

# Tencent Cloud EdgeOne

## Glossary

### Product Documentation



## Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

## Trademark Notice



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

## Service Statement

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

# Glossary

Last updated : 2023-11-15 10:42:28

## Secure Sockets Layer

Secure Sockets Layer (SSL) is a widely used encryption-based security protocol. It was first developed by Netscape in 1995 to ensure privacy, authentication, and data integrity in internet communications. It is the predecessor to the modern TLS encryption used today. A website that implements SSL/TLS has "HTTPS" in its URL instead of "HTTP".

An Address (A) record is a DNS record used to point a hostname or domain name to an IP address.

## Edge Function

Edge Function (EF) is a serverless code execution environment running on Tencent Cloud edge nodes. It enables you to develop JavaScript functions and deploy them to edge nodes within seconds.

## Edge node certificate

To access a site or domain name over the HTTPS protocol, you need to configure the HTTPS certificate for the site or domain name in EdgeOne. During NS access, 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. In addition, EdgeOne allows you to upload a custom certificate or use a Tencent Cloud-managed certificate.

## Bot management

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 blockings for low-risk crawlers and legitimate APIs. For more information, see [Bot Management](#).

## Cache key

A cache key is the unique identifier of a resource cached on a node. Each file cached on an EdgeOne node has a cache key, which is a client request URL with parameters by default. EdgeOne allows you to adjust the query string in

the resource URL, concatenate the HTTP request header, and configure case insensitivity. You can customize resource cache keys to optimize node cache and respond requests with corresponding resources based on the business scenario. For more information, see [Custom Cache Key](#).

## CAM

For more information, see [Glossary](#).

## CNAME record

A canonical name (CNAME) record is a DNS record that resolves a domain name to another domain name (i.e., canonical name) and eventually to the target server IP address. If you use a CNAME record for access, after you add an acceleration domain name and enable proxy acceleration, EdgeOne will assign a canonical name in the form of `.acc.edgeoneddy1.com` or `.acc.tyxcdn.com` to the acceleration domain name.

## CDN

For more information, see [CDN](#).

## Transport Layer Security

The Transport Layer Security (TLS) protocol is a widely adopted security protocol designed to facilitate privacy and data security for communications over the internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS protocol versions include TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3.

## CNAME access

You can add the CNAME record of your domain name connected to EdgeOne at your DNS provider and enable proxy to access the EdgeOne security and acceleration services.

## Bandwidth

Bandwidth refers to the amount of traffic transferred per unit of time in bps (bit/s). For example, 1 Mbps bandwidth indicates one-megabit traffic transferred per second.

## Proxy mode

The proxy mode specifies whether a site connected to EdgeOne uses only the DNS resolution service or also uses the security and acceleration services. Proxy mode options are as detailed below:

Only DNS (Disable proxy): EdgeOne provides only DNS resolution.

Proxy acceleration: After proxy is enabled, access requests from end users will pass through the EdgeOne platform, and EdgeOne will provide security and site acceleration services for the current host record (subdomain name) based on your plan.

## DDoS mitigation

DDoS mitigation is to use the DDoS mitigation algorithm to accurately identify DDoS attacks at the network and transport layers, remove the malicious traffic, and allow legitimate traffic to pass. For more information, see [DDoS Mitigation](#).

## DDoS attack

Distributed Denial of Service (DDoS) attacks are malicious behaviors of flooding the target server or peripheral infrastructure with a massive amount of internet traffic so as to corrupt the target server, service, or normal network traffic. Common attack types include SYN, UDP, and ICMP flood attacks.

## DNS

As part of the Internet service, Domain Name System (DNS) is a distributed database that maps between domain names and IP addresses, making it easier for users to access the Internet. DNS uses TCP and UDP port 53. Each level of domain name is up to 63 characters, and a full domain name cannot exceed 253 characters.

## Dynamic resource (dynamic content)

Dynamic resources are frequently changing resources, including ASP, JSP, PHP, Perl, and CGI files, APIs, and database interaction requests. If a user requests such a resource multiple times, different data may be returned each time. If you want to better accelerate dynamic content, you can enable smart acceleration.

## EdgeOne rule engine

The rule engine feature of EdgeOne allows you to configure various condition rules in the console. To make a configuration or policy take effect by subdomain, directory, file extension, or file path, you can configure conditional statements in the rule engine to customize configurations at a fine granularity. For more information, see [Configuration Guide](#).

## EdgeOne node

EdgeOne nodes, aka edge nodes, are computing and storage servers that are deployed around the globe to provide the nearby access service. They are usually used to cache static business resources or optimize the origin-pull linkages for dynamic resources. Compared with origins, they offer better responsiveness and faster connection to end users.

## EdgeOne origin

EdgeOne origins are upper-level servers or cloud storage objects running applications or storing various resources. They are accessed through IP addresses or domain names and are sources of data for accelerated delivery.

EdgeOne supports the following origin types:

**Customer origin:** It is the customer's origin server storing business resources.

**Object storage origin:** It is a third-party object storage origin server, which is a bucket address that can be accessed over the private network.

**Tencent Cloud COS:** Select a Tencent Cloud COS bucket under the current account as origin.

## EdgeOne

Tencent Cloud EdgeOne (EdgeOne) is a one-stop platform product providing acceleration and security services based on Tencent's edge computing nodes, so as to safeguard diverse industries such as ecommerce, retail, finance service, content and news, and gaming and improve their user experience.

## Cloud Access Management

[Cloud Access Management](#) (CAM) is a web-based Tencent Cloud service that helps you securely manage permissions to access, manage, and use resources under your Tencent Cloud accounts.

## Range GETs

Range GETs refers to origin-pull based on range requests. `Range` is one of the HTTP request headers, which is used to get files in the specified range. You can use a range request to request only partial file content from the server. For example, if a request carries the HTTP header `range: bytes=0-999`, the first 1,000 bytes of the file will be returned to the user. If Range GETs is enabled, when the client requests a complete file, the EdgeOne node will pull a part of the file based on the set part size (1 MB by default) from the origin each time until the complete file is pulled. If

you have large static files and your origin supports range requests, we recommend you enable Range GETs to improve the delivery efficiency and response speed.

## HTTP/2

Hypertext Transfer Protocol 2.0 (HTTP/2 or HTTP/2.0) evolves from the SPDY protocol. It compresses the data in HTTP header fields and adopts methods such as multiplexing and increasing server pushes to reduce the network latency and accelerate page loading of the client.

## Origin domain

The origin domain is the `HOST` value carried in the origin-pull request headers. When an acceleration node performs origin-pull, the domain name of the accessed site is the acceleration domain name by default. If the origin server provides multiple domain name services, you can specify the domain name to be accessed by nodes during origin-pull based on your business needs. For example, if you want nodes to request `www.example.com` but not the acceleration domain name `abc.example.com` during origin-pull, you need to configure the origin domain as `www.example.com`.

## Origin-pull request

When a user sends a request through a browser, if the EdgeOne node hasn't cached the requested resource or the cached resource has expired, the EdgeOne node will request the resource from the origin and return it to the user. The request to the origin is called an origin-pull request.

## IP anycast

IP anycast is a technology where multiple servers use the same IP address (the shared unicast address of the servers). When a sender sends a packet to the shared unicast address, the packet will be routed to the server nearest to the sender over the routing protocol, so as to effectively cope with high traffic, network congestion, and DDoS attacks.

## IPv4

Internet Protocol Version 4 (IPv4) is the first widely used protocol that has laid a foundation for the current internet technology. An IPv4 address is in `A.B.C.D` format, that is, it contains 32 decimal digits divided into four sections by ".".

## IPv6

Internet Protocol Version 6 (IPv6) is the next-gen IP protocol designed by the Internet Engineering Task Force (IETF) to replace IPv4. It has enough addresses to number every grain of sand on earth, so it can solve the problem of insufficient IPv4 network addresses. An IPv6 address is in the format of

`XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX` (each `x` is a hexadecimal number), that is, it contains 128 characters divided into eight sections by ".".

## Health check

Health check refers to a mechanism where test methods such as listeners or network probes over L4/L7 protocols are used to check the status of real servers. Origin health check is to bind a custom health check task to an origin group to monitor the availability of the origins. Origin groups identified as "healthy" can be used for origin-pull, while "unhealthy" origin groups will be blocked from origin-pull.

## Acceleration domain name

An acceleration domain name is a site or domain name connected to EdgeOne for which the acceleration service is enabled. For example, after you connect the domain name `www.example.com` to EdgeOne and set the proxy mode to **Proxy acceleration**, `www.example.com` will become an acceleration domain name.

## Node cache

When you use proxy acceleration, EdgeOne will cache static resources on the origin to the edge node nearest to the client. When a user accesses a static resource, the user can directly get it from the edge node, which improves the resource response speed. When user requests or the target resources on the origin are forwarded through the edge node, you can configure various flexible policies, such as setting the cache validity period or rewriting origin-pull requests, for the node cache based on your business needs.

## Node cache TTL

The node cache TTL refers to the cache validity period of resources on the node. The default policy is **Follow origin server**, i.e., following the `Cache-Control` header of the origin. You can set the cache expiration time of resources on the node based on the update frequency of your business resources to optimize the node cache, load requested resources more quickly, and remove old resources timely. For more information, see [Node Cache TTL](#).

## Node cache prefresh



You can set a certain prefresh interval threshold to verify whether cached resources are still valid before the node cache TTL expires, with no need to verify the validity on the origin after the resource expires, so as to improve the site acceleration performance and respond to requests more quickly. The threshold is an integer ranging from 1 to 99, and the default value is `90`. For example, if the node cache TTL is 10 seconds and the threshold is 60%, when a user initiates a request at the sixth or tenth second, the node will first respond with the cached resource and asynchronously perform origin-pull to verify whether the cached resource is valid. If the resource is valid, the node will still use the cached resource and reset the node cache TTL to 10 seconds; otherwise, the node will get the latest valid resource from the origin and reset the node cache TTL to 10 seconds. For more information, see [Node Cache Prefresh](#).

## Access mode

The access mode refers to the mode where a site is connected to EdgeOne. Currently, the NS access and CNAME access modes are provided.

## Static resource (static content)

Static resources are infrequently changing resources such as images, videos, and HTML, CSS, and JS files on websites, software packages, APK files, and compressed files. If a user requests such a resource multiple times, the same content will be returned. The proxy acceleration feature of EdgeOne caches the static resources on the origin to edge nodes for nearby access by end users so as to accelerate resource access.

## Client

The client, by contrast to the server, is a program providing a local service to users. In addition to some applications only running locally, a client is installed on a general device to interact with the server. As the internet develops, common clients include web browsers used over the World Wide Web (WWW), email clients used to send/receive emails, and IM clients.

In Tencent QiDian, client refers to the PC or mobile application used by agents to answer or make calls.

## Browser cache

When a browser accesses a website, if the response message from the server contains the `Cache-Control` header, the browser will save the target file locally and set the cache validity period of the file to the value of `Cache-Control`. Before the browser initiates an HTTP request again to the server, it will check the validity period of the cached file first. If the file hasn't expired, the browser will directly load the resource from the local disk with no need to pull it from the server, which effectively improves the access efficiency.

## Browser cache TTL

The browser cache TTL refers to the cache validity period of resources in the browser. The default policy is **Follow origin server**, i.e., following the `Cache-Control` or `Last-Modified` header of the origin. You can set the cache expiration time of resources in the browser based on the update frequency of your business resources to optimize the browser cache and load requested resources more quickly. For more information, see [Browser Cache TTL](#).

## Traffic

Traffic is the total size of sent and received data packets. In EdgeOne, traffic units include B, KB, MB (M), and GB (G), among which the factor between two adjacent traffic units is 1,000.

## Offline cache

Offline cache is enabled in EdgeOne by default. 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 no cache on nodes, an error message of the origin failure will be passed through.

## Offline log

To help you analyze user access, EdgeOne packages access logs of the entire network at an hourly granularity and retains them for 30 days by default. These logs can also be downloaded. For more information, see [Offline Logs](#).

## Content Delivery Network

Content Delivery Network (CDN) is a new layer of network architecture built on the existing internet. It consists of servers distributed across regions to accelerate internet content delivery. These high-performance cache nodes store your content based on caching policies. When a user makes a content request, it will be routed to the node closest to the user, reducing access latency and improving availability.

## NS access

You can change the NS record of your NS server to the NS record provided by EdgeOne so as to transfer your site's DNS resolution permission to EdgeOne. In this way, you can access the EdgeOne security/acceleration services by enabling proxy while implementing a stable and professional DNS service.

## NS record

A name server (NS) record specifies the DNS server to resolve the requested domain name. After you register a domain name, the default DNS server will be assigned. To access EdgeOne through an NS record, you need to change the NS record at the domain name registrar to the one provided by EdgeOne.

## Cache purge

Cache purge is to clear resources cached on EdgeOne nodes. After purge, when a user accesses a resource, the EdgeOne node will get the latest resource from the origin and return it to the user. This feature is suitable for scenarios where resources on the origin are updated and non-compliant resources on nodes need to be cleared.

## Number of requests

The number of requests refers to the number of all requests sent to the server over a certain period of time. It is related to the file format. Taking a VOD file as an example, if the format is MP4, it equals to the number of playbacks; if the format is HLS, it equals to the number of requests for M3U8 and TS parts.

## QUIC protocol

Quick UDP Internet Connections (QUIC) is a general UDP-based network protocol. It not only guarantees the network security (similar to TLS/SSL) but also has a lower connection and transfer latency, so as to effectively avoid network congestion while still offering an available service when the network latency is high. It can implement different congestion control algorithms at the application layer without the support of the OS and kernel. Compared with the traditional TCP protocol, it has a higher adaptability and is more suitable for businesses where TCP protocol optimization hits the bottleneck.

## SecretKey

SecretId and SecretKey collectively refer to the TencentCloud API key, which is the security credential required for authentication when you access TencentCloud API. SecretKey is used to encrypt signature strings and verify them on the server. You can create multiple TencentCloud API keys for one APPID.

## SecretId

`SecretId` and `SecretKey` collectively refer to the TencentCloud API key, which is the security credential used for authentication when you access TencentCloud APIs. `SecretId` is used to identify the API requester. You can create multiple TencentCloud API keys for one `APPID`.

## Role

Roles of Tencent Cloud accounts include root account, collaborator, and sub-user. You can create users with the desired role in CAM.

## Note

CAM is a web-based Tencent Cloud service that helps you securely manage permissions to access, manage, and use resources under your Tencent Cloud accounts.

## Real-time log

EdgeOne's real-time log feature can collect and publish access logs in real time, enabling fast retrieval and analysis of log data. You can quickly access comprehensive, stable, and reliable one-stop log services such as log collection, log storage, and log search in the EdgeOne console. For more information, see [Real-time Logs](#).

## L4 proxy

L4 proxy provides customer-grade DDoS mitigation and L4 acceleration services for TCP/UDP applications. By leveraging widely distributed L4 proxy nodes, unique DDoS mitigation 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 L4 applications. For more information, see [L4 Proxy](#).

## SSL

For more information, see [Glossary](#).

## Plan

A plan is a collection of EdgeOne product capabilities and quotas available for a site. Different plans offer different collections of product capabilities and quotas. You must subscribe to a plan for each site connected to EdgeOne, and each plan contains quota limits. Currently, EdgeOne provides Standard and Enterprise plans.

## TEO

For more information, see [Glossary](#).

## Terraform

Terraform is an open-source automated IT infrastructure orchestration tool used to securely and efficiently preview, configure, and manage cloud infrastructure and resources.

## TLS

For more information, see [Glossary](#).

## Identical Site Identifier

When you create two or more sites with the same site name, you need to use the identical site identifiers (limited to entering digits, letters, underscores(\_), and hyphens (-), with a length of no more than 20 characters) to distinguish them. For instance, you need to separately integrate a.example.com and b.example.com under the same account for two example.com sites with distinct authority control, you will first create example.com for the integration of a.example.com, with the identical site identifier set as a. Subsequently, when you create example.com for the integration of b.example.com, the identical site identifier can be set as b. If the identical site identifier was not specified when you create example.com for the first time, the identical site identifier for the first example.com will default to default-alias when you create the second time.

## Web protection

The web protection feature protects the application layer for HTTP/HTTPS protocols to safeguard your site. It has a rule library with over 500 managed rules and an AI engine and provides many complex security actions for you to choose from based on your actual business scenarios. For more information, see [Web Protection](#).

## 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 constantly 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 (IoT). It can better save server resources and bandwidth and implement communication with higher real-timeliness.

## Origin protection

You can set firewall rules to allow access to only trusted IP addresses to protect the origin. You can update the latest origin-pull IP information obtained from L4 proxy and site acceleration services to your business origin firewall rules to

allow only traffic passing through the specified IPs to be forwarded to the origin, so as to implement origin protection. To ensure normal operations of your business, when you receive a message of IP list update, you need to go to the console to confirm and update the IP list promptly. For more information, see [Origin Protection](#).

## ICP filing for domain name

Any website providing services in the Chinese mainland must first apply for ICP filing, and the website can be launched for access only after the ICP filing number is obtained from the competent communications administration. Websites whose DNS service points to servers in the Chinese mainland must get the ICP filing; otherwise, they cannot be connected to EdgeOne.

## Prefetch

Prefetch is to proactively load a resource from the origin and cache it on an EdgeOne node. After prefetch, when a user requests the resource for the first time, the user can directly get the cached resource from the EdgeOne node. It can increase the cache hit rate and is suitable for scenarios such as operational campaigns and installation package release.

## Site

A site is a website. In EdgeOne, a site refers to a second-level domain name connected to a service, such as `example.com`. EdgeOne provides plans and services by site.

## Site speed test

You can initiate an instant page performance test task for a site or domain name for which proxy acceleration is enabled. After a site is connected to EdgeOne, a speed test will be initiated automatically to display the performance. You can also select a domain name and click **Start test** to initiate an instant speed test task. For more information, see [Site Speed Test](#).

## Site-wide settings

Site-wide settings are configurations or policies that take effect for a site connected to EdgeOne and each level of subdomains under the site.

## Site verification

If you use CNAME access for a site or domain name, and the site or domain name is connected for the first time or it has been added by another account, you need to verify its ownership. EdgeOne uses the TXT record for such verification.

## Smart acceleration

Smart acceleration refers to smart dynamic routing acceleration provided by EdgeOne. 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 acceleration minimizes problems such as high network latency, connection errors, and request failures.

## Host record

The host record is the domain name prefix.

To resolve the domain name `www.example.com`, set the host record to `www`.

To resolve the primary domain name `example.com`, set the host record to `@`.

To resolve the wildcard domain name `*.example.com`, set the host record to `*`.

## Subdomain name

A subdomain name is a lower-level domain name under the same site. For example, the third-level domain name `www.example.com` is a subdomain name of the site `example.com`.