https://www.example.com/foo/bar`. |
| Carry query parameters | Whether to carry the original query parameters to the destination URL. By default, they are carried. |
| Status code | Select the response status code of the redirect. Valid values:<br>◦ 302 (default)<br>◦ 301<br>◦ 303<br>◦ 307 |

# Sample Configuration

If the request URL `https://www.example.com/path/foo.html` is configured with the access URL redirect as follows:


Then, when the client requests `https://www.example.com/path/foo.html?key1=value1`, the node will return the 301 status code and redirect it to `https://www.example.com/newpath/bar.html`.

# Origin-Pull URL Rewrite

Last updated：2022-12-13 16:25:41

## Overview

Based on specified rules, this feature rewrites the user request URL received by the node to the destination URL when the node sends the request to the origin server, which doesn't affect the node cache key.

## Use cases

In certain cases, the URL accessed by the client has been published and should not be modified, but the origin server has changed its URL for certain reasons; or the URL accessed by the client differs from that on the origin server for SEO. Then, you can set origin-pull URL rewrite rules, so that the node can rewrite the origin-pull URL to the actual resource URL on the origin server without changing the URL accessed by the client.

## Directions

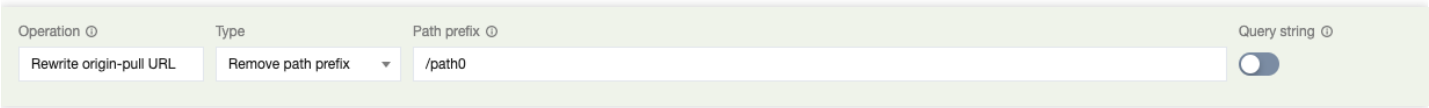
1. Log in to the EdgeOne console and click **Rule engine** on the left sidebar.
2. On the **Rule engine** page, select the target site and configure the origin-pull URL rewrite rule as needed. For more information, see Overview.
   Configuration item description:

| Configuration Item | Description |
| --- | --- |

| Configuration Item | Description |
| --- | --- |
| Type | Rewrite type:<br>◦ Add a prefix: Add the specified prefix to the request URL. For example, if the request URL is `http://www.example.com/path0/index.html` and the prefix to be added is `/prefix`, the rewritten URL will be `http://www.example.com/prefix/path0/index.html`.<br>◦ Remove the prefix: Remove the specified prefix from the request URL. For example, if the request URL is `http://www.example.com/path0/path1/index.html` and the prefix to be removed is `/path0`, the rewritten URL will be `http://www.example.com/path1/index.html`.<br>◦ Replace the complete path: Replace the complete request URL. For example, if the request URL is `http://www.example.com/path0/index.html` and the path to be replaced is `/new/page.html`, the rewritten URL will be `http://www.example.com/new/page.html`. |
| Carry query parameters | Whether to carry the original query parameters to the destination URL. By default, they are carried. |

## Sample Configuration

If the request URL `https://www.example.com/path0/path1/foo.html` is configured with the origin-pull URL rewrite as follows:




Then, when the client requests `https://www.example.com/path0/path1/foo.html?key1=value1`, the URL will be rewritten to `https://www.example.com/path1/foo.html` during origin-pull to get the requested resource.

# Modifying Header
# Modifying HTTP Response Headers

Last updated：2023-02-22 17:28:26

## Overview

You can customize, add, and delete headers in HTTP responses from nodes to clients, which will not affect the node cache.

## Directions

1. Log in to the EdgeOne console and click **Rule engine** on the left sidebar.
2. On the page that displays, select the target site and create rules to modify HTTP response headers as needed. For more information, see Overview.
   Description of configuration items:

| Type | Description |
| --- | --- |
| Set | Sets the specified header to the specified value. The header must be unique.<br>Note: If the specified header does not exist, it will be added. |
| Add | Adds the specified header.<br>Note: If the header already exists, it will be overwritten for uniqueness. |
| Delete | Deletes the specified header. |

## Must-knows

- A custom header parameter must be in the following format:
  - Parameter name: It can contain 1–100 digits, letters, and hyphens.
  - Parameter value: It can contain 1–1000 characters.
- During one HTTP request header modification operation, you can add up to 30 headers of different types, which will be executed in sequence from top to bottom.
- The following standard headers cannot be modified:

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

# Configuration Samples

### Access-Control-Allow-Origin

This header requests permission to access cross-origin resources, so as to implement CORS.

- Header name: Access-Control-Allow-Origin.
- Header value: Enter domain names and/or IPs starting with "http://"/"https://", separated by commas (up to 1000 characters). Note that wildcards (*) can be used. Example: `http://test.com,http://1.1.1.1` .
- Value description:

| Header value | Description |
| --- | --- |
| * | Matches all origins:<br>The header `Access-Control-Allow` is included in the response to allow reque origins. |

| Header value | Description |
| --- | --- |
| `http://www.tencentcloud.com`, `https://www.tencentcloud.com`, `http://www.b.com` | Matches specific origins:<br>◦ The origin `https://www.tencent` hits the list of allowed origins, so the he `Access-Control-Allow-Origi` `https://www.tencentcloud.cor` in the response.<br>◦ The origin `https://www.qq.com` the list, so the Access-Control-Allow-C not present. |
| `https://*.tencent.com` | Matches origins by second-level wildcard name:<br>◦ The origin `https://www.tencent` hits the list of allowed origins, so the he `Access-Control-Allow-Origi` `https://www.tencentcloud.cor` in the response.<br>◦ The origin `https://cloud.qq.cc` the list, so the Access-Control-Allow-C not present. |
| `https://cloud.tencent.com:8080` | Matches origins by port:<br>◦ The origin `https://cloud.tencent.com:8` list of allowed origins, so the header `Access-Control-Allow-Origin:https://cloud.tencent` is included in the response.<br>◦ The origin `https://www.tencent` doesn't hit the list, so the Access-Cont Origin header is not present.<br>Note: A special port used by the origin added to the header value. |

### Access-Control-Allow-Methods

This header specifies the HTTP request methods allowed for cross-origin access.

- Header name: Access-Control-Allow-Methods.
- Header value: Multiple values can be set, such as `POST`, `GET`, and `POTIONS`.

### Access-Control-Max-Age

This header specifies the validity period of the result of a preflight request in seconds.

> Note：
> A non-simple CORS request requires a preflight request (that uses HTTP request methods) before being initiated. It is made to check whether the CORS request is secure and acceptable. Typical cases requiring preflight requests:
> A CORS request uses methods other than `GET`, `HEAD`, and `POST` or is initiated via `POST` with the request data type other than `application / x-www-form-urlencoded`, `multipart / form-data`, and `text / plain` (such as `application / xml` or `text / xml`).

- Header name: Access-Control-Max-Age.
- Header value: Enter the number of seconds, for example, `1728000`.

### Content-Language

This header specifies the language to be used by the accessed page.

- Header name: Content-Language.
- Header value: `zh-CN` or `en-US`.

### Content-Disposition

This header activates download in the browser and sets the default name of the downloaded file.

When the server sends a file supported by the client browser (such as a TXT or JPG file), the browser opens the file by default. If you want to ask the user to save the file, configure the `Content-Disposition` field to override the browser's default behavior.

- Header name: Content-Disposition.
- Header value: `attachment;filename=FileName.txt`.

# Modifying HTTP Request Headers

Last updated：2023-02-22 17:28:26

## Overview

You can customize, add, and delete headers in HTTP origin-pull requests from nodes to the origin.

> Note：
> EdgeOne forwards `X-Forwarded-For` and `X-Forwarded-Proto` to the origin by default, so you don't need to configure them.

## Directions

1. Log in to the EdgeOne console. Click **Rule Engine** on the left sidebar.
2. On the page that displays, select the target site and create rules to configure HTTP request headers as needed. For more information, see Overview.
   Description of configuration items:

| Type | Description |
| --- | --- |
| Set | Sets the specified header to the specified value. The header must be unique.<br>Note: If the specified header does not exist, it will be added. |
| Add | Adds the specified header.<br>Note: If the header already exists, it will be overwritten for uniqueness. |
| Delete | Deletes the specified header. |

   Description of header types:

| Header Type | Description |
| --- | --- |
| Custom | Custom header.<br>◦ Name: Must be between 1-100 characters, containing numbers, letters and special symbols ( `-` ).<br>◦ Value: Must be between 1-1000 characters. |

| Header Type | Description |
| --- | --- |
| Preset | `User-Agent` header, which contains information about the client:<br>◦ `EO-Client-Device`: The device that the client uses.<br>Values: `Mobile`, `Desktop`, `SmartTV`, `Tablet`, `Others`.<br>◦ `EO-Client-OS`: The OS that the client uses.<br>Values: `Android`, `iOS`, `Windows`, `MacOS`, `Linux`, `Others`.<br>◦ `EO-Client-Browser`: The web browser that the client uses.<br>Values: `Chrome`, `Safari`, `Firefox`, `IE`, `Others`. |

# Notes

- During one HTTP request header modification operation, you can add up to 30 headers of different types, which will be executed in sequence from top to bottom.
- The following standard headers cannot be modified:

| | | | |
| --- | --- | --- | --- |
| Host | Content-Length | If-Modified-Since | Etag |
| Accept-Encoding | Last-Modified | Content-Range | Content-Type |
| X-Cache-Lookup | X-Last-Update-Info | Transfer-Encoding | Content-Encoding |
| Connection | Range | Server | Date |
| Location | Expect | Cache-Control | Expires |
| Referer | User-Agent | Cookie | X-Forwarded-For |
| Accept-Language | Accept-Charset | Accept-Ranges | Set-Cookie |
| Via | X-Via | Pragma | Upgrade |
| If-None-Match | If-Match | If-Range | From-Tencent-Lego-Cluster |
| From-Tencent-Lego-Cluster-Client-Info | From-Tencent-Lego-Cluster-Edge-Server-Info | From-Tencent-Lego-Dsa | From-Tencent-Lego-Dsa-Client-Info |
| From-Tencent-Lego-Dsa-Edge-Server-Info | Accept | Upgrade-Insecure-Requests | Server-Timing |
| Age | Proxy-Connection | Authorization | Proxy-Authorization |

| Host | Content-Length | If-Modified-Since | Etag |
| --- | --- | --- | --- |
| normal | multirange | chunked | identity |
| keep-alive | close | upgrade | x-redirect-to-self |
| From-Tencent-Lego-Overload | - | - | - |

# Custom Error Page

Last updated：2023-02-22 17:28:26

## Overview

You can redirect requests to a custom error page for specific error status codes returned by the origin. The redirection is performed when a 302 is returned.

> Note：
> Only status codes returned for origin-pull requests are supported.

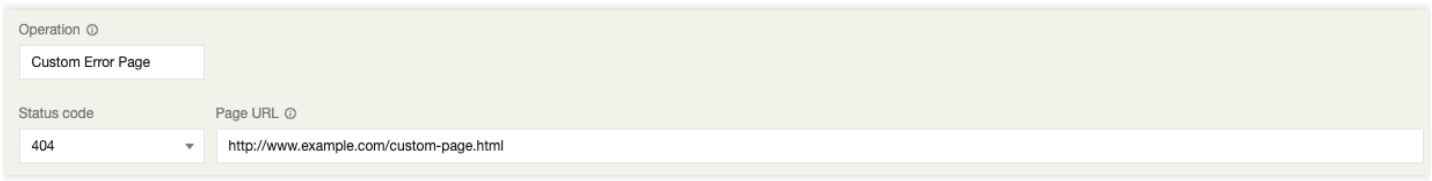
## Directions

1. Log in to the EdgeOne console. Click **Rule Engine** on the left sidebar.
2. On the page that displays, select the target site and create rules for configuring a custom error page as needed. For more information, see Overview.
   Parameters:

| Configuration Item | Description |
| --- | --- |
| Status code | Specifies the error status code returned by the origin:<br>◦ 4XX: 400, 403, 404, 405, 414, 416, 451<br>◦ 5XX: 500, 501, 502, 503, 504 |
| Page address | Specifies the error page address, such as `http://www.example.com/custom-page.html` |

## Configuration Sample

The following configuration sample shows how to redirect requests to a custom error page for the 404 Not Found error:



# Origin Configuration
# Origin Group
# Origin Group List

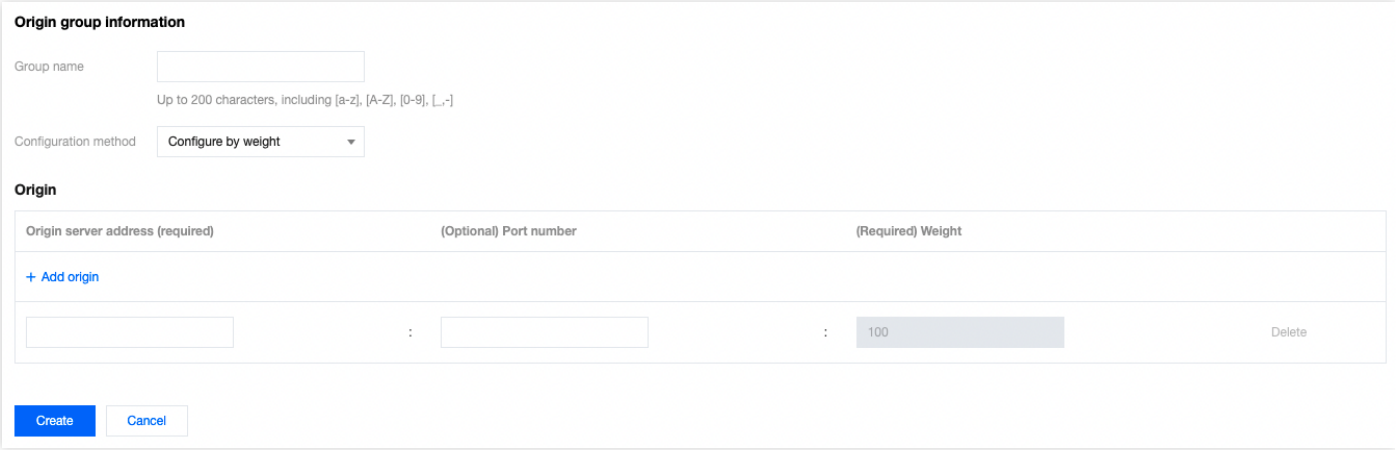
Last updated：2022-12-13 16:25:41

## Overview

You can manage business origin servers by origin group. The configured origin group can be used by the load balancing and layer-4 proxy features as needed.

## Directions

1. Log in to the EdgeOne console and click **Origin Configuration** > **Origin Group** on the left sidebar.
2. On the origin server group page, select the target site and click **Create origin group**.
3. On the origin group creation page, configure relevant parameters and click **Create**.




**Parameter description:**

- Group name: Origin group name or description, which must be unique and can contain 1–200 letters, digits, underscores, and hyphens.
- Origin type: Type of the origin server, which can be customer origin, object storage origin, or Tencent Cloud COS.

- Customer origin: It is the customer's origin server storing business resources, which can be an IP or a domain name.
- Object storage origin: It is a third-party object storage origin server, which is a bucket address for which private access can be enabled. Now only Amazon Web Services S3 is supported.
- Tencent Cloud COS: Select a Tencent Cloud COS bucket under the current account as origin.

- Configuration method: If you select **Customer origin** as the origin type, you can select:
  - Configure by weight: Origin-pull by weight.

    Note：
    - If there is only one origin server, the weight is set to 100 by default and cannot be adjusted.
    - If there is more than one origin server, specify weights in the range 1-99.

- Configure by region: Origin-pull by client IP region.

  Note：
  - **All** is the default global rule, which cannot be deleted.
  - If multiple rules have the same region, the higher the rule position, the higher the priority.

- Configure by HTTP protocol: Origin-pull by the HTTP protocol of the client request.

  Note：
  Configure at least one origin address for the HTTPS and HTTP protocols respectively.

## Customer origin configuration restrictions

- You can add up to 100 origin server addresses to a single origin server group but cannot enter IPv4 and IPv6 addresses together.

  Note：
  Currently, only certain nodes support IPv6 origin-pull.

- Port number: Specify a port in the range 1-65535.
- If an origin group is used by load balancing, then:
- If the proxy mode is **Only DNS**, you cannot configure a port for origin server addresses or enter IPs and domains together as origin servers.
- If an origin group is used by L4 proxy, then:
  - All origin server addresses must be configured with a port.
  - **Configure by region** and **Configure by HTTP protocol** are not supported.
  - You can configure only one domain origin server but cannot enter it together with IP origin servers.
  - Currently, L4 proxy doesn't support IPv6 origin-pull. Therefore, IPv6 origin servers cannot be configured.

# Origin Health Check

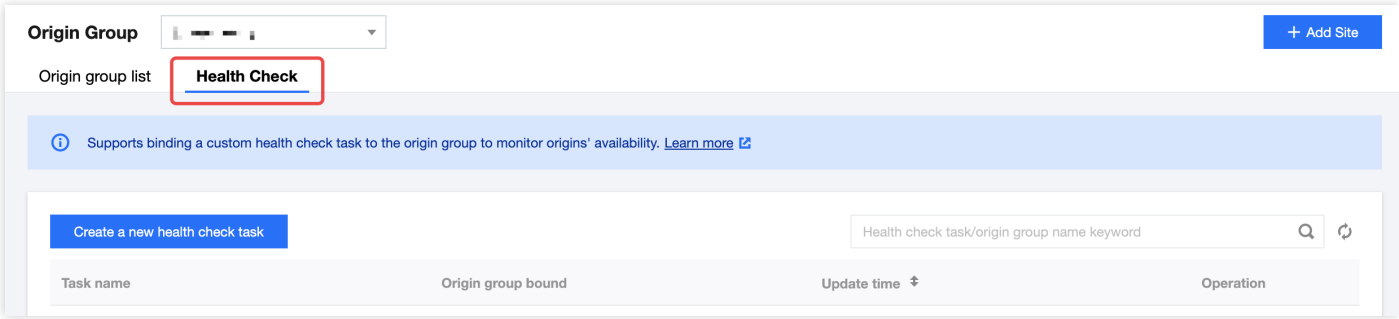
Last updated：2022-10-18 10:34:21

## Overview

A health check task can be created to monitor the availability and health of an origin group. The origin group is considered healthy when it responds appropriately to origin-pull requests, otherwise it is in an unhealthy state.

## Directions

1. Log in to the EdgeOne console. Select **Origin Configuration** > **Origin Group** on the left sidebar. Switch the tab to **Health check**.




2. On the page displayed, select a target site to create or edit a health check task.

- Create a health check task: Click **Create health check task**, enter the required parameters, and click **Create**.

| Parameter | Description | Remarks |
| --- | --- | --- |
| Select origin group | Select one or more origin groups. | • The origin groups that you select must be used in domain service, i.e., these origin groups are bound to load balancing tasks.<br>• For multiple origin groups bound to the same domain name, associate them with the same health check task.<br>• <7>L4 proxied origin groups are not supported currently. |

| Parameter | | Description | Remarks |
| --- | --- | --- | --- |
| Configure health check task | Task name | Name of the health check task. | - |
| | URL | Request URL. The default path is `/`. | - |
| | HTTP method | HTTP request method. | - |
| | Check frequency | How often this health check task is initiated. | Checking frequently can detect origin failures more timely, but the origin load will be increased. |
| | Timeout period | The amount of time to wait for a response from an origin group until it is considered unhealthy. | - |
| | HTTP status code | HTTP status codes to be expected from a healthy origin group. | - |
| | Retries | The number of times to retry when the health check result is unhealthy. | - |
| | Healthy origins | The number of healthy origin servers required to consider an origin group healthy. | This parameter determines the health status of an origin group based on the number of healthy origin servers. A origin group may contain more than one origin server. |
| | Healthy threshold | The number of consecutive successes required for an origin group to be considered healthy and available. | - |
| | Follow redirect | Whether to follow 301/302 redirects (3 redirects by default). When it's on, a 301/302 code is returned to report a healthy status. | - |
| | Custom request header | Custom request header to send when a health check is initiated. | - |

- Edit a health check task: Click **edit** on the right of the target task. Modify the parameters and click **Save**.

## Must-knows

1. If an origin group is used for multiple load balancing tasks at the same time, its health is determined based on different load balancing tasks. Suppose an origin group is considered healthy in load balancing task A, while considered unhealthy in load balancing task B. In this case, EdgeOne will notify you via the console, Message Center, email and SMS.
2. If the health check task is not bound to any origin group, or the bound origin group is no longer used for load balancing, the health check task will be suspended.

# Cloud Load Balancer

Last updated：2022-12-13 16:25:41

## Overview

Load balancing dynamically optimizes origin-pulls and intelligently assigns traffic to effectively avoid failed origin servers and reduce origin server overloads, ensuring the availability of the entire service.

> Note：
> Load balancing can be performed by region or weight.

## Directions

1. Log in to the EdgeOne console and click **Origin Configuration** > **Cloud Load Balancer** on the left sidebar.
2. On the load balancing page, select the target site and click **Create load balancing task**.
3. On the load balancing creation page, configure the relevant parameters and click **Submit task**.

**Parameter description:**

- Hostname: Domain name of a site, which is accessed on the origin server during origin-pull.

  > Note：
  > - To set an origin domain different from the acceleration domain when you bind a customer origin server, you can use host header rewriting to rewrite the host header to the actual origin domain.
  > - If the hostname conflicts with existing DNS records, the load balancing configuration takes higher priority and will overwrite the records in Domain Name Service.

- Proxy: **Proxy acceleration** or **Only DNS**.
  - Proxy acceleration: EdgeOne will automatically deliver security/acceleration configuration for the host record (subdomain name) according to your plan.
  - Only DNS: EdgeOne will only provide DNS resolution.

- TTL: If you select **Only DNS** for **Proxy** and select **NS access**, the TTL is configurable.

- Origin: If you select **Proxy acceleration** for **Proxy**, you can select primary/secondary origin-pull and advanced origin-pull configuration.
  - Primary/Secondary origin-pull: You can configure up to two origin groups, and requests will be forwarded to them by priority. Only when the origin group at priority 1 fails and becomes unavailable will requests be forwarded to the group at priority 2. This implements the concept of primary/secondary origin groups.
  - Advanced origin-pull configuration: You can configure the load balancing origin server based on the matched URL path.

> Note：
>
> - If you select the **Only DNS** mode, you can configure only one origin group.
> - If you select the **Proxy acceleration** mode, you can configure up to two origin groups, and requests will be forwarded to them by priority. Only when the origin group at priority 1 fails and becomes unavailable will requests be forwarded to the group at priority 2. This implements the concept of primary/secondary origin groups.
> - Secondary object storage origin groups are not supported.

4. On the load balancing page, you can view a created task. Each task has a deployment status.

- Deploying: The current load balancing task is being deployed and cannot be deleted.
- Running: The current load balancing task is taking effect in the production environment and cannot be deleted. You need to disable it before you can delete it.
- Disabled: The current load balancing task is disabled.

# FAQs

### Why are some origin groups grayed out during origin server configuration?

- The grayed out origin group conflicts with the currently selected proxy mode in the following situations:
  - A port has been configured for an origin server in the origin group, so the group cannot be used in **Only DNS** mode.
  - The origin group has an IPv6 origin server, so the group cannot be used in **Only DNS** mode.
  - The origin group has both IP and domain origin servers, so it cannot be used in **Only DNS** mode.
- The maximum number of configurable origin groups is reached:
  - If you select the **Only DNS** mode, you can configure only one origin group.

  - If you select the **Proxy acceleration** mode, you can configure up to two origin groups.
- Grayed-out origin groups are object storage origin servers with private access enabled:
  - Secondary object storage origin servers cannot be created currently.

# Host Header Rewrite

Last updated：2022-10-18 10:50:16

## Overview

Host header rewriting enables you to rewrite the host header to the actual origin domain when the origin domain is different from the acceleration domain in the load balancing task.

## Directions

1. Log in to the EdgeOne console. Select **Origin Configuration** >**Rule Engine** on the left sidebar.

2. On the rule engine page, select the target site and click to configure host header rules as needed.
3. On the rule engine page, select **Host** for the match type and **Rewrite host header** for the action, and configure other parameters as needed. Click **Save and publish** or **Save only**.

> Note：
> Supported match types: "Host".

# Range GETs

Last updated：2022-10-18 10:55:43

## Overview

Range GETs can be enabled to reduce the consumption of large file origin-pulls and response time.

**Why can Range GETs improve the efficiency of large file delivery?**

When caching large files, nodes will split them into smaller parts in order to improve cache efficiency. All parts cached expire at the same time and follow the node cache TTL configuration. Range requests are also supported. For example, if a client request carries the HTTP header `Range: bytes = 0-999`, only the first 1000 bytes of the file will be returned to the user.

If Range GETs is enabled: When parts of the file are requested and their caches expire, nodes only pull and cache the requested parts and return them to the user, so that origin-pull consumption and response time are greatly reduced.

If Range GETs is disabled, when the client requests only parts of a file, the node will pull only the requested parts according to the `Range` header in the client request, cache them, and return them to the client at the same time. However, this may not be able to achieve the optimal performance. In large file scenarios, we recommend you enable Range GETs.

## Use Cases

You can use Range GETs to cache large static files in either of the following cases: The origin server supports Range requests, or you use a Tencent Cloud COS origin server and do not apply any data processing methods such as image processing.

## Notes

- The origin server must support Range requests, or the origin-pull may fail.
- The origin-pull may fail if Range GETs is enabled for small static files, or if you enable it while using a Tencent Cloud COS origin server and data processing methods such as image processing.

## Directions

1. Log in to the EdgeOne console. Select **Origin Configuration** > **Rule Engine** on the left sidebar.

2. On the rule engine page, select the target site and click to configure Range GETs rules as needed.
3. On the rule engine page, select the operation **Range GETs** and configure other parameters as needed. Click **Save and publish** or **Save only**.

> Note：
> Currently, supported match types include host, URL path, and file extension.

# HTTP/2 Origin-Pull

Last updated：2022-10-18 11:00:25

## Overview

Request origin-pull over the HTTP/2 protocol is supported.

**What is HTTP/2?**

Hypertext Transfer Protocol Version 2 (HTTP/2 or HTTP 2.0) is the second major version of the HTTP protocol. It can effectively reduce the network latency and accelerate site page loading.

## Directions

1. Log in to the EdgeOne console and Select **Origin Configuration** > **Rule engine** on the left sidebar.

2. On the rule engine page, select the target site and click to configure HTTP/2 origin-pull rules as needed.

> Note：
> Currently, you can configure HTTP/2 origin-pull rules only if the match condition is **Host**.

Parameter description:

| Switch Status | Description |
| --- | --- |
| Enabled | Request origin-pull over the HTTP/2 protocol is enabled.<br>Note: It can take effect only if the origin server supports origin-pull over the HTTPS protocol. |
| Disabled | Request origin-pull over the HTTP/2 protocol is disabled. |

# Redirect Following During Origin-Pull

Last updated：2022-12-16 09:24:36

## Overview

When origin-pull is requested, the redirect will be based on the 302/301 status code of the origin server, and you can specify the maximum number of redirects (which is 3 by default and can be 1–5).

## Use cases

Nodes do not cache 301/302 status codes by default. When an origin server returns a 301/302 request, the node will return the response to the client by default, and the client will be redirected to the corresponding resource for access.

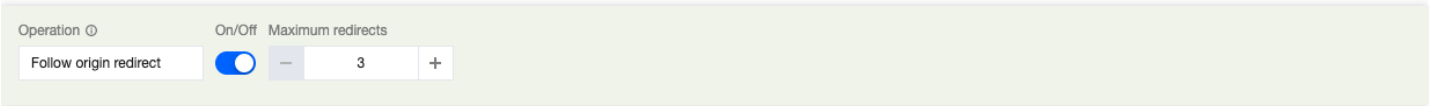
You can enable redirect following during origin-pull. Then, when the 301/302 status code is returned, the request will be automatically redirected (for up to the maximum number of times that is set). If the requested resource is obtained, the node will return it to the client, which no longer needs to be redirected.

## Directions

1. Log in to the EdgeOne console and click **Rule engine** on the left sidebar.
2. On the **Rule engine** page, select the target site and configure the redirect following rule during origin-pull as needed. For more information, see Overview.

## Sample configuration

If the host `www.example.com` is configured with the redirect following rule during origin-pull as follows:




Then, if user A requests a resource `http://www.example.com/a` not cached on the node, the node will request it from the origin server. If the HTTP response status code returned by the origin server is 302, and the redirect address is `http://www.example.com/b`, then:

1. The node sends a request to the `http://www.example.com/b` redirect address.

2. If the requested resource is obtained within three redirects, see 3; otherwise, see 4.
3. The resource is cached on the node and sent to user A. At this time, user B also sends a request for `http://www.example.com/a`, which will be directly hit on the node and returned to user B.
4. The 301/302 status code is returned to the user, and the client is redirected once more.

# Controlling Origin-pull Requests

Last updated：2023-02-22 17:28:26

## Overview

You can specify which part of the query string and Cookie to be included in the request when it's forwarded to the origin. Note that this configuration does not affect node caching.

## Use Cases

1. Allow the origin to serve resources based on the query string or Cookie.
2. Ensure a successful origin-pull by ignoring the authentication parameter in the request.

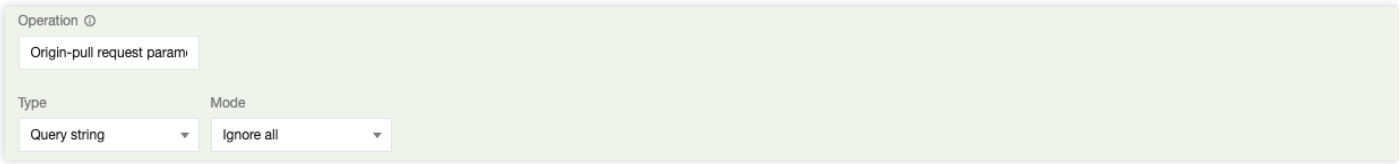
## Directions

1. Log in to the EdgeOne console. Click **Rule Engine** on the left sidebar.
2. On the page that displays, select the target site and create rules for origin-pull request parameters as needed. For more information, see Overview.
   Description of configuration items:

| Configuration Item | Description |
| --- | --- |
| Query string | Modify the query string in the URL. By default, all query parameters included in the request. |
| Cookie | Modify the Cookie. By default, all cookie parameters are included in the request. |

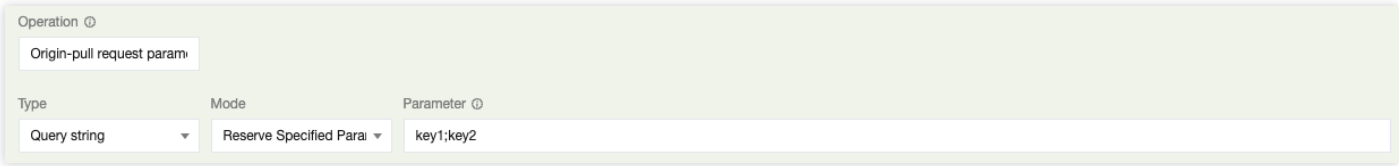
## Configuration Samples

- If the request contains the authentication parameter in the query string, ignore the authentication parameter before origin-pull as follows:



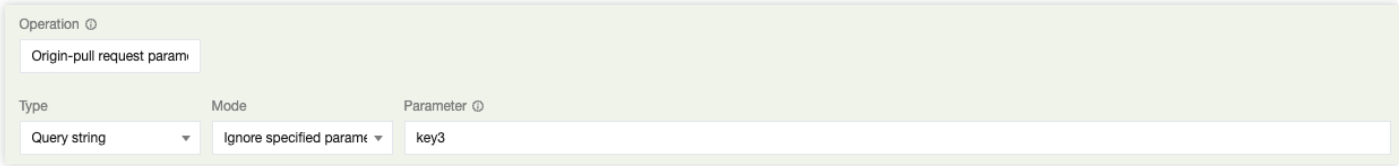

Client request URL: `http://www.example.com/path/demo.jpg?abc=18867530-chgdksbvhjsbvdjhsbvfj12` ( `abc` is the authentication parameter.)
Origin-pull request URL: `http://www.example.com/path/demo.jpg`

- To include the `key1` and `key2` query parameters in the request, ignore the rest part of the query string before origin-pull as follows:




Client request URL: `http://www.example.com/path/demo.jpg?key1=a&key2=b&key3=c&key4=d` and `http://www.example.com/path/demo.jpg?key1=a&key2=b&key3=c&key4=d&key5=e`
Origin-pull request URL: `http://www.example.com/path/demo.jpg?key1=a&key2=b`

- To exclude the `key3` query parameter in the request, ignore it before origin-pull as follows:




Client request URL: `http://www.example.com/path/demo.jpg?key1=a&key2=b&key3=c&key4=d`
Origin-pull request URL: `http://www.example.com/path/demo.jpg?key1=a&key2=b&key4=d`

# Domain alias Configuration Guide

Last updated：2022-12-13 15:59:01

This document describes how to create, edit, and delete a domain alias, configure the CNAME record of the domain alias to point to the target domain name, and configure a certificate for the domain alias.

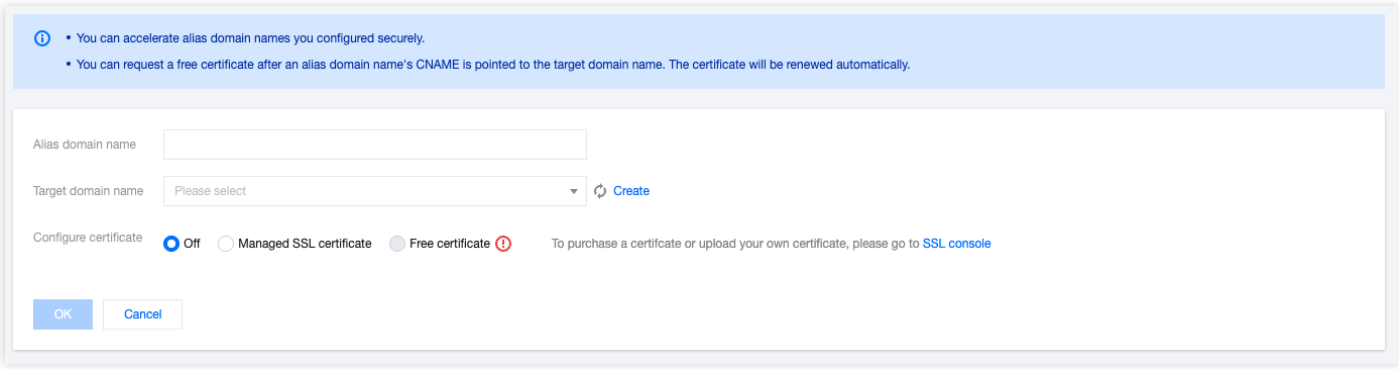
## Prerequisites

You have purchased the EdgeOne Enterprise plan, connected your site, and created the target domain name.

## Creating a Domain Alias

### Step 1. Create a domain alias

1. Log in to the EdgeOne console and click **Domain Alias** on the left sidebar.
2. On the domain alias list page, click **Create domain alias**, configure parameters, and click **OK**.

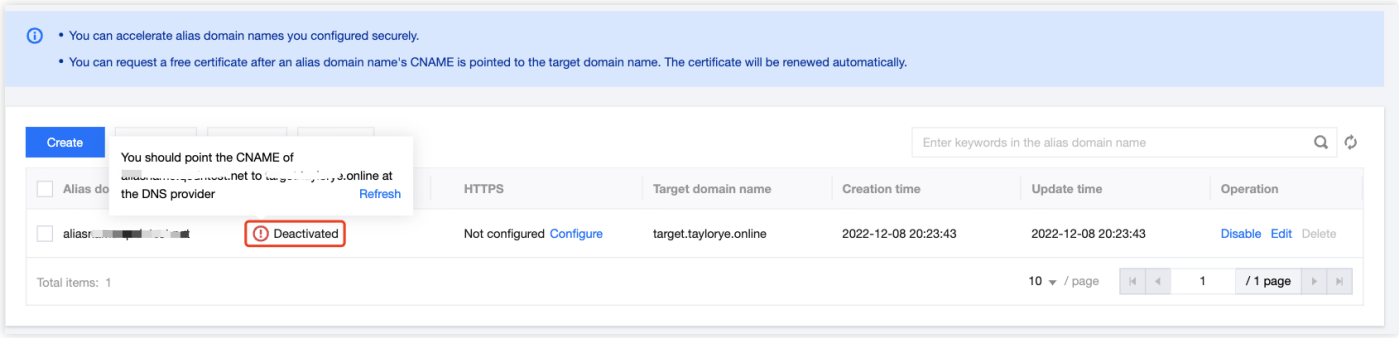



| Parameter | Description |
| --- | --- |
| Domain alias | It can contain up to 81 characters. Wildcard domain names such as `*.test.com` are not supported. If the acceleration region of your site is in the Chinese mainland, you need to get an ICP filing for your domain alias. |
| Target domain name | You can select a domain name of the current site in the **Activated** or **Deploying** status. For more information, see CNAME Connection and NS Connection. |

| Parameter | Description |
| --- | --- |
| Certificate configuration | ◦ Do not configure: It indicates not to configure the HTTPS certificate. If you select this option, the domain alias has only HTTPS access capabilities.<br>◦ SSL managed certificate: It indicates to select a certificate managed in SSL. To purchase or upload an external certificate, contact us.<br>◦ Apply for free certificate: The platform implements the application and automatic update of free certificates. To select this option, add a domain name and point the CNAME record of the domain alias to the target domain name at your DNS service provider. |

## Step 2. Add the CNAME record of the domain alias that points to the target domain name

1. After the domain alias is added successfully, it is **not activated** by default as shown below:

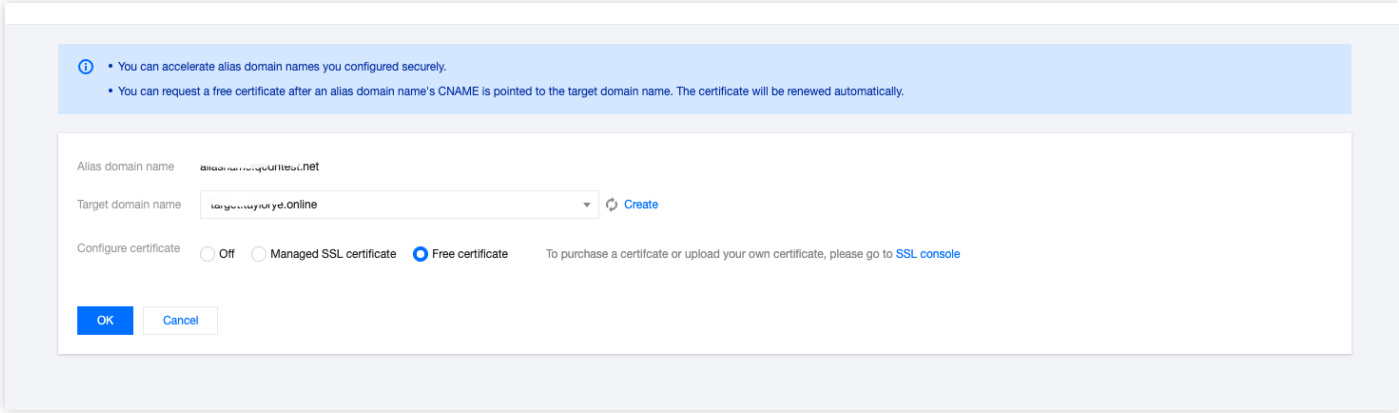



2. Go to your DNS service provider and add a CNAME record that points to the target domain name to activate the domain alias.
3. EdgeOne will automatically perform a check and change the status of the domain alias to **Activated**.

## Step 3. Apply for a free certificate (optional)

If you have pointed the CNAME record of the domain alias to the target domain name at your DNS service provider, you can apply for a free certificate in EdgeOne.

1. On the domain alias list page, click **Edit** and select **Apply for free certificate**.




2. Click **OK**.

## Editing a Domain Alias

1. On the domain alias list page, select the target domain alias and click **Edit**.
2. Modify the target domain name and certificate configuration type as needed and click **OK**.

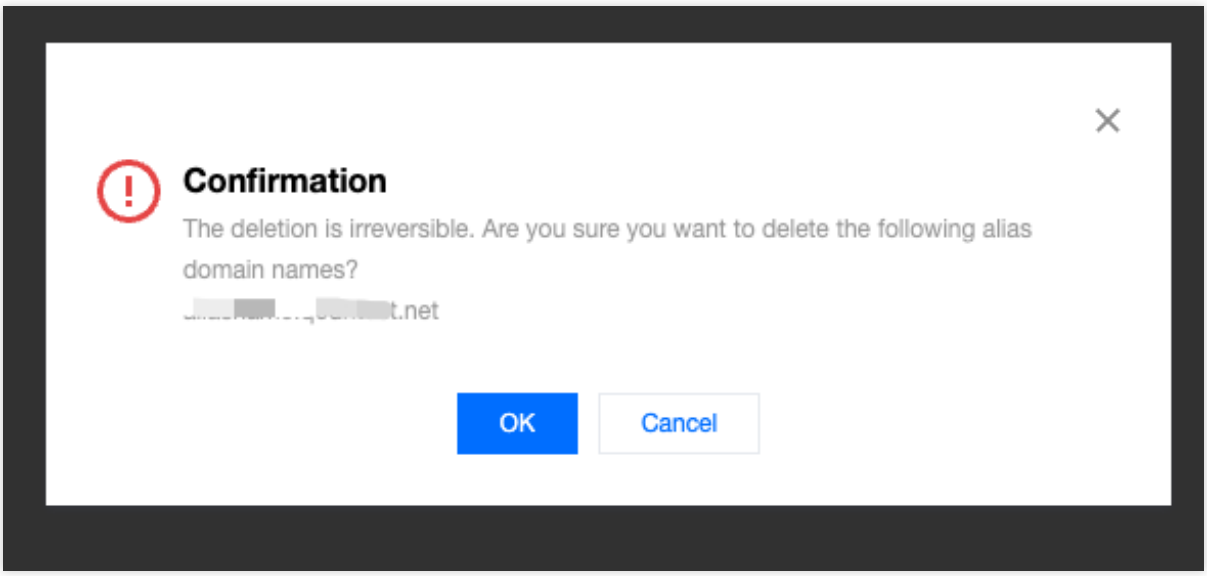
## Deleting a Domain Alias

Note：

- A domain alias not disabled cannot be directly deleted.
- The data cannot be recovered once a domain alias is deleted. Proceed with caution.

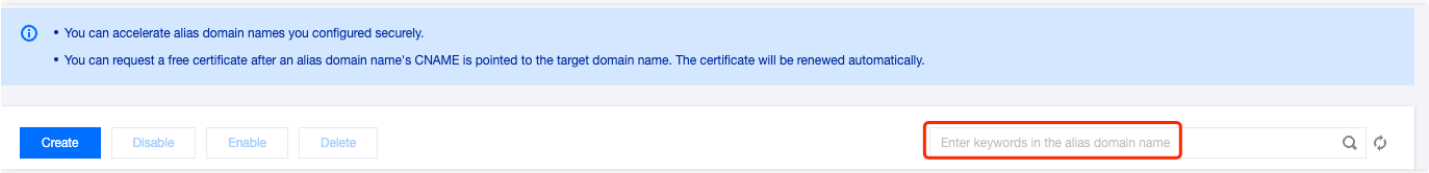
1. On the domain alias list page, select the target domain alias and click **Disable** > **Delete**.

2. In the pop-up window, click **OK**.




## Searching for a Domain Alias

On the domain alias list page, enter a keyword in the search input box and press Enter to search for a domain alias.



# Rule Engine
# Overview

Last updated：2023-02-22 17:28:26

## Rule Engine

Leveraging rich rule languages, the rule engine allows you to customize rules for specific request types. Custom rules will overwrite the default behaviors of the edge server.

## Use Cases

- Provide custom configurations based on different conditions (subdomain name, path and file extension) when site-level configuration in **Site Acceleration** cannot meet your needs.
- Provide basic features (caching and HTTPS) and acceleration features (custom cache key, URL rewrite and HTTP header modification).

## Directions

1. Log in to the EdgeOne console. Click **Rule Engine** on the left sidebar.
2. On the **Rule engine** page, select the target site and click **Add rule**.
3. In the pop-up window, configure parameters and submit the rule:
   - Save only: Saves the rule but does not publish it to the production environment.
   - Save and publish: Saves and publishes the rule to the production environment.

## Key Terms

| Term | Description |
| --- | --- |
| Rule | A rule identifies specific types of requests and the series of operations applied to them. It includes:<br>• A set of conditional expressions that define the logic for request identification.<br>• A set of conditions that define the criteria for request identification.<br>• A set of features that define how CDN processes requests. |

| Term | Description |
| --- | --- |
| Conditional expression | It defines the logic for identifying a request and is available in the following types:<br>• IF<br>Note: An IF statement can be nested inside another IF statement, indicating that the nested one will be executed only after the other is met.<br>• ELSE IF<br>• ELSE |
| Condition | It defines the criteria for identifying a request, including:<br>• Matching type<br>• Operator<br>• Value |
| And/Or | Logical AND/OR, which can link multiple conditions. |
| Operation | A wide range of feature configurations that can be applied to hit requests. |

# Rule Precedence

| Scope | Description |
| --- | --- |
| Rule engine | The rule engine takes precedence over the site acceleration configuration. |
| Single rule in the rule engine | Rules are executed from top to bottom in sequence. The bottom rule has a higher priority and is the configuration that eventually takes effect. |
| Multiple rules in the rule engine | Rules are executed from top to bottom in sequence. The bottom rule has a higher priority and is the configuration that eventually takes effect.<br>Note: You can place general or coarse-grained rules at the top as the default configuration and request-specific or finer-grained rules at the bottom. |

### Notes

The following operation is not subject to the execution order:

- Token authentication
  Token authentication will be executed first no matter where it is placed. If a request hits two rules, token authentication will be executed first even if it is at the bottom, as other operations will be performed only after authentication is passed.

# Condition

Last updated：2022-12-13 16:40:38

## Notes

A condition defines the standard for identifying a request, including:

- Matching type
- Operator
- Value

## Matching Type

| Type | Description | Value (Sample) |
| --- | --- | --- |
| HOST | Request host | `www.example.com` |
| URL Path | Request URL path | `/example/foo/bar` |
| URL Full | Complete request URL | `https://www.example.com/foo` |
| Query string | Query string in the request URL | Parameter name: `key`<br>Parameter value: `value` |
| File extension | File extension of the request content | jpg, png, css |
| Filename | Filename of the request content | foo.txt |
| HTTP request header | HTTP request header | Header name: `name`<br>Header value: `value` |
| Country/Region of the client | Country/Region of the client IP | US |
| All | Any site request | - |

## Operator

| Type | Description |
| --- | --- |

| Type | Description |
| --- | --- |
| Equal to | The request is equal to a specified value (value of the matching type). |
| Not equal to | The request is not equal to a specified value (value of the matching type). |
| Exist | A specified value exists in the request (HTTP header name or query parameter name). |
| Not exist | A specified value does not exist in the request (HTTP header name or query parameter name). |
| Find matching items via regex | It supports Google RE2 regular expressions. |

# Value

It indicates the content of the selected matching type.

### Wildcard

You can enter content containing wildcards for certain matching types:

| Type | Description | Value (Sample) |
| --- | --- | --- |
| * | Matches 0 or multiple characters | If the `URL Path` is `/foo/*/bar`, both `/foo/example/bar` and `/foo/demo/bar` are valid values. |

### Ignoring the case

You can modify the case sensitivity of certain matching types. By default, they are case sensitive. If you enable the **Ignore case** switch, they will be case insensitive.

# Operation

Last updated：2023-02-22 17:28:26

## Notes

A series of configurations are applied to the hit request, including:

| Operation | Description |
| --- | --- |
| Access control | Token Authentication |
| | Video Dragging |
| Cache configuration | Node Cache TTL |
| | Browser Cache TTL |
| | Offline Caching |
| | Status Code Cache TTL |
| | Custom Cache Key |
| | Node Cache Prefresh |
| Network optimization | HTTP/2 |
| | HTTP/3 (QUIC) |
| | WebSocket |
| | Maximum Upload Size |
| | Real Client IP Header |
| | Client IP Geographical Location |
| URL rewrite | Access URL Redirection |
| | Origin-Pull URL Rewrite |
| Origin-pull optimization | Smart Acceleration |
| | HTTP/2 Origin-Pull |

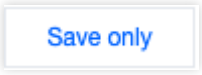
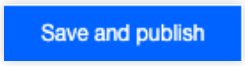
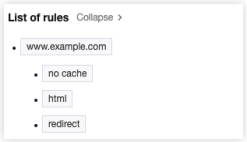
| Operation | Description |
| --- | --- |
| | Range GETs |
| | Following Origin Redirects |
| | Controlling Origin-pull Requests |
| HTTPS configuration | HTTPS Configuration |
| | Origin-Pull HTTPS |
| | HTTPS Configuration |
| | TLS version |
| | OCSP stapling |
| HTTP header modification | Modifying HTTP Request Header |
| | Modifying HTTP Response Header |
| | Host Header Rewrite |
| Advanced configuration | Custom Error Page |

# Rule Management

Last updated：2022-12-13 16:25:41

The console supports a series of icons and buttons to manage rules, for example, sorting, copying, enabling, and disabling rules, as follows.

| Icon/Button | Description |
| --- | --- |
|  | Drags a rule up or down. |
|  | Pins a rule to the top. |
|  | Pins a rule to the bottom. |
|  | Edits a rule. |
|  | Creates the same rule as the copied rule. |
|  | Deletes a rule. |
|  | Searches for a rule by rule name or keyword. |
|  | Rule status<br>• Enable: Publishes a rule to the production environment.<br>• Disable: Saves a rule but does not publish it to the production environment. |

| Icon/Button | Description |
| --- | --- |
|  | Saves a rule but does not publish it to the production environment. |
|  | Saves and publishes a rule to the production environment. |
|  | If a single rule is complex and has multiple IF statements, you can add comments to them. Then, the rule navigation will be automatically generated on the right of the rule content to simplify viewing and locating. |