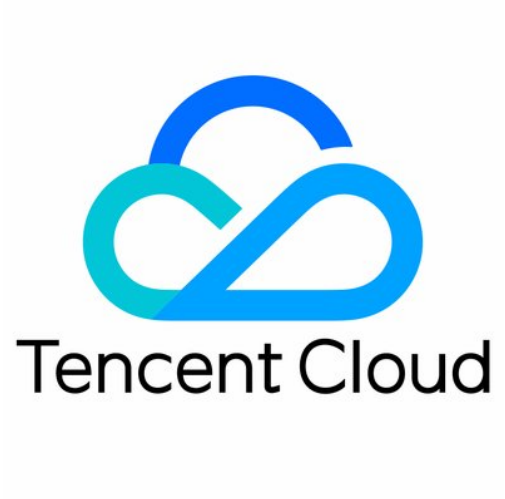
Tencent Cloud EdgeOne

FAQs

Product Documentation



Contents

FAQs
- Reference for Abnormal Status Codes
- Product Features FAQs
- Domain Service FAQs
- Site Acceleration FAQs
- Data and Log FAQs
- Security Protection-related Queries

FAQs

Reference for Abnormal Status Codes

Last updated：2023-12-06 11:03:23

EdgeOne responds with the following types of exception status codes:

Standard Status Codes

You can refer to the HTTP Status Code Standard to see the specific meanings of these status codes.

These codes are typically responded to in the following situations:

After the request is sent back to the origin, the status code information is responded by the origin server, and the node will pass transmit status code from the origin server to the client.

Direct responses from EdgeOne nodes, for example, Token authentication fails, responding with a 403 status code.

Possible status codes that may be directly responded by EdgeOne nodes include the following status ones:

Status Code	Description
400	The client's request is deemed invalid because the requested method is not within the allowed range set by EdgeOne.
403	Fail to pass the link protection verification, such as the Token authentication in the rule engine.
416	Range exception, for example, rangeStart < 0,< 0, rangeStart > rangeStart > rangeEnd, or rangeStart > FileSize.
418	For each domain name connected to EdgeOne, the system automatically allocates service nodes for the domain. Each corresponding node receives the domain's configuration file, which includes settings such as the origin server, cache, headers, etc. When a request is sent to a node, it reads the domain's configuration file. If the file is not found, the node responds with a 418 status code. For example, if a client sends a request to `http://example.com/test.jpg` , the node reads the configuration file for the domain `example.com` . If, due to reasons such as the service node binding to a `non-example.com` domain name, CNAME configuration errors, or issues with the scheduling system, the configuration file is not found, the client will receive a 418 response.
423	There are two scenarios that can trigger a looping request: When the Loops value in the CDN-Loop header is ≥ 16. For more details, see CDN-Loop. When the same request passes through the same node device twice.

EdgeOne Custom Status Codes

EdgeOne defines special status codes with unique meanings. Status codes within the range of 499 and 520-599 are reserved by EdgeOne for custom non-standard responses. It is recommended to avoid using status codes within this range in your business to prevent confusion with EdgeOne's status codes.

Below are the custom EdgeOne status codes along with their meanings, facilitating self-troubleshooting when encountering abnormal business access.

Status Code	Meaning Explanation
499	The client's request reaches the node, and if the client disconnects before receiving a response from the node, such as closing the request page, the log and monitoring will record it as status code 499.
520	After the node successfully establishes a connection with the origin server and sends a request, if the origin server directly sends a RST packet, the node responds to the client with a 520 status code.
521	When the node requests the origin server, during the TCP connection establishment phase, if the origin server directly sends a RST packet, the node responds to the client with a 521 status code.
522	When the node requests the origin server, during the TCP connection establishment phase, if the origin server does not respond, causing the node to time out, the node responds to the client with a 522 status code.
523	If the domain is configured with a domain name as the origin server, when the node goes to the origin, it needs to resolve the domain to obtain the origin server's IP. If the resolution fails, the node cannot go to the origin, and it responds to the client with a 523 status code.
524	After successfully establishing a connection with the origin server, if the node initiates a request to the origin server and there is no response from the origin server, causing a timeout at the node, the node responds to the client with a 524 status code.
525	If the origin protocol is HTTPS, the node needs to perform an SSL handshake with the origin server when going back to the source. If the handshake fails, the node responds to the client with a 525 status code.
566	When a request is intercepted by Web Protection - Managed Rules, the default response is a 566 status code along with the default interception page. If the user has configured a custom interception status code, the configured status code will be used.
567	When a request is intercepted by Web Protection - Custom Rules, Web Protection - Rate Limiting or Bot Management rules, the default response is a 567 status code along with the

	default interception page. If the user has configured a custom interception status code, the configured status code will be used.

Product Features FAQs

Last updated：2023-10-13 14:27:26

How can I connect my site to EdgeOne?

EdgeOne supports NS and CNAME connection.

What security capabilities does EdgeOne have?

It can prevent web application layer, DDoS, CC, bot, and crawler attacks and allows you to configure complicated custom access control rules based on your business needs.

Does EdgeOne support cross-region accerlation?

EdgeOne deploys edge nodes in to fully meet your cross-region business needs. For specific available regions, contact us.

Does EdgeOne support sites not deployed on Tencent Cloud?

Yes. For more details, please contact us.

Does EdgeOne support API operations?

Yes. EdgeOne supports TencentCloud API and Terraform API.

Does EdgeOne support dynamic acceleration?

Yes. It supports scenarios where requests for dynamic/static hybrid resources need to be accelerated. It can optimize the request response time and stability to deliver a high-quality and smooth access experience for websites.

What site business security protection capabilities does EdgeOne offer?

EdgeOne provides web and bot protection for HTTP and HTTPS-based website businesses. Specific web protection rules include those for web security, OWASP rules, custom characteristics, and frequency control.

What non-site business security protection capabilities does EdgeOne offer?

EdgeOne provides DDoS attack protection for TCP and UDP applications with specified ports, such as detection and protection against common types of DDoS attack, filtering rules by port, protocol, source IP region, and custom packet characteristic, and UDP watermark protection (coming soon).

Domain Service FAQs

Last updated：2023-11-23 20:31:55

Why do I get a CNAME and MX record conflict prompt when adding a DNS resolution record?

Take `example.com` as an example.

Record type	Host	Value
MX	www	mx.mail.com
CNAME	www	test.edgeone.com

When performing a recursive resolution query, each record type has different priority, and CNAME has the highest priority. See RFC1034 and RFC2181. Therefore, during the resolution request process, the CNAME resolution record result will be returned first. When the host record value is the same, CNAME record and MX record cannot be configured at the same time, and you will get a prompt about the conflict.

If you do need to add CNAME and MX records at the same time when the host record is @, EdgeOne allows you to configure CNAME and records at the same time:

Record type	Host	Value
MX	@	mx.mail.com
CNAME	@	test.edgeone.com

Reminder:
This configuration will lead to unstable mailbox reception. If the Local DNS of the mailbox server prioritizes the resolution of the CNAME type of the @ record, the resolution of the MX type of the @ record will be affected, resulting in a resolution failure. If the host record is not @ , but the MX and CNAME records still indicate a conflict, please refer to the description of other record type conflicts below.

Why do I get a CNAME and TXT record conflict prompt when adding a DNS resolution record?

Take `example.com` as an example.

Record type	Host	Value
TXT	www	edgeone-txt-flag

CNAME	www	test.edgeone.com

The CNAME record has the highest priority, so if the host record is the same, configuring the CNAME record and the TXT record at the same time may cause the TXT record to fail to be parsed. **In this case, EdgeOne will prompt record conflict**.

If you do need to add CNAME and MX records at the same time when the host record is @, EdgeOne allows you to configure CNAME and TXT records at the same time:

Record type	Host	Value
TXT	@	edgeone-txt-flag
CNAME	@	test.edgeone.com

Reminder:
This configuration will cause the TXT verification to fail, you can remove the CNAME record to solve this problem. TXT and CNAME records will still conflict when the host record is not @.

How do the record types conflict with one another?

See below for details:
✓: No conflict. When the HOST is the same, these two record types can both be configured. For example, after configuring the A record for `www.example.com`, you can still configure the MX record.
×: Conflict. When the HOST is the same, these two record types cannot be both configured. For example, after configuring the A record for `www.example.com`, you can not configure the CNAME record.

Record type	A	AAAA	CNAME	MX	NS	TXT	SRV	CAA
A	✓	✓	×	✓	×	✓	✓	✓
AAAA	✓	✓	×	✓	×	✓	✓	✓
CNAME	×	×	×	×	×	×	×	×
MX	✓	✓	×	✓	×	✓	✓	✓
NS	×	×	×	×	✓	×	×	×
TXT	✓	✓	×	✓	×	✓	✓	✓
SRV	✓	✓	×	✓	×	✓	✓	✓
CAA	✓	✓	×	✓	×	✓	✓	✓

Note

The table above shows the conflict relatoinship when the HOST is not @. If the HOST is @, a CNAME record does not conflict with an MX or TXT record.

When the record type is A/AAAA/CNAME, can I configure both the resolution and acceleration when the HOST is the same?

Take the following configuration as an example:

Record type	Host	Value
A	www	1.1.1.1
A	www	2.2.2.2

In this case, if you want to enable acceleration for one record, there will be a conflict. To enable acceleration for `1.1.1.1`, you need to delete `2.2.2.2` first.

Note

The above conflict happens on A/AAAA/CNAME records.

Site Acceleration FAQs

Last updated：2023-10-13 14:30:10

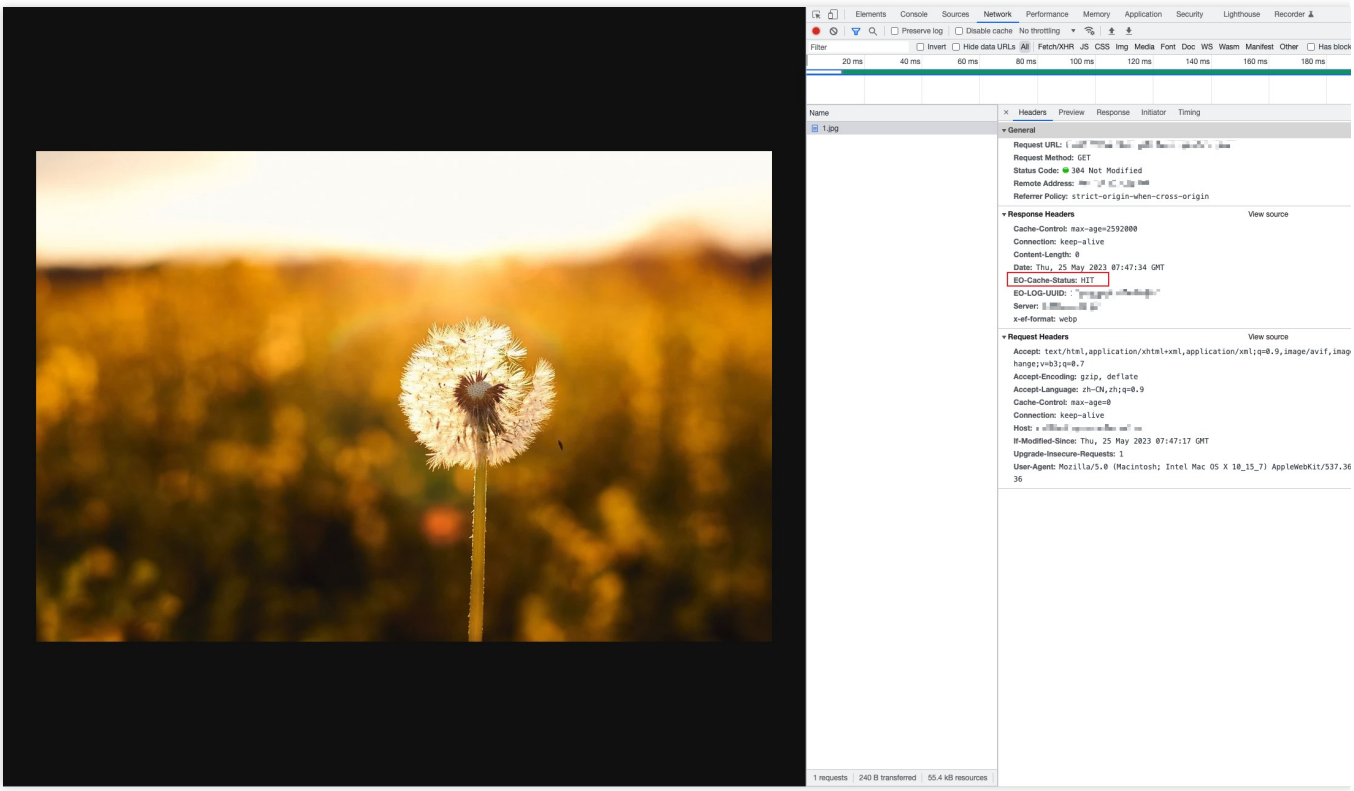
How do I tell whether user access has hit the EdgeOne cache?

EdgeOne identifies whether a request hit the cache via EO-Cache-Status.

Open in browser

Curl command

Open the console in the browser and access the request URL (such as https://example.com/test.webp). Check the response header. If the value of `EO-Cache-Status` is `HIT`, the cache is hit.



For Mac/Linux OS, you can use curl command to verify (such as `curl https://example.com/test.webp -i`). Check the response header. If the value of `EO-Cache-Status` is `HIT`, the cache is hit.

How to handle cross-origin errors whenprefetching?

Since resources are prefetched through URLs, cross-origin headers are not required. When a cross-origin request isinitiated, the request fails because these headers are not present in thecache.

To enable cross-origin support for yourresources when prefetching, you can customize the HTTP response header in EdgeOne.

How long does it take for Cache Purge and Cache Pre-Warming to take effect after each content submission?

Cache Purge：

Type	Single Submission quantity	Effective Time
URL	1-5000 URLs	5-50 minutes
Directory	1-1000 directories	5-220 minutes
Hostname	1-1000 Hostname	5-220 minutes
Cache-Tag	1-100 Cache-Tag	5-10 minutes
All Cache	-	5-220 minutes

Cache Pre-Warming:

Type	Single Submission quantity	Effective Time
URL	1-5000 URLs	5-30 minutes

Note：

1. When the cache TTL configured for a file is less than 5 minutes, it is suggested not to use the purge tool, but to wait for the timeout update.
2. The actual total time for any type of cache purge mainly depends on the quantity of submitted content, the more content, the longer the waiting time.
3. The actual total time for cache pre-warming mainly depends on the file size, the larger the file, the longer the waiting time. The pre-warming effective time for more large files (≥100MB) may be extended, exceeding 30 minutes.

Data and Log FAQs

Last updated：2024-07-30 15:25:56

Why are the traffic data in the console and the traffic data derived from logs inconsistent?

The traffic data derived from the byte count recorded in the `EdgeResponseBytes` field of the site acceleration access logs may not match the traffic data displayed on the console and the billing traffic data. The reasons are as follows:

Access logs can only record application layer data. In actual network transmission, the network traffic generated is 5-15% more than the pure application layer traffic. It consists of two parts:

Consumption by TCP/IP packet headers. In TCP/IP-based HTTP requests, each packet has a maximum of 1,500 bytes, including TCP and IP headers of 40-60 bytes, which generate traffic that cannot be counted by the application layer. The overhead of this part is approximately 3-4%.

TCP retransmission. During normal network transmission, around 3-10% of packets are lost on the Internet, and the server retransmits the lost packets. This type of traffic cannot be counted by the application layer and constitutes approximately 3-7% of the total traffic.

The monitoring data I see in Tencent Cloud Observability Platform and EdgeOne are not the same.

Data trends on Tencent Cloud Observability Platform and EdgeOne are generally consistent. However when it comes to the 1-minute granularity, the data can be slightly different. See below for details:

Tencent Cloud Observability Platform: Collect data from edge servers and aggregate the data with 1-minute granularity on the domain name level. This can guarantee the timeliness and stability. But it only provides data related to key metrics on the domain name level.

EdgeOne: Collect and analyze logs in real-time upon receiving the request, and then print out the result. It supports more metrics, such as traffic and requests by the device type and browser type. But the print-out time can be affected in case of request surges.

Assume that a user requests a 1 GB file. The download starts at 10:00:00 and ends at 10:01:40.

Tencent Cloud Observability Platform: Every edge server reports the metric data at a 1-minute interval. Data of this event is recorded at both 10:01 and 10:02.

EdgeOne: Every edge server prints a log when the download ends (10:01:40). The data is recorded at 10:01.

Therefore, data from Tencent Cloud Observability Platform and EdgeOne can differ at a 1-minute granularity due to the difference of sampling rules.

Security Protection-related Queries

Last updated：2023-12-06 10:19:23

What Security Features Does EdgeOne Have?

EdgeOne provides reverse proxy and protocol-specific security protection for Web application services and TCP/UDP application services.

Access Service Type	L3/L4 DDoS Protection	HTTP DDoS Protection (L7 CC Attack Protection)	Web Protection	Bot Management
L4 Proxy (TCP/UDP Application Service)	✓[1]	-	-	-
L7 Zone(Web Application Service)	✓[1]	✓	✓	✓[2]

Note:

Note 1
: Default platform-level protection is provided. If you have specific protection capacity requirements, please use Exclusive DDoS Protection Usage.

Note 2
: Bot Management subscription is required; see Billing Overview (New Version).

I've already configured a Web Application Firewall (WAF) on my origin server. Do I need to use EdgeOne security protection?

EdgeOne aims to provide integrated acceleration and security capabilities. Therefore, when you connect your application and services to EdgeOne, EdgeOne starts providing protection services. In addition to the protection already in place on your origin server, EdgeOne offers:
Distributed Security Protection: Provides protection resources distributed in multiple independent cleansing centers worldwide, offering efficient redundancy and disaster recovery through a distributed access architecture.
Protection Capability for Cached Resources: Can simultaneously check requests accessing cached resources. The usage of security policies intercepted by EdgeOne is not billed, reducing unnecessary content delivery costs.

Threat Recognition Closest to the Client: EdgeOne is typically accessed directly by clients, enabling collection and analysis of L4 connection session information from clients, assisting in identifying malicious access.
Compatibility with Your Origin Server Security Policies: Supports marking of origin-pull requests [3] allowing further analysis of requests at the origin server.
Note:

Note 3
: You need to subscribe to and enable Bot Management. Bot Management includes identification headers in origin-pull requests to assist in further analysis.

How to configure IP blocklists/allowlists? Can I configure network segment blocklists/allowlists?

If you need to configure an IP blocklist (i.e., block specified client IPs), you can configure the **Basic Access Control** in Custom Rules, select **Client IP Control**, configure the list of IPs to be blocked, and choose the blocking method.

If you need to configure an IP allowlist (i.e., allow specified client IPs), you can use Exception Rules, select the **Client IP** matching condition, and choose the security modules to be skipped.
Note:
The application scenarios for an IP allowlist may vary:
(1) Allow specified client IPs to pass. In this scenario, configure Exception Rules to skip specified security modules.
(2) Only allow specified client IPs to access. In this scenario, configure Basic Access Control rules in Custom Rules to block client IPs not in the specified list.

How to configure region blocking? How to block access from regions outside the Chinese mainland?

You can use **Basic Access Control** in Custom Rules, select **Regional Control**, configure the list of client regions to be blocked, and choose the blocking method. If you need to block access from regions outside the Chinese mainland, select the **Region Mismatch**, match the content to Chinese mainland region, and choose the blocking method.

How to configure Hotlink Protection? How to allow access only from this domain and specified domains?

Hotlink protection is mainly used to prevent static resources from being loaded by external website pages.

Common Hotlink Protection Techniques

The basic hotlink protection policy judges whether the request comes from page loading through the Referer header, intercepting requests for resources referenced by external sites and requests not accessed directly through page loading (example: directly accessing static resources by entering the URL in the browser). You can use **Basic Access Control** in Custom Rules to block requests with a Referer header not in the specified domain list.

Further Validation of Data Access Security

Using HTTP header fields can address common hotlinking scenarios, but malicious requests can still generate legitimate HTTP requests through technical means to obtain site resources. To further improve the security of resource access, you can dynamically generate URLs with time-sensitive random signatures. Before providing access to resources, verify the legality and validity of the signature to identify whether the request has permission to access resources. EdgeOne's Rule Engine offers Token Authentication options, assisting in generating signed URLs and providing a signature verification mechanism. You can also use EDGE-FUNCTION to implement custom dynamic access authentication.

What is "Monitor," and does the "Monitor" action involve interception?

The "Monitor" action only logs information and does not intercept requests. This is helpful for evaluating policies, as rules set to "Monitor" won't impact your business. Therefore, you can assess the impact on normal business and evaluate matching situations with malicious requests by checking the logs. This helps determine whether to enable interception. See Actions for more details.

What is "JavaScript Challenge," and what impact does the "JavaScript Challenge" action have on business?

The "JavaScript Challenge" action responds with a page that verifies whether the requesting client supports Cookie and JavaScript runtime environments. Browsers that meet the verification conditions can proceed with access, while other tools (example, cURL) will be intercepted. This method helps identify some non-browser tools.

Note:

APIs cannot handle JavaScript challenges and will be intercepted by the "JavaScript Challenge" action.