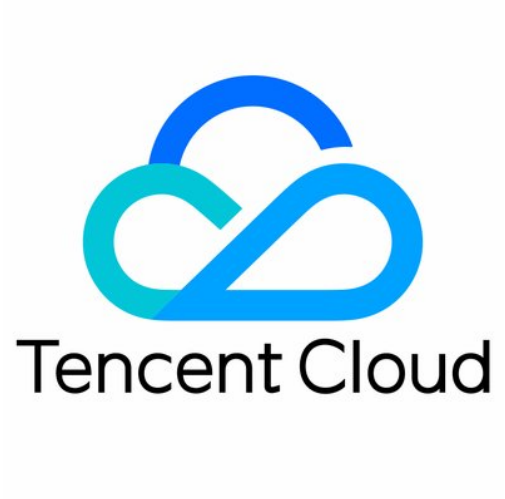
Tencent Cloud EdgeOne

Release Notes and Announcements

Product Documentation



Contents

Release Notes and Announcements

Release Notes

Last updated：2025-04-22 15:13:38

March 2025

Update	Description	References
Support security configuration read/write API	Add read/write APIs for serialization configuration of custom rules and managed rules, enabling batch reading and editing of security policies in standard format, and significantly improving the operation efficiency of cross-platform policy automatic management.	-

February 2025

Update	Description	References
Accessing the Tencent Cloud Assistant in Wechat Mini Program	EdgeOne has been integrated with the Tencent Cloud Assistant in Wechat Mini Program, allowing users to conveniently query usage and security protection data within EdgeOne. It supports the management of sites/domains, enabling users to renew their packages and purchase various add-on packs to offset usage at any time.	-
Origin Server Supports VOD Professional Edition Storage Buckets	Users can seamlessly designate the origin to VOD Professional Edition specific storage buckets without the need for business restructuring, facilitating the swift integration of original VOD services into EO.	-

January 2025

Update	Description	References
Add metric analysis dimensions	Metric analysis now supports additional metrics for L7 access response time and first byte response time, helping users to more accurately analyze and monitor business performance metrics.	Analysis

Added support for VOD Professional Version origin server	Domain name supports direct selection of VOD Professional Version origin server, and can link with video just-in-time processing capability to achieve more flexible video storage method and process video content on demand.	-

December 2024

Update	Description	References
Support Custom Statistical Metrics	Supports users to achieve personalized business monitoring through flexible configuration methods.	Custom Statistical Metrics
Support Speed Limit for Single Connection Download	Control the downlink rate of requests to help businesses save costs.	-

November 2024

Update	Description	References
API Asset Identification	API Asset Identification helps enterprises quickly discover known and unknown API resources, provides information on API usage, and assists in analyzing and formulating API security policies.	-
Site Configuration Import/Export	Supports quick export of site configurations, allowing the reuse of these configurations for other sites with similar requirements, enabling rapid configuration or migration of site configurations.	Quickly Importing and Exporting Site Configuration
Support Chinese/underscore domain name access	Support domain names with special characters such as Chinese/underscores to meet the needs of Chinese domain name customers.	-

October, 2024

Update	Description	Documentation

Optimization of metric analysis display component	The time distribution statistics component for metric analysis supports displaying multi-dimensional time curves simultaneously and enabling a more intuitive comparison of trend changes for different domain names and status codes.	Metric Analysis
DNS records' support for regional resolution capabilities	DNS records now support regional resolution capabilities, including rich dimensions such as countries, provinces, and ISPs, and enabling more flexible control of DNS record resolution.	Configuring DNS Records

September 2024

Update	Description	Documentation
New preset templates for web security protection	Preset rule templates for web protection covering high-frequency scenarios are provided, allowing quick deployment of protection rules through scenario-based selection and parameter tuning.	-
Managed security protection rules support automatic updates	Managed security protection rules will be automatically updated to the latest version when a new zero-day vulnerability is detected. Whether the update takes effect immediately will be determined by your configured automatic update policy, thereby better balancing security risks and operational investments.	Managed Rules
Launch of traffic signature	**Exclusive Anti-DDoS** supports enabling traffic signature. By embedding an encryption signature in the traffic, it can collaborate with edge Anti-DDoS to identify normal traffic from legitimate clients and filter out the rest of the traffic.	-

August 2024

Update	Description	Documentation
New mode of connection via DNSPod	When the user's connected domain name is currently managed on Tencent Cloud DNSPod, domain name connection can be quickly completed via DNSPod, enabling the user to skip domain name ownership verification. One-click CNAME addition is also supported.	Description of Connection Modes
Configurable retention days for offline logs	For Standard and Enterprise plan users, the retention period of offline logs can be configured for up to six months, helping users' business comply with the requirements of Cybersecurity Classified	Offline Logs

	Protection Compliance Service assessment and the Cybersecurity Law.	

July 2024

Update	Description	Documentation
Mutual authentication capability launched	Mutual authentication provides a higher level of security authentication for HTTPS handshakes by requiring both the client and server to provide certificates to verify each other's identity, thereby ensuring secure data transmission and strictly controlling visitor's identity.	Mutual Authentication
TypeV authentication added in Token authentication	The existing Token authentication capability has been extended to further enhance permission control in video scenarios, flexibly adapting to the needs for video URL encryption in complex business scenarios.	Authentication Method V
New console launched	The interactive interface of the console has been fully upgraded, with new divisions of features and navigation hierarchies, providing more convenient and efficient operation experience.	EdgeOne Console Upgrade Instructions

June 2024

Update	Description	Documentation
Support for bandwidth usage cap policy	You can configure the upper limit of bandwidth usage. When the bandwidth exceeds the threshold, it triggers business termination, addressing the need of some users to control business through bandwidth.	Usage Cap Policy
Refund supported for prepaid renewal orders	Refunds can be made for prepaid orders before the renewal order takes effect.	Refund Policy

May 2024

Update	Description	Documentation

Origin-pull frequency limit policy launched	Origin-pull frequency limit policy can be configured in the console to prevent the origin server from crashing due to excessive access during sudden activity spikes. This feature is currently in beta test. If you need to use it, contact us.	-
Weight configuration supported for DNS records	The A/AAAA/CNAME records can be configured with a weight, enabling resolution distribution by weight, achieving resolution load balancing.	Configuring DNS Records
Web debugging supported for edge functions	It is mainly used to debug the execution results of edge functions, making it easier for you to troubleshoot and check whether the function execution meets expectations.	Web Debugging

April 2024

Update	Description	Documentation
Integration of security alarms into Tencent Cloud Observability Platform (TCOP)	Security alarm events can be configured in TCOP, enabling you to centrally manage all alarm events, and customize the alarm event notification channels to promptly receive security alarm information.	-
Custom formats supported for real-time log push	You can customize the format for real-time log push, with JSON Lines and CSV formats currently supported.	-

March 2024

Update	Description	Documentation
HTTP response feature launched	The HTTP response feature is supported by the rule engine. By using HTTP response, you can configure response status codes and pages based on client IP addresses, custom request headers, regions, and more, achieving effects like IP allowlist/blocklist, Referer hotlink protection, UA hotlink protection, and region access control.	HTTP Response

February 2024

Update	Description	Documentation
Global policy configuration supported for security protection	The default global security policy configuration automatically covers newly added domain names, simplifying the security policy configuration process for sites with multiple domain names.	-
Custom request headers supported for real-time log push	When pushing real-time logs to HTTP service, you can customize the volume of logs carried in the request header, and modify the default request header for pushing logs.	Push Real-Time Logs
Load balancing capability launched	Primary and replica origin servers can be configured for disaster recovery by using load balancing. The health status of origin servers is actively detected, proactively shielding failed origin servers, and allocating business traffic to healthy origin servers.	Quickly Create Load Balancers

January 2024

Update	Description	Documentation
Custom bot rules and rate limiting capability enhancement	Custom bot rules and rate limiting support more matching conditions, including bot intelligent features and JA3 fingerprint, providing more refined optimization and protection measures.	Custom Bot Rule
Personal plan capability upgrade	In the Personal plan feature, web protection exception rules support skipping rate limiting and managed rules modules.	Comparison of EdgeOne Plans
Billing usage statistics launched	The account-level and plan-level billing usage can be queried on the Billing Usage page, and filters such as domain names, tags, and billing regions are supported.	Billing Usage
Origin-pull timeout	The rule engine supports customizing origin-pull timeout.	Origin-Pull Timeout

December 2023

Update	Description	Documentation
Importing DNS records in batches	Importing DNS records in batches is supported.	Batch Importing DNS Records

Token authentication tool	URL generation and testing tools are provided for Token authentication, making it easier for developers to accurately verify whether the URL's logic meets the authentication rules.	Token Authentication

November 2023

Update	Description	Time	Documentation
Prepaid plans support self-service refunds	For eligible prepaid plans, user self-service refunds are supported and the user refund process is simplified.	2023-11	Refund Policy
The personal edition supports richer security protection capabilities	Open vulnerability protection rule set, web protection > rate limiting, Web attack log, Web security analysis and other security protection-related capabilities to the personal edition plan.	2023-11	Comparison of EdgeOne Plans

October 2023

Update	Description	Time	Documentation
Security protection actions support dimension upgrade	Rate limiting and Bot related rules, supporting redirection and returning of custom pages.	2023-10	Action
Custom error page	Addition of entrance to custom error page.	2023-10	-

September 2023

Update	Description	Time	Documentation
Display optimization of the same name sites	In the site management list page, the display mode for sites with same name has been optimized. Multiple sites under the same name are consolidated under the same domain name, making it convenient for user searches. It also supports filtering by the type of access mode, service area, and effective status.	2023-09	-

Integration of SSL certificates management into domain name services	Within domain name services, HTTPS certificates can be selected directly for domains, and batch deployment of certificates is also supported.	2023-09	Configuring Own Certificate for A Domain Name
Prepaid plan supports unbinding sites	For prepaid plans, unbinding from the site by deletion is supported. Once deleted, other sites can be reselected for access within the same plan.	2023-09	-
Personal edition enables real-time logs capabilities	The personal edition plan supports real-time logs, satisfying personal edition plan users' demand for access log analysis.	2023-09	Comparison of EdgeOne Plans

August 2023

Update	Description	Time	Documentation
Edge functions provide default access domain	Support for providing a default access domain for edge functions, which can be triggered by the default access domain even without site access.	2023-08	-
Web Security Analysis supports more analysis dimensions	Web Security Analysis supports Request path, JA3 fingerprint, Request method, and Request ID as statistical dimensions.	2023-08	Web Security Analysis
L4 proxy supports port translation mapping	L4 proxy ports are no longer limited to keeping the forwarding port and origin port consistent, and can be configured as long as the port segment length is consistent.	2023-08	Create L4 proxy instances
Usage capping policy released	Support for configuring usage capping policies, which will trigger service suspension when the limit is reached, avoiding abnormal usage and high bill risks.	2023-08	-
Automatic preheating capability released	Combining Tencent Cloud COS+SCF+EdgeOne can automatically preheat resources to EdgeOne edge nodes after uploading to COS.	2023-08	-
Dynamic packaging capability released	Combining Tencent Cloud COS+SCF+EdgeOne can automatically trigger cloud functions to process APK base package with different information insertion after uploading to COS.	2023-08	-

July 2023

Update	Description	Time	Documentation
Rule engine supports variables	New ability to obtain variables, allowing users to dynamically extract and process data information within request in the rule engine.	2023-07	Variables
Self-service debugging capability released	Provide self-service debugging capability to help users quickly obtain node cache TTL, whether resources are cacheable, Cache Key, etc., for easy business configuration debugging.	2023-07	Self-service debugging
Cache Purge supports selecting deletion method	In Cache Purge, you can support using "marked expired" and "directly delete" two methods according to different cache purge types.	2023-07	Cache Purge

June 2023

Update	Description	Time	Documentation
Enterprise plan upgrade	Plan mode upgrade, supporting more flexible value-added service purchase capabilities.	2023-06	Billing Overview (New)
New standalone DDoS protection capability	For Enterprise plan users, if they have higher requirements for DDoS protection, they can choose to purchase, and provide a standalone DDoS protection platform.	2023-06	Exclusive DDoS protection related fees (Pay-as-you-go)
Web Protection custom rule supports content matching	Support request content matching method, adapting to more flexible security scenarios.	2023-06	-
Origin-pull supports any private object storage bucket	Object storage origin now supports any third-party private read object storage bucket that uses AWS Signature v4 & v2 compatible authentication protocol.	2023-06	-

compatible with S3			
Support for deploying SM2 encryption certificates	By uploading the SM2 encryption certificate to the SSL console, the certificate can be deployed to the specified domain in EdgeOne, with up to one SM2 encryption certificate supported per domain.	2023-06	-

May 2023

Update	Description	Time	Documentation
Rewrite access URL supports regex matching	Support separate configuration of request protocol, hostname, and path after redirect, with path supporting exact match and regex match.	2023-05	Access URL Redirection
IP grouping supports batch import	Support batch configuration of security protection IPs and IP segments by importing.	2023-05	-
Web Protection Managed rules support auto-renewal	When there are updates to 0-day vulnerability rules, automatically update rule configurations according to user configuration and protection level.	2023-05	-

April 2023

Update	Description	Time	Documentation
Bot management supports active detection	Through Cookie verification and Client behavior verification, detect and identify potential malicious bot access, meeting customer requirements for accurate interception of malicious traffic in complex network environments.	2023-04	-
Web Protection Exception rules support skipping CC protection	Solves the problem of misjudgment of valid high-concurrent traffic in specific scenarios, ensuring business continuity and reliability.	2023-04	-
API supports IP group	Support for configuring IP groups through API, closely linked with security policy, quickly adjusting IP groups	2023-04	Modify security IP grouping

configuration	according to security policy in real-time, reducing operation and maintenance costs.		
QUIC SDK released	QUIC SDK officially released to the public, providing developers with simple and easy-to-use API interfaces for quick integration of QUIC protocol into developer Apps.	2023-04	QUIC SDK
L4 proxy acceleration capability optimization	Support configuration of port segments, removal of port quantity limit, and support for SPP protocol.	2023-04	-

March 2023

Update	Description	Time	Documentation
Transmitting analysis results of Bot management to the origin server	Supports transmitting the analysis results of Bot management to the origin server through the request header, providing the origin server with multi-dimensional security analysis results.	2023-03	-
Post verification for site ownership	After connecting the site to EdgeOne, you can verify the site ownership through the third-level domain.	2023-03	-
Metrics for origin-pull	Metrics related to origin-pull are added, which help users analyze the origin-pull performance.	2023-03	-
SSL/TLS security level selection	You can configure the protocol version and Cipher suite that are allowed to use when a client shakes hands with an edge server TLS as needed, and also disable insecure encryption suites.	2023-03	Configuring SSL/TLS Security Level

February 2023

Update	Description	Time	Documentation
Optimized domain name service experience	Completed the reconstruction of domain name service module. Fixed the problem of configuration splitting for service connection. All types of origins can be configured and recommended configurations specific to a scenario are added.	2023-02	-
WAF protection upgrade	WAF custom protection rules supports extracting the client IP in X-Forwarded-For header for conditional matching, and frequency data can be collected based on the actual client IP.	2023-02	-
Custom rules of Bot management	The matching conditions and execution actions of the rules can be customized, and obfuscated confrontation and combined disposal are added.	2023-02	-

January 2023

Update	Description	Time	Documentation
`X-Forward-For` request header	The origin-pull request carries the `X-Forward-For` header by default to indicate the IP addresses of the client and proxies.	2023-01	-
`Vary` header	The response from the origin carries the `Vary` header to indicate the data to be cached. This header makes caching more flexible in multiple scenarios.	2023-01	-
gRPC protocols	EdgeOne supports gRPC protocols, including the Simple RPC and Server-side streaming RPC protocols.	2023-01	gRPC
Plan switchover	You can easily switch between the Enterprise plan and Standard plan in pay-as-you-go billing mode.	2023-01	-

December 2022

Update	Description	Time	Documentation
Enhancement of custom fields in real-time logs	You can add custom HTTP request headers, HTTP response headers, and cookie headers in real-time logs to be pushed.	2022-12	-
Release of the image resize feature	The origin stores only the original images. The size and format of an image can be changed as needed on EdgeOne nodes.	2022-12	Resizing and Converting Images
Enhancement of Web protection rules	More rule matching methods, such as regular matching, are supported.	2022-12	-

November 2022

Update	Description	Time	Documentation
IP information query	Query whether an IP is used by an EdgeOne node and view its geolocation and ISP information.	2022-11	-
Certificate Management 2.0	New **SSL Certificate** page. Support configuring certificates for multiple domain names at a time. Provide free certificates for sites connected via CNAME.	2022-11	-
Optimized navigation	The navigation structure is optimized so that the statistics and settings of each site are displayed on the details page of the site.	2022-11	-
Webhooks for security alarm pushing	Push Web monitoring alerts to Webhook addresses. The event push formats of WeCom, Lark, and DingTalk are supported.	2022-11	-
Security log filters	The policy optimization process is streamlined. You can quickly configure hit rules to filter logs, and can create protection exception rules with a few clicks.	2022-11	-

October 2022

Update	Description	Time	Documentation
Traffic scheduling management	Set up custom traffic scheduling policies to control traffic between the origin and service providers to implement smooth canary migration of traffic and flexible allocation of services	2022-10	Traffic Scheduling Management
Release of Rule Engine 2.0	Support more types of nested conditional expressions and improve cache and origin-pull configuration capabilities. In addition, rich rule management features, such as quick rule copy and automatic generation of dynamic rule navigation, are provided.	2022-10	Rule Engine
Support for Terraform	EdgeOne supports the Terraform resource orchestration tool to make infrastructures codified and versioned, simplify configuration change and management, and effectively improve the Ops efficiency.	2022-10	Terraform
Support for security policy templates	Multiple sites and domain names can be quickly reused, and security policy configurations are adjusted accordingly, greatly simplifying the configuration process.	2022-10	For more information, contact Us
Support for cache purge based on `Cache-Tag`	Caches can be purged based on the tag value of the `Cache-Tag` response header in the HTTP response packet. This feature is only applicable to the Enterprise plan.	2022-10	Cache Purge

September 2022

Update	Description	Time	Documentation
Alias domain name	For business scenarios with many domain names and the same configuration, such as SaaS site construction, only one target domain name needs to be connected, and all other bound domain aliases can enjoy the EdgeOne acceleration and security services.	2022-09	For more information, contact Us
Release of Edge Functions	Edge Functions is a serverless code execution environment provided by Tencent Cloud for enterprises and developers.	2022-09	For more information,

	Custom requirements can be met simply by writing business function code and setting trigger rules for deployment to edge nodes.		contact Us
File-based site ownership verification	A file verification method is provided, which allows for adding specified files on the origin server of the domain name to verify their ownership. Currently, EdgeOne supports DNS txt verification and file verification.	2022-09	Verifying Site Ownership

August 2022

Update	Description	Time	Documentation
Security whitelist policies	Managed web protection rules and bot management exception rules are supported, so you can configure business allowlists to avoid false positives.	2022-08	Web Protection
Support for Chinese Mainland regions	EdgeOne is available in Chinese mainland regions.	2022-08	Overview

July 2022

Update	Description	Time	Documentation
Release of the Standard and Enterprise plans	The Standard and Enterprise plans are launched for you to purchase based on your business needs.	2022-07	Billing Overview
Support for IPv6 access and protection	IPv6 is supported comprehensively for IPv6 access and layer-4/7 security protection.	2022-07	CNAME Access
Release of RUM	Real User Monitoring (RUM) is a one-stop frontend monitoring solution that supports page performance	2022-07	Real User Monitoring

	analysis, access analysis, and resource speed test for real users.		
More match conditions supported by the rule engine	Match conditions **URL Full** and **Filename** are added to the rule engine to support more custom configuration scenarios.	2022-07	Rule Engine

June 2022

Update	Description	Time	Documentation
Support for tag management	Tags are supported for you to use different standards to easily manage cloud resources with the same attributes by category.	2022-06	Tags
Origin health check	You can customize the origin health check mechanism to monitor the origin health status.	2022-06	Origin Health Check
Support for smart bot analysis and client filtering for security protection	IP profiling-based bot management rules (client reputation) are added. Requests can be matched with categories that are configured with different processing methods. Smart client filtering is supported to accurately block high-risk clients	2022-06	Bot Management
Integration of data statistics with Tencent Cloud Observability Platform	Data statistics are connected to Cloud Monitor, so you can configure custom monitoring alarms.	2022-06	Creating Alarm Policy

May 2022

Update	Description	Time	Documentation

Enhancement of site acceleration and rule engine capabilities	The async cache purge feature and capabilities such as Transport Layer Security (TLS) versioning, Online Certificate Status Protocol (OCSP) stapling, maximum upload size, Brotli compression, and custom cache key are supported to flexibly meet diversified business needs.	2022-05	Rule Engine
Security enhancement	JavaScript challenge, dynamic verification code, AI engine-based SQL injection and XSS attack identification, and dynamic DDoS protection policies based on business baseline analysis are added to make protection more fine-grained and accurate and make deployment easier.	2022-05	DDoS Mitigation
Data analysis enhancement	Traffic analysis: Bandwidth data can be queried and filtered by country/region to meet the requirements in more query scenarios. Cache analysis: Cache analysis is supported to analyze data such as cache traffic, origin-pull traffic, and top URLs in real time.	2022-05	Traffic Analysis
L4 proxy support for log download and real-time log push	The L4 proxy provides log download capabilities and supports real-time log push.	2022-05	Real-time Logs

April 2022

Update	Description	Time	Documentation
Support for more acceleration and origin-pull capabilities	Capabilities such as video dragging, Range GETs, custom origin domain, Cloud Object Storage (COS) origin, and token authentication are supported.	2022-04	Origin Group List Rule Engine
L4 proxy support for Anycast IP addresses	The L4 proxy can be connected through an anycast IP address, making the connection easier and more secure.	2022-04	L4 Proxy
DDoS	You can enable protection enhancement to use dedicated	2022-	DDoS

protection with dedicated resources	resources to improve protection capabilities. You can also subscribe to DDoS attack alarms.	04	Mitigation
Support for more web protection methods	Various web protection methods are added, including IP blocking, redirection, returning to the specified page, and returning the specified error code.	2022-04	Web Protection
Basic bot protection capabilities	Bot management rules and custom rules are provided to implement basic bot management features.	2022-04	Bot Management

March 2022

Update	Description	Time	Documentation
Release of EdgeOne	Tencent Cloud EdgeOne provides acceleration and security solutions in regions outside the Chinese mainland based on Tencent edge computing nodes to safeguard diverse industries such as e-commerce, retail, finance service, content and news, and gaming and improve their user experience.	2022-03	Overview

Security Announcement
Protection against DDoS attacks targeting HTTP/2 protocol vulnerabilities

Last updated：2023-10-13 12:40:16

Overview

Starting from September 2023, EdgeOne has noticed a new type of HTTP DDoS attack that exploits a new vulnerability in the HTTP/2 protocol. This vulnerability (CVE-2023-44487) poses a security threat to Web services and applications that use the HTTP/2 protocol to provide shared services. EdgeOne's reverse proxy architecture and security policy can effectively isolate and mitigate the risks posed by such DDoS attacks.

The DDoS attack exploiting this vulnerability is also known as the "HTTP/2 Rapid Reset Attack" and targets flawed HTTP/2 applications through the HTTP/2 protocol mechanism. EdgeOne's reverse proxy architecture and implementation of HTTP/2 have provided corresponding isolation and mitigation mechanisms for this feature of the HTTP/2 protocol.

Based on known information and vulnerability behavior, the attack form exploiting this vulnerability is a DDoS attack, affecting the availability of HTTP/2 application services; a single attack exploiting this vulnerability will not cause business data leakage. There is currently no evidence to suggest that any customer information has been leaked due to this vulnerability.

Attack Details

Attackers can exploit this HTTP/2 protocol vulnerability to launch DDoS attacks on HTTP/2 application services. By first sending a large number of HEADERS frames and then a large number of RST_STREAM frames, attackers can generate a large amount of traffic to HTTP/2 application services in a short period of time. By exploiting the connection mechanism of HTTP/2 (for details, please refer to RFC9113: HTTP/2 Stream Lifecycle and State Transition Mechanism), attackers can send a large number of HEADERS and RST_STREAM frames within the same TCP connection, causing high CPU load and exhausting service resources for flawed HTTP/2 application services.

Protection against CVE-2023-44487

This attack is a DDoS attack targeting the application layer protocol (L7 protocol). EdgeOne has optimized and strengthened its proxy architecture and security policy for application layer protocols, protecting Web application services using EdgeOne. EdgeOne's reverse proxy architecture and HTTP/2 implementation can effectively isolate the business availability risks caused by attacks exploiting this vulnerability. At the same time, EdgeOne will continue to monitor new security threats and evaluate security policies, continuously optimizing protection efficiency.

We recommend that you:
Check your origin and HTTP/2 service architecture, update security vulnerability patches in a timely manner, and mitigate the risk of DDoS attacks exploiting this vulnerability.
Configure security protection policies, enable and configure Rate Limiting rule. EdgeOne's rate limiting can provide effective protection against application layer security threats, including HTTP DDoS attacks.
If you cannot update security vulnerability patches for your origin, we recommend enabling Origin protection and allowing only origin-pull requests from EdgeOne to avoid attackers launching attacks by directly accessing the origin server.

Using EdgeOne's HTTP Security Protection

To protect your Web services, EdgeOne offers a variety of HTTP security features (Refer to Web Protection) depending on your subscribed service specs. You can refer to the following methods to reduce the risk of application layer DDoS attacks.

Mitigate high-frequency DDoS attacks that cause a decline in origin availability. You can enable CC attack defense rules to dynamically identify and mitigate high-risk HTTP DDoS attacks.
Block IPs or CIDR subnets with a history of malicious access. You can configure Custom rule to block specified IP list or subnet list.
Limit the allowed access service area. You can configure Custom rule to block access from outside the specified business area.
Control resource consumption. You can configure rate limiting rules to mitigate the resource consumption caused by high-frequency access. We suggest limiting the request rate for global or non-specified business areas to control resource consumption.
Note:
Enterprise users can contact us to evaluate customized protection strategies, including advanced rate limiting rules based on headers and JA3 fingerprint[1], to specifically mitigate application layer DDoS attacks and service abuse risks.
Note 1: The rate limiting option based on JA3 fingerprint requires subscribing to Bot management service.
Block high-risk bot access behavior. You can enable and configure Bot Intelligent analysis, which dynamically identifies bot behavior and tags requests, helping you identify and block malicious bot access.

Block access from high-risk clients. You can enable and configure Client reputation, which helps you identify and block high-risk clients through continuously updated IP threat intelligence.

Announcements

Origin Protection Upgrade Guide

Last updated：2025-06-26 11:52:54

To decrease the number of IP ranges and reduce the change frequency of origin server IPs, EdgeOne will upgrade the protection capability of origin servers starting June 26, 2025. At the same time, the form of origin server IP changes and the notification frequency will also be adjusted accordingly. See the following table for details.

Comparison Dimension	Legacy Origin Protection	New Origin Protection
Number of IP ranges	more than 300	less than 200
change frequency	Once a week under normal circumstances	On average, once every 3-6 months
change format	Click Confirm in the console to take effect after updating. The newly-added origin IPs in the new version will not take effect until confirmed, while the reduced origin IPs will be deleted directly. Long-term failure to update can cause a continuous decrease in available IP ranges, impacting origin quality.	Send a notification 14 days in advance. After the window period, the new version of origin IPs will take effect regardless of confirmation on the console. Maintain full availability of origin IP ranges.
Notification format	Send change notifications on the 1st of each month.	Send change notifications when actual changes occur.
Support Package	Standard Edition Enterprise Edition	Personal Edition, Basic Edition, Standard Edition, Enterprise Edition
API	Provide only query API	Open APIs for enablement, querying, modification, disable, and upgrade, supporting integration with automated Ops.

Note:

1. Note: Starting from June 26, 2025, sites under accounts with new origin protection enablement will adopt the new origin protection directly.
2. Accounts with origin protection enabled on the earlier version will gradually open the portal to upgrade to the latest version from June 30, 2025 to July 30, 2025. We will not automatically upgrade your account's origin protection from

the old version to the new version before you proactively confirm the update. Only after you confirm the update will the IP range version, update method, and notification method of origin protection switch over from the old version to the new version.

If you have any questions, please contact us for support at any time. Thank you for your continuous support of EdgeOne.

[Tencent Cloud EdgeOne] Announcement On Image Processing Billing Adjustment

Last updated：2025-06-12 16:16:57

Thank you for your continuous support and trust in Tencent Cloud EdgeOne's Image Processing servers. Since its launch, EdgeOne has been committed to providing efficient and high-quality image processing servers, including format conversion、resize and more servers. By processing, caching, and responding to images directly at EdgeOne's edge servers, we help numerous customers enhance user experience while reducing image management costs and maintaining image quality.

To further provide more stable, higher-quality, better-experienced, and more powerful Image Processing services, **EdgeOne Image Processing will officially transition to commercial billing starting July 1, 2025.**

All Image Processing operations（Including image processing functions initiated by edge functions）will be billed under the **Media Processing** usage item. Different processing capabilities will have distinct **deduction ratios** applied to corresponding processing counts. Please monitor your current usage and plan/service adjustments in advance. Ensure your account balance is sufficient to avoid service interruptions due to overdue payments. If you no longer require the service, we recommend destroying relevant resources beforehand.

Before July 1, 2025, you may continue using EdgeOne Image Instant Processing free of charge without any action required. Starting July 1, 2025, usage will be billed on a pay-as-you-go basis. For details, please refer to the **Media Processing Billing Documentation.**

If you have any questions, please feel free to **contact us f**or support. Thank you for your ongoing support for the EdgeOne product!

Service Dashboard Upgrade

Last updated：2025-06-03 16:57:53

Since the launch of the EdgeOne product, the Service Dashboard page primarily displays current site overview data and other quick access points for users. However, its daily usage rate has fallen far short of our expectations. As the platform's content gradually becomes richer, the original Service Dashboard page is no longer sufficient to display all asset data. Therefore, to further reduce redundant information interference, optimize redundant click paths, and provide users with a smoother and simpler experience in using the EdgeOne console, we plan to gradually release the revamped Service Dashboard page starting on **2025.06.03**. You can refer to this document for an introduction to our new Service Dashboard page.

New Scene-Specific Access Methods

EdgeOne has supported various business capabilities such as **Website Security Acceleration** and **Pages**. To help users more accurately find the suitable access model for their business during onboarding, the scene-specific lobby will provide access guidance upon first connection to EdgeOne. You can choose the access method that best matches your actual business scenario. Currently, there are two entry options available:
Website Security Acceleration: By adding sites on EdgeOne, once connected, EdgeOne can provide a variety of rich capabilities including intelligent acceleration for dynamic and static content, security protection, L4 proxy, edge functions, and DNS record management.
Pages: Quickly deploy websites at EdgeOne's global available zone edge nodes through connecting Git repository code, template creation, and code upload, achieving “serverless” operations and simplifying website deployment and maintenance costs.
In the future, EdgeOne will continue to expand more scene capabilities based on this foundation, helping clients deploy their business in EdgeOne’s global available zone nodes, allowing EdgeOne's edge nodes to provide fast, secure, and stable business responses.

Brand New Service Overview Interface

The new Service Dashboard interface supports switching to view all currently added website acceleration resources and Pages projects.

View Website Security Acceleration Resources

Switching to the **Website Security Acceleration** tab, users can view the overview metrics and corresponding trend graphs of all current site data, as well as view all sites added to EO on this interface. We have also optimized the performance for viewing the site list, allowing you to quickly open the page even with a large number of sites, making it easier to overview the current resource status on one page.

Site Data Overview

From the data overview, you can view the total traffic, total bandwidth peak, total request count, protection hit count metrics, and their corresponding trend graphs for all sites over the past 24 hours or the last 7 days. If you notice any anomalies in the indicators or trend graphs, you can directly click the corresponding indicator to jump to the metrics analysis interface for more detailed data analysis. If you do not wish to view the data overview each time, you can click "**Collapse Data Overview**" in the upper right corner to hide the overview data.

Quick Site Configuration Entry

In the site list, the new interface provides you with three commonly used quick entry points, allowing you to quickly jump to the corresponding secondary menu for site configuration, further simplifying user operation paths directly to the configuration entry.

New Domain Addition Interface

In the website security acceleration domain addition process, the original pop-up format will be changed to a landing page format. This can further enrich the capabilities and guidance content that can be added in the domain addition process. For example, the new domain addition process will also support configuring the origin-pull HOST header at the same time.
In the domain addition process, we have also made different interaction attempts. In the new domain addition process, all configuration options have been changed from being laid out flat to drop-down menus, reducing information interference. You can modify the corresponding configuration items based on your actual configuration needs to see supported option capabilities. Meanwhile, the original recommended configurations for domains have been integrated into the domain addition steps, allowing you to complete domain configuration and select the recommended configuration template suitable for your current business in one step.

View Pages Projects

All functions supported by the original primary menu “Pages” have been migrated to the current Service Dashboard menu, allowing you to directly switch to the Pages list in the Service Dashboard to create new projects or manage all currently created Pages projects.

The purpose of this revamped version is to further optimize the user experience in connecting to EdgeOne and managing sites. For any questions regarding the interaction in the new version, feel free to contact us for feedback!

[Tencent Cloud EdgeOne] Announcement On Edge Function Billing Adjustment

Last updated：2025-03-07 18:11:36

Thank you for your continuous support and trust in Tencent Cloud EdgeOne edge functions. Since its launch, EdgeOne has been committed to providing efficient and convenient edge computing services, helping businesses run code elastically and securely on edge nodes close to users around the world, achieving ultra-low latency and high-performance business needs.

To further provide more stable, higher-quality, better-experienced, and more powerful edge function services, **EdgeOne edge functions will be officially upgraded from the beta version to a fully available commercial version on April 10, 2025**. This upgrade will bring the following core optimizations:

Feature Expansion: Added logging and data analysis for business insights, monitoring, and fault location.

Performance improvement: Millisecond-level cold start speed, supporting intelligent Auto Scaling, meeting high-performance scenarios under sudden traffic spikes.

Stability guarantee: Built on a high availability architecture with more than 3,200 global edge nodes, SLA availability is no less than 99.9%.

After the upgrade, the platform will configure corresponding edge function quotas based on your EdgeOne plan type. Please pay attention to the quota and actual usage of your current plan, and plan and adjust your services in advance. If you need to continue using it, please ensure that your account balance is sufficient to avoid service interruption due to arrears; if you no longer use it, it is recommended to terminate the related resources in advance.

Before April 10, 2025, you can still try EdgeOne edge functions for free without any operation; **starting from April 10, 2025, the plan's quota will be deducted first, and the excess will be billed based on usage.** For more details, please refer to Edge Function Billing Documentation.

If you have any questions, please feel free to contact us for support. Thank you for your continuous support for the EdgeOne product!

Notice regarding the addition of TrustAsia free certificate issuance source

Last updated：2024-12-18 17:29:56

Dear Tencent Cloud User:
Since the launch of the Tencent Cloud EdgeOne product, we have been providing free certificate application and automatic renewal services for all connected site domains. This service is designed to help your site quickly achieve HTTPS access while reducing your certificate maintenance burden.Currently, these free certificates are issued by Let's Encrypt. In our ongoing efforts to enhance the efficiency and reliability of our free certificate issuance, we are planning to incorporate additional free certificates from TrustAsia, starting from December 30, 2024. The issuing authority and certificate trust chain of these certificates will be identical to those of Tencent Cloud's SSL free certificates.

After the update, your existing free certificates will remain valid and unaffected. Any new applications or automatic renewals for free certificates after December 30, 2024, will be randomly issued by either TrustAsia or Let's Encrypt. We anticipate that this change in the issuing source will not impact your regular business operations.

Should you notice any potential effects on your business due to this transition in the free certificate issuing authority, please do not hesitate to reach out to us for assistance. We appreciate your ongoing support for the EdgeOne product!

[Tencent Cloud EdgeOne] Impact of Root Certificate Changes from Let's Encrypt

Last updated：2024-10-16 15:06:30

The free certificates currently provided in the EdgeOne console are RSA certificates issued by Let's Encrypt. Starting from September 30, 2024, the cross-signed chain of the RSA certificates previously used by Let's Encrypt will expire, and its self-signed root certificate, ISRG Root X1, will become the only trusted root certificate for RSA certificates.

The changes to the root certificate will mainly affect systems that currently lack the chain of trust for ISRG Root X1, potentially leading to certificate-related alarms or HTTPS service unavailability. The following systems are compatible with the root certificate only in a specific version and later.
Windows >= XP SP3, Server 2008 (except systems with automatic root certificate updates disabled)
macOS >= 10.12.1 Sierra
iOS >= 10
Android >= 7.1.1
Firefox >= 50.0
Ubuntu >= 12.04 Precise Pangolin (package updates required)
Debian >= 8 / Jessie (package updates required)
RHEL >= 6.10, 7.4 (package updates required), 8+
Java >= 7u151, 8u141, 9+
NSS >= 3.26
Chrome >= 105 (OS certificate store used directly for earlier versions)
PlayStation >= PS4 v8.0.0
For more information, refer to Let's Encrypt Certificate Compatibility Documentation.

Regarding potential platform compatibility issues with the Let's Encrypt certificate, we strongly recommend you check the compatibility of the current access terminals with the certificate. If this change impacts your business, we suggest mitigating it through the following methods:
1. If you need to use a free certificate from another brand, you can apply for a free Tencent Cloud SSL certificate, and then deploy it to your current domain name by referring to Deploying/Updating SSL Certificate for a Domain Name.
2. To ensure your business remains stable and unaffected, we recommend you upgrade your current certificate to a paid Tencent Cloud SSL certificate. Then, refer to Deploying/Updating SSL Certificate for a Domain Name to complete the certificate replacement. Paid certificates are issued by more authoritative CAs that provide higher compatibility and have a validity period of 1 year. This can more effectively provide stable HTTPS service for your website.

We appreciate your support and trust in EdgeOne products. If you have any questions, please feel free to contact us.

[Tencent Cloud EdgeOne] NS Access Mode Upgrade Announcement

Last updated：2024-09-24 18:02:05

The current NS access mode provided by EdgeOne provides DNS record resolution for domain names and can switch resolution records to acceleration domain names immediately. In this mode, because switching to an acceleration domain name takes effect immediately after domain name deployment, users cannot complete all domain name-related configurations in advance, such as security protection rule or rule engine configurations, and cannot verify the access effect beforehand. This lack of grayscale access means is challenging for users seeking business stability and smoothness.

Therefore, EdgeOne plans to optimize the process and behavior of switching DNS records to acceleration domain names in NS access mode. This optimization will occur in two phases, with the first phase completed on September 11, 2024. Below is a comparison of the experience changes before and after the first phase of the upgrade:

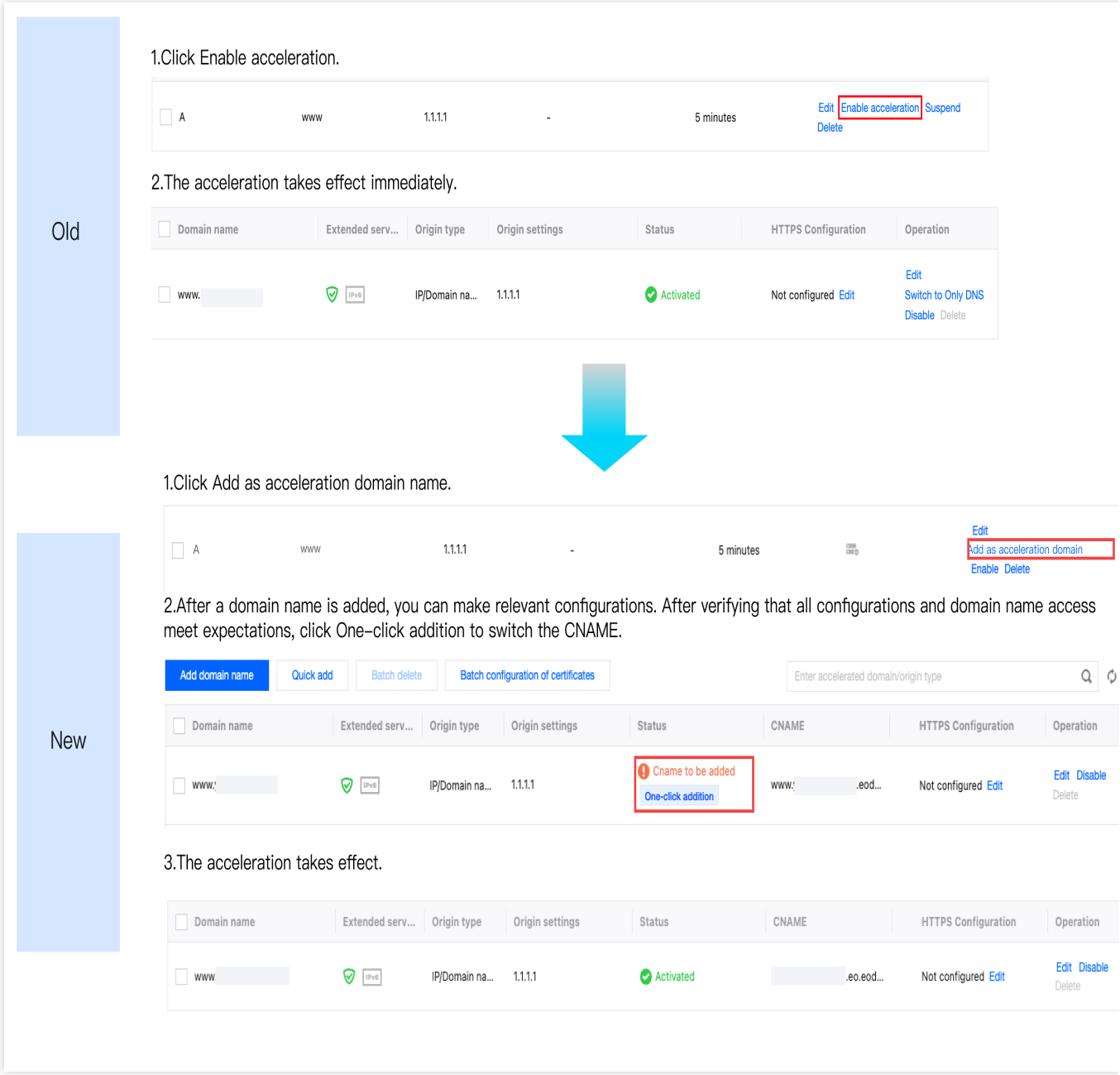
Before Upgrade

1. On the **DNS Records** page, if the host record value corresponding to an acceleration domain name has been added and you need to add it as the acceleration domain name, click **Enable acceleration** on this page. The enabled acceleration will take effect immediately after the domain name deployment is completed, but it cannot be configured or verified. In addition, no other related DNS records with the same name as the current host record can be added. That is, only the DNS record or the acceleration domain name can exist.
2. Before the upgrade, DNS records in the **Paused** state cannot be **edited**, which can be modified only after being **enabled**.

After Upgrade

1. After the upgrade, **Add as acceleration domain** is displayed on the **DNS Records** page instead of Enable acceleration. When you click **Add as acceleration domain**, a window for adding a domain name appears. After a domain name is added, the domain name will not automatically enable acceleration immediately. The backend will automatically add a CNAME record pointing to EdgeOne on the **DNS Records** page. You can enable acceleration for this accelerated domain name immediately in the third step of adding the domain name, or quickly enable this CNAME in the domain name management area by clicking **One-click addition**.
2. After the upgrade, DNS records in the **Paused** state can be **edited**.

3. After the upgrade, even if there is an acceleration domain name with the same host record name, you can continue to add other DNS resolution records as long as there is no DNS record conflict, supporting the DNS weight feature.



Note:

Currently, CNAME records automatically added by EdgeOne cannot be deleted from the DNS Records page. To delete a CNAME record, you can remove the acceleration domain name, so that the record will be automatically deleted.

Before this upgrade is completed, if you call the CreateAccelerationDomain API to create a domain name in NS access mode, the acceleration will automatically be enabled after creation. After the upgrade is completed, the

acceleration will not be automatically enabled. You will need to call the ModifyDnsRecordsStatus API to enable the corresponding CNAME record for the acceleration to take effect.

Next-Phase Upgrade Plan

After this upgrade is completed, the NS mode will undergo the next phase of optimization in the near future. The second phase will mainly address the following two issues:
1. To accommodate users who value operational convenience, a switch control will be provided during the addition of a resolution to allow the record to be enabled for acceleration immediately upon addition. This enables users' domain names to be quickly and conveniently integrated with EdgeOne.
2. The backend will no longer automatically add a CNAME record pointing to EdgeOne. DNS records will be entirely controlled by users.

The upgrade of the NS access mode will completely resolve the issues of insufficient domain name configuration and verification during the acceleration process, as well as problems related to using DNS record weights or configuring multiple resolutions after domain name acceleration. If you encounter any usage issues in the new mode, please feel free to contact us for further support.

[Tencent Cloud EdgeOne] VAU Unit Change Notification

Last updated：2024-08-13 14:42:36

In order to adapt to the globalization trend, EdgeOne will change the product unit from **10,000 times to 1 million times** starting from August 1, 2024, to help global users more easily understand the billing logic of EdgeOne about VAU and more intuitively estimate the fee consumption. The billable items affected by this change mainly include:

Billing Category	Billable Item	Before Change	After Change	Fee Impact
Value-Added Service Usage Unit (VAU)	QUIC requests	0.5 VAU/10,000 requests	100 VAU/million requests	The conversion rate is doubled. **To ensure that the fees of all users remain unchanged, the VAU price for QUIC requests will have a 50% discount for a long term.**
	Smart acceleration requests	1 VAU/10,000 requests	100 VAU/million requests	No impact
	Bot requests	1 VAU/10,000 requests	100 VAU/million requests	No impact
	Real-time log entries pushed	1 VAU/million entries	Provided for free, with no charges	Provided for free
	Precise access control rule quotas in Web Protection - Custom Rules	50 VAUs/unit/month	100 VAUs/unit/month	This billable item is supported only for Enterprise plan users. Adjustments have been made for all enterprise customers involved. If there are any enterprise customers with no adjustments made, please feel free to contact us.

Note:

This change takes effect simultaneously on the Tencent Cloud Chinese Site and International Site.

If you have any questions about the above change, please feel free to contact us for confirmation and consultation.

Thank you for your support and understanding.

EdgeOne Console Upgrade Instructions

Last updated：2024-11-20 17:30:19

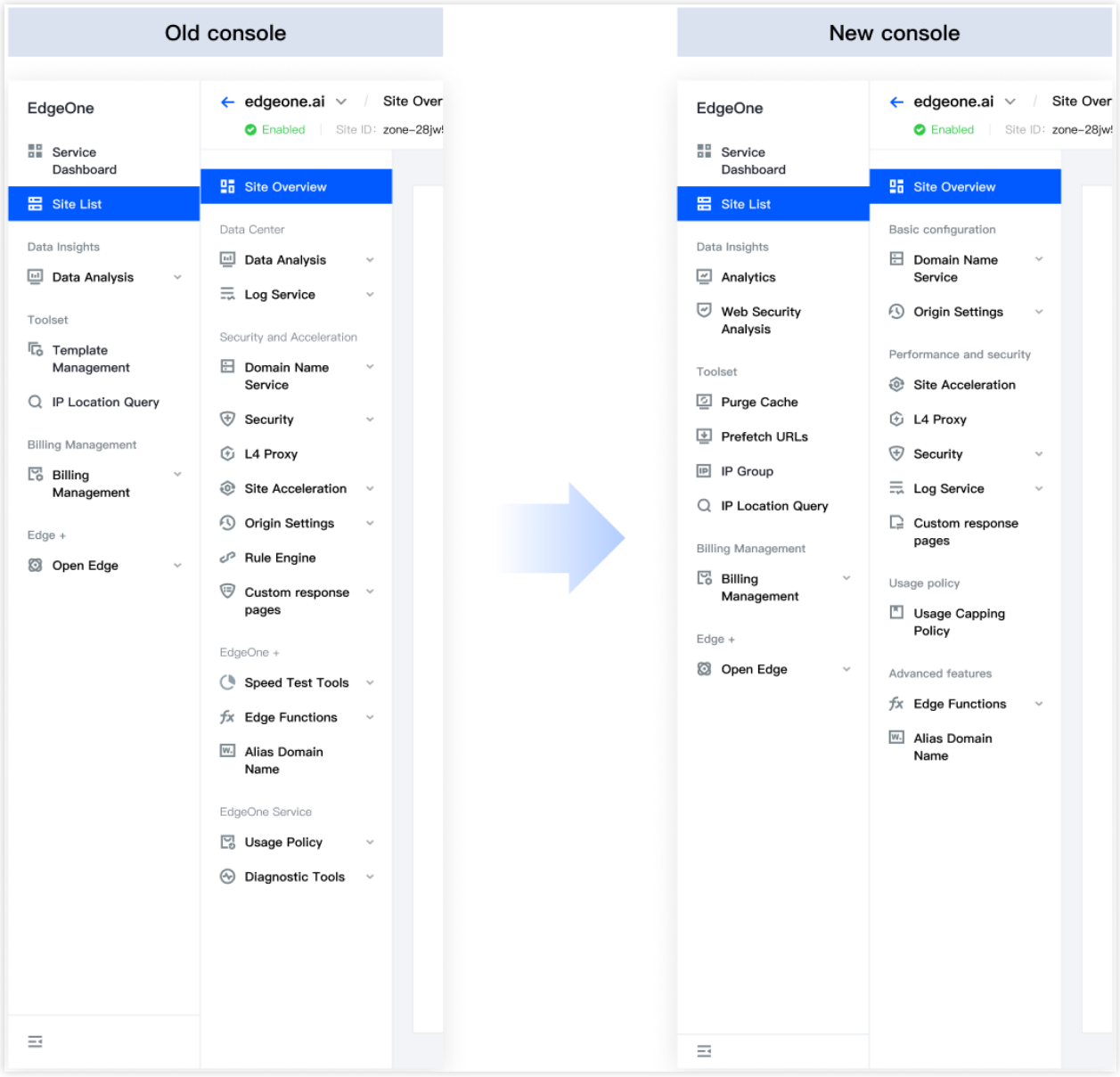
Based on historical user behavior analysis and multi-channel feedback, as of July 15, 2024, the EdgeOne console has been fully upgraded with a new interactive interface, featuring a complete reorganization of features and navigation hierarchy, aiming to provide you with a more convenient and efficient operation experience. This document will introduce the details of this upgrade.

Note:

This upgrade does not affect your business configuration and data in any way, so please feel free to explore.

Starting from November 21, 2024, the EdgeOne Old Console will be officially decommissioned.

Overview of Navigation Changes



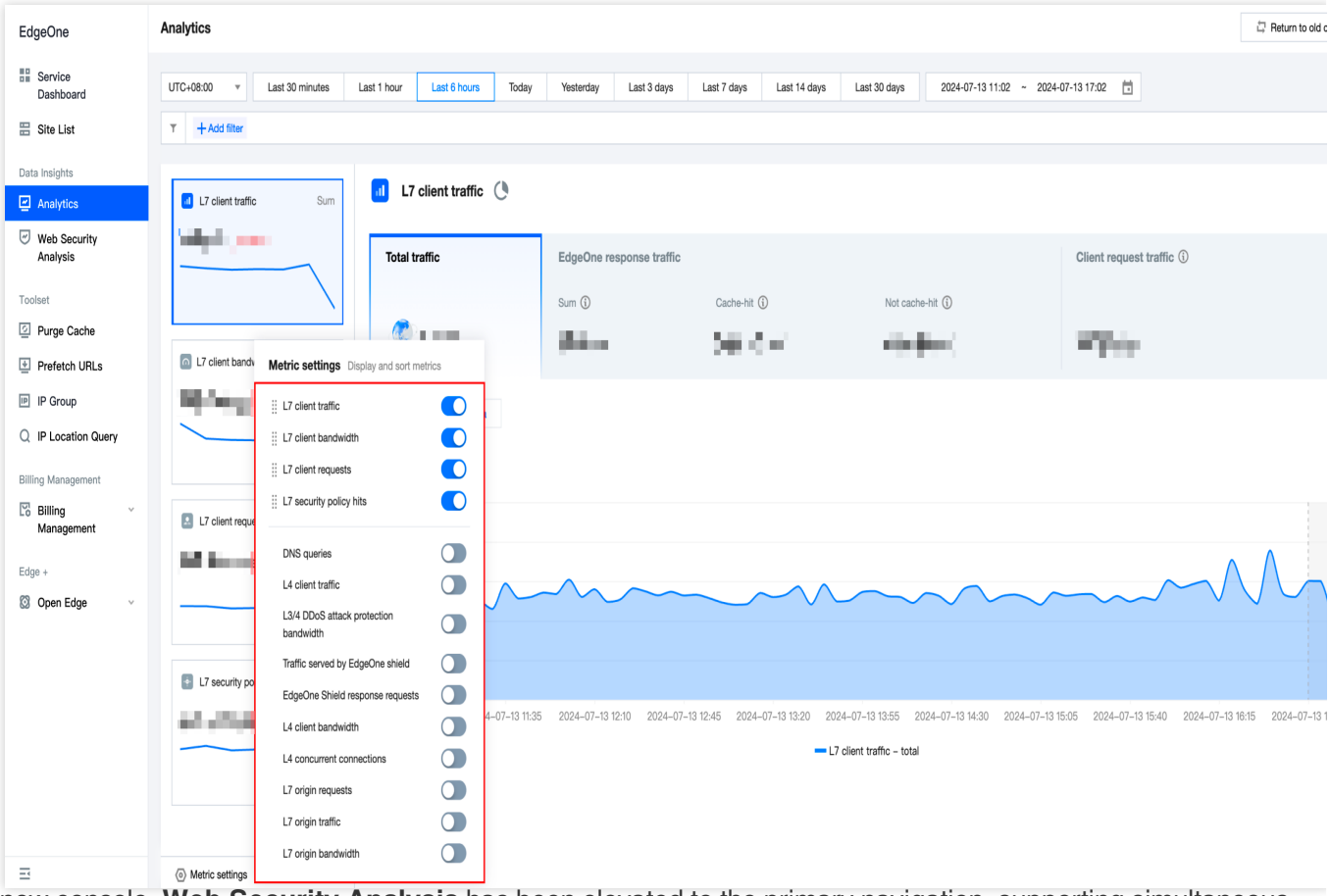
Description

Following modules have been changed in this console upgrade:

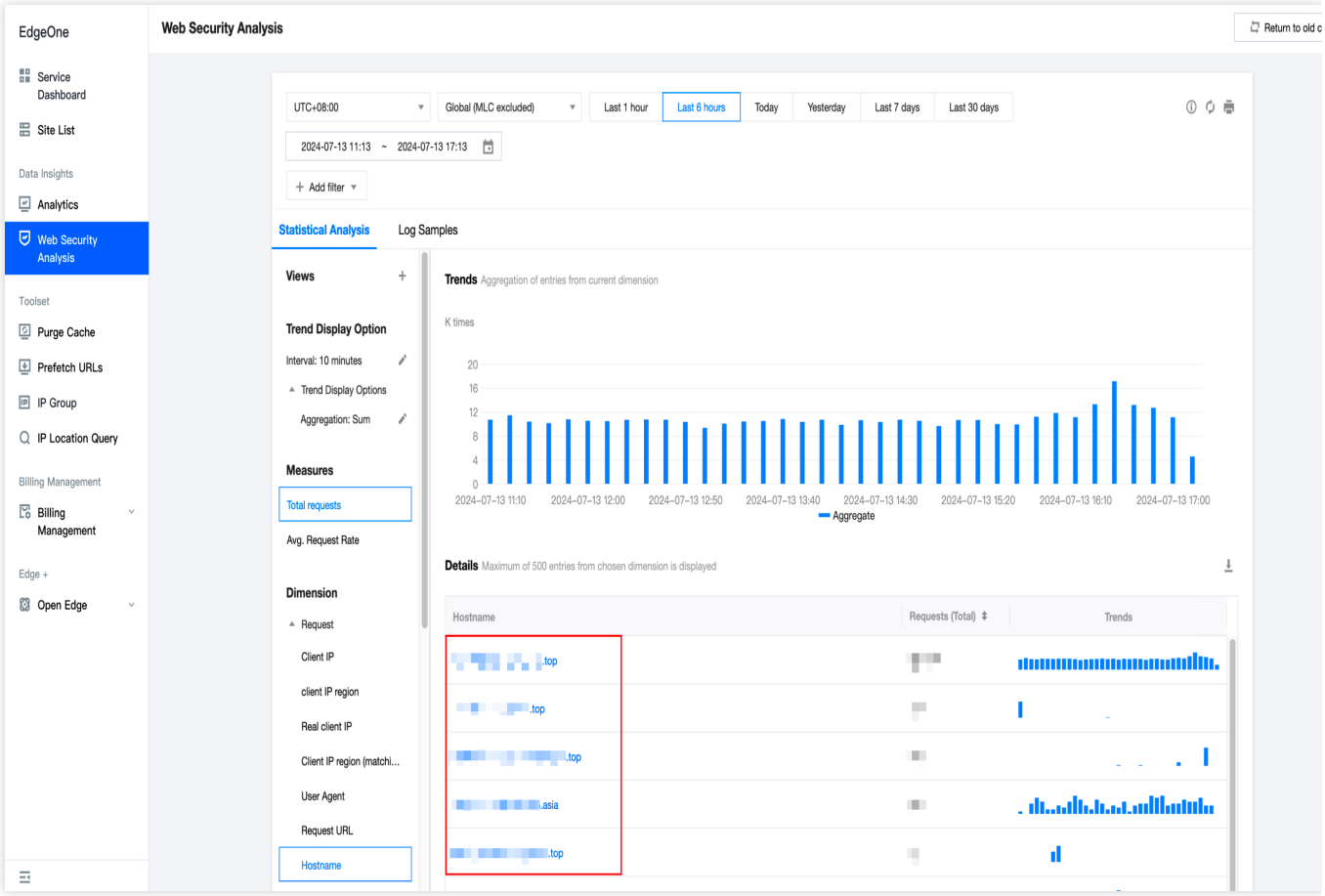
Data Insights

Under the primary navigation of the new console, we have reorganized the **Data Insights** category to help you more quickly view business conditions.

Under the primary navigation of the new console, we have introduced **Metric Analysis**, supporting a unified interface to centrally view multi-dimensional data like access traffic, cache, origin pull, security protection, and L4 proxy, making it easier for you to quickly and comprehensively grasp business dynamics.



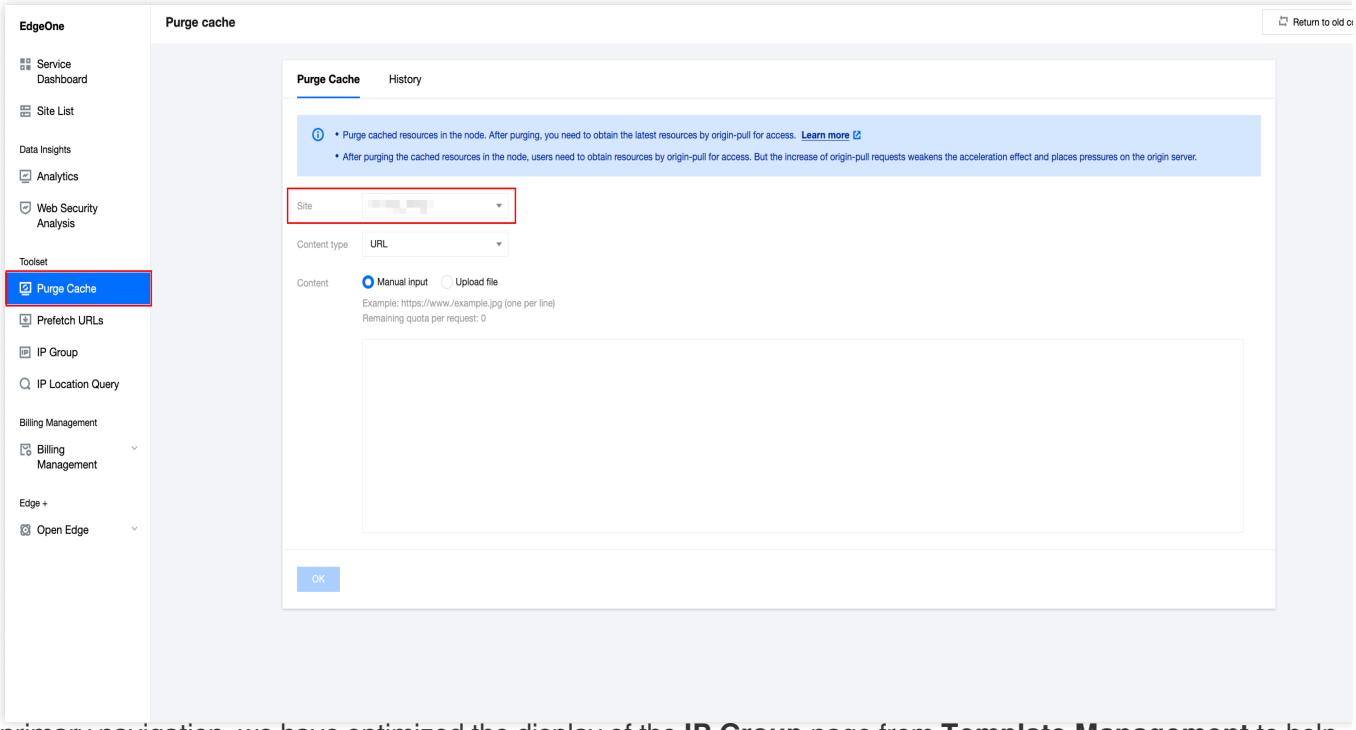
In the new console, **Web Security Analysis** has been elevated to the primary navigation, supporting simultaneous query of security logs for multiple sites, helping you enhance operations security policy.



Toolset

Under the primary navigation of the new console, we have added a **Toolset** category, integrating tool-type features into the primary navigation to improve operations efficiency for you.

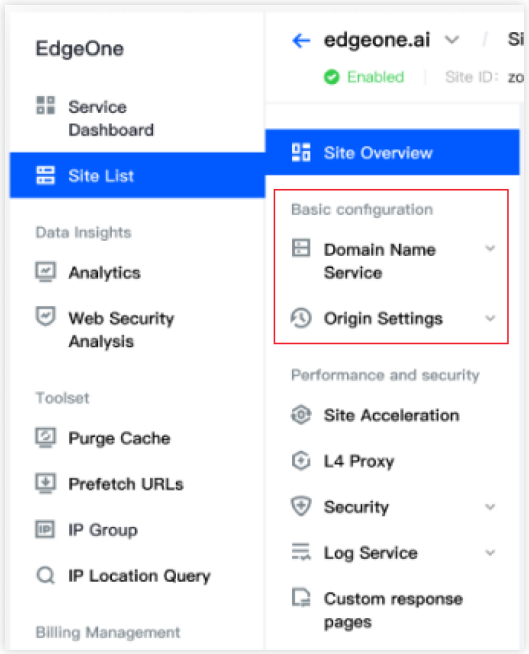
In the old console, **Purge Cache** and **Prefetch URLs** can be executed only after you enter a specific site. If multiple sites are involved, you have to switch sites multiple times in the secondary navigation to perform operations. After the update, these operations can be directly completed in the primary navigation.



In the primary navigation, we have optimized the display of the **IP Group** page from **Template Management** to help you quickly locate specific IP group configurations. The security policy template list originally displayed in the **Protection templates** has been moved to the **Web Security** module under the secondary navigation, with added support for viewing the list of domains associated with security policy templates, helping you better determine the scope of the policy's effectiveness.

Basic Configuration

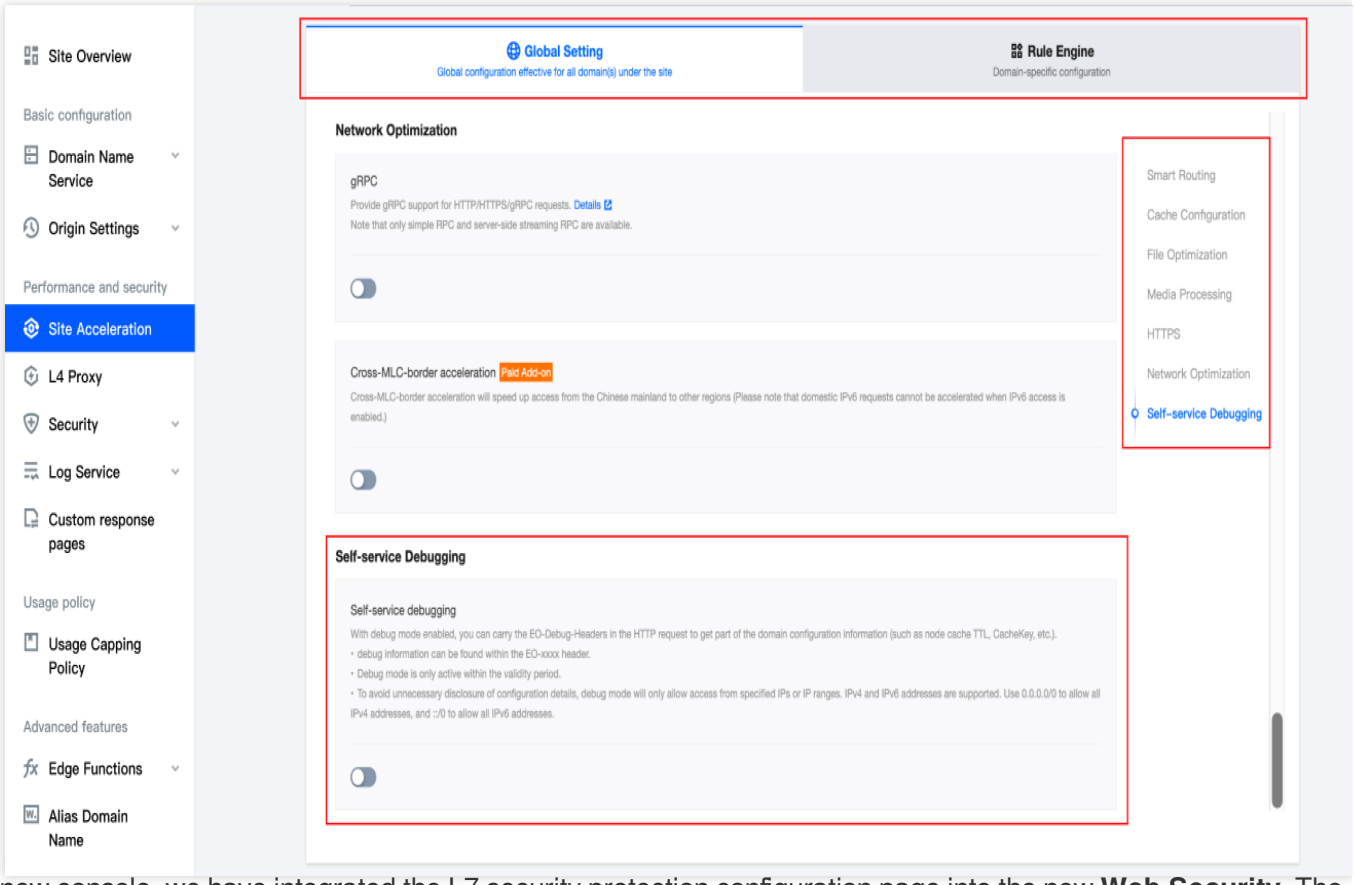
Under the secondary navigation of the new console, we have added a **Basic configuration** category and included **Domain Name Service** and **Origin Settings** in this category. There are no changes to the subdirectories and features of **Domain Name Service** and **Origin Settings**.



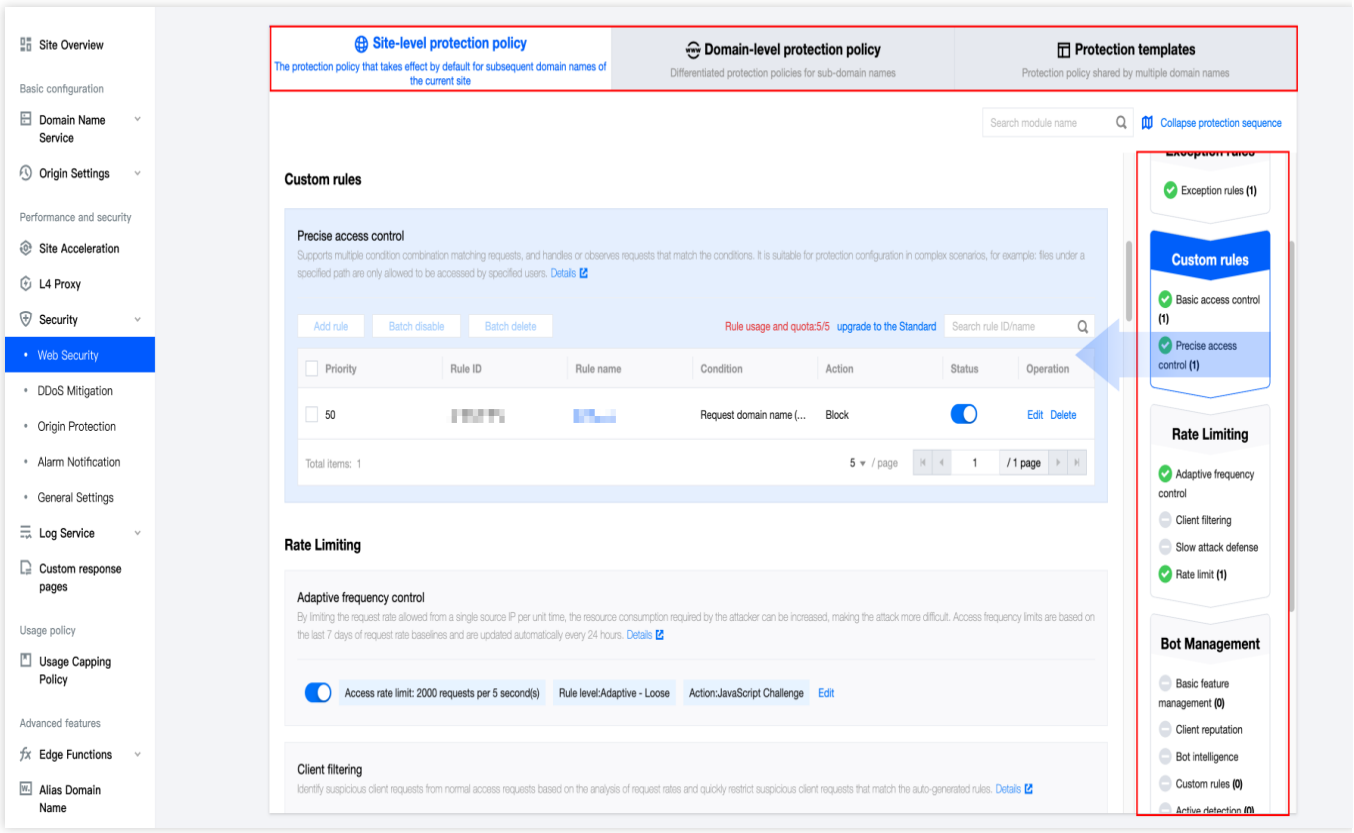
Performance and Security

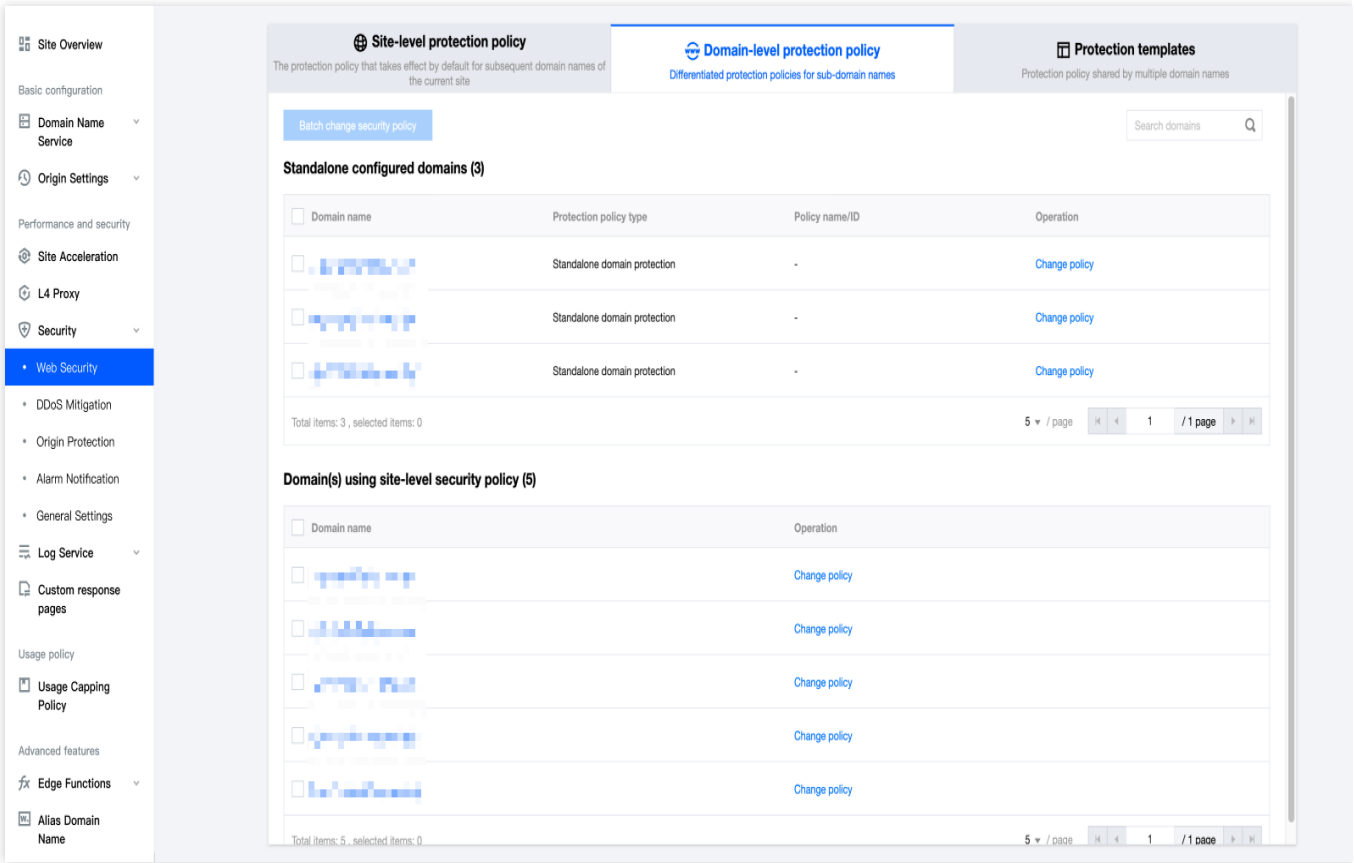
Under the secondary navigation of the new console, we have reorganized the **Performance and security** category to help you quickly complete acceleration and security configurations.

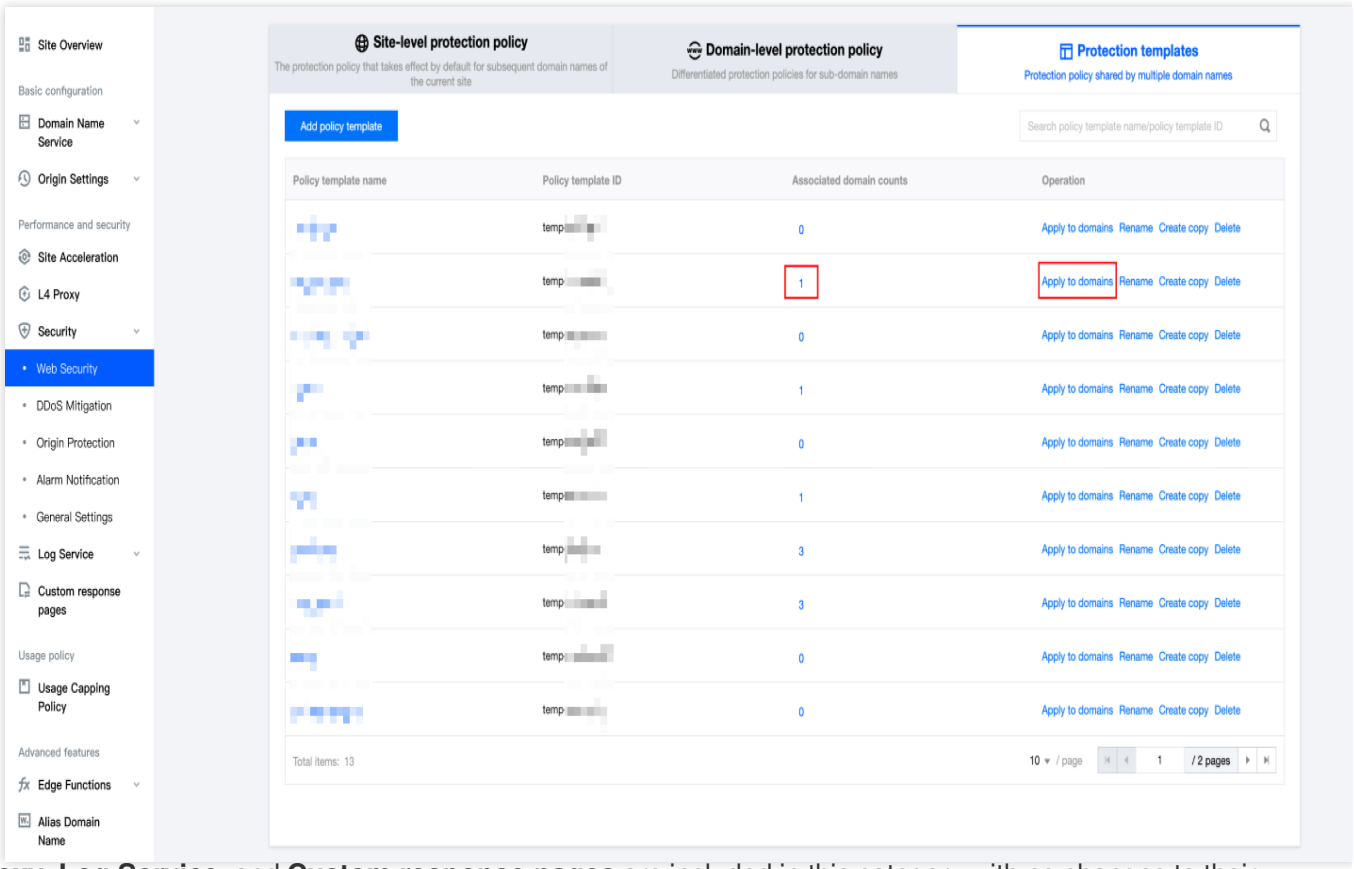
In the new console, we have defined **Site Acceleration** as the entry point for all L7 acceleration configurations. The page is divided into **Global Setting** and **Rule Engine** to facilitate easier global and differentiated acceleration configurations. Additionally, in the site's **Global Setting**, we have consolidated all the subdirectories and features under the original **Site Acceleration** into a single screen for easier feature location, search, and configuration. **Self-service Debugging** has also been merged into **Global Setting** to help you quickly verify whether your cache configurations are effective.



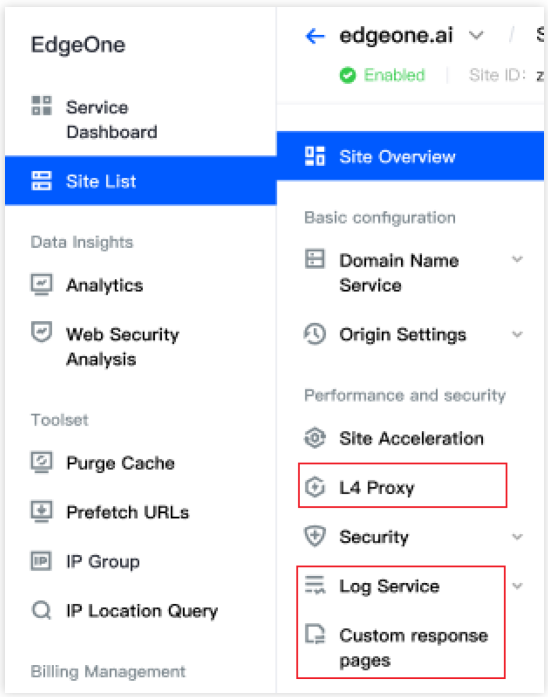
In the new console, we have integrated the L7 security protection configuration page into the new **Web Security**. The new **Web Security** page includes all configuration items from the original **Web Security**, **Bot Management**, **Custom rules**, and **Policy Template** under security protection, unifying the interaction methods of various configurations. Additionally, a **protection sequence** is newly presented on the right side of the page, allowing you to quickly locate specific feature modules by clicking the security feature names on the right side. The new **Web Security** page better assists you in understanding the execution sequence of EdgeOne's L7 security configurations, quickly finding security configuration items, and improving your work efficiency in security operations.


Site Overview
Basic configuration
Domain Name Service
Origin Settings
Performance and security
Site Acceleration
L4 Proxy
Security
Web Security
DDoS Mitigation
Origin Protection
Alarm Notification
General Settings
Log Service
Custom response pages
Usage policy
Usage Capping Policy
Advanced features
Edge Functions
Alias Domain Name
Site-level protection policy
The protection policy that takes effect by default for subsequent domain names of the current site
Domain-level protection policy
Differentiated protection policies for sub-domain names
Protection templates
Protection policy shared by multiple domain names
Search module name
Collapse protection sequence
Custom rules
Precise access control
Supports multiple condition combination matching requests, and handles or observes requests that match the conditions. It is suitable for protection configuration in complex scenarios, for example: files under a specified path are only allowed to be accessed by specified users. Details
Add rule
Batch disable
Batch delete
Rule usage and quota:5/5 upgrade to the Standard
Search rule ID/name
Priority
Rule ID
Rule name
Condition
Action
Status
Operation
50
Request domain name (...
Block
Edit Delete
Total items: 1
5 / page
1
/ 1 page
Rate Limiting
Adaptive frequency control
By limiting the request rate allowed from a single source IP per unit time, the resource consumption required by the attacker can be increased, making the attack more difficult. Access frequency limits are based on the last 7 days of request rate baselines and are updated automatically every 24 hours. Details
Access rate limit: 2000 requests per 5 second(s)
Rule level:Adaptive - Loose
Action:JavaScript Challenge
Edit
Client filtering
Identify suspicious client requests from normal access requests based on the analysis of request rates and quickly restrict suspicious client requests that match the auto-generated rules. Details
Exception rules (1)
Custom rules
Basic access control (1)
Precise access control (1)
Rate Limiting
Adaptive frequency control
Client filtering
Slow attack defense
Rate limit (1)
Bot Management
Basic feature management (0)
Client reputation
Bot intelligence
Custom rules (0)


Site Overview
Basic configuration
Domain Name Service
Origin Settings
Performance and security
Site Acceleration
L4 Proxy
Security
Web Security
DDoS Mitigation
Origin Protection
Alarm Notification
General Settings
Log Service
Custom response pages
Usage policy
Usage Capping Policy
Advanced features
Edge Functions
Alias Domain Name
Site-level protection policy
The protection policy that takes effect by default for subsequent domain names of the current site
Domain-level protection policy
Differentiated protection policies for sub-domain names
Protection templates
Protection policy shared by multiple domain names
Batch change security policy
Search domains
Standalone configured domains (3)
Domain name
Protection policy type
Policy name/ID
Operation
Standalone domain protection
-
Change policy
Total items: 3 , selected items: 0
5 / page
1
/ 1 page
Domain(s) using site-level security policy (5)
Domain name
Operation
Change policy
Total items: 5 , selected items: 0
5 / page
1
/ 1 page



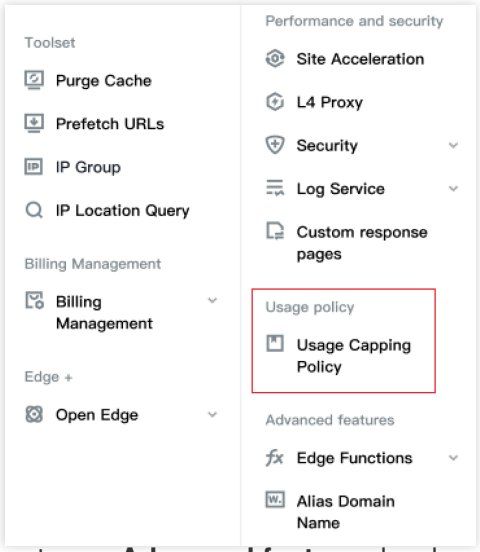
L4 Proxy, **Log Service**, and **Custom response pages** are included in this category with no changes to their subdirectories and features.



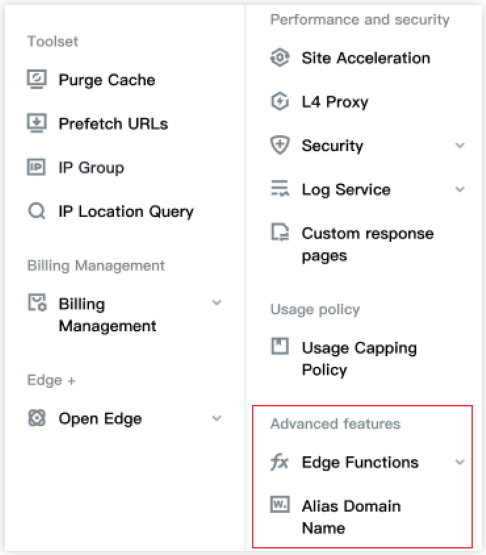
Others

The new console no longer provides the **Speed Test Tools** - **Performance Monitoring** module. If you have already created related applications, you can continue using them in Tencent Cloud console - RUM.

A new category **Usage policy** has been added to the secondary navigation of the new console, and **Usage Capping Policy** is included in this category.

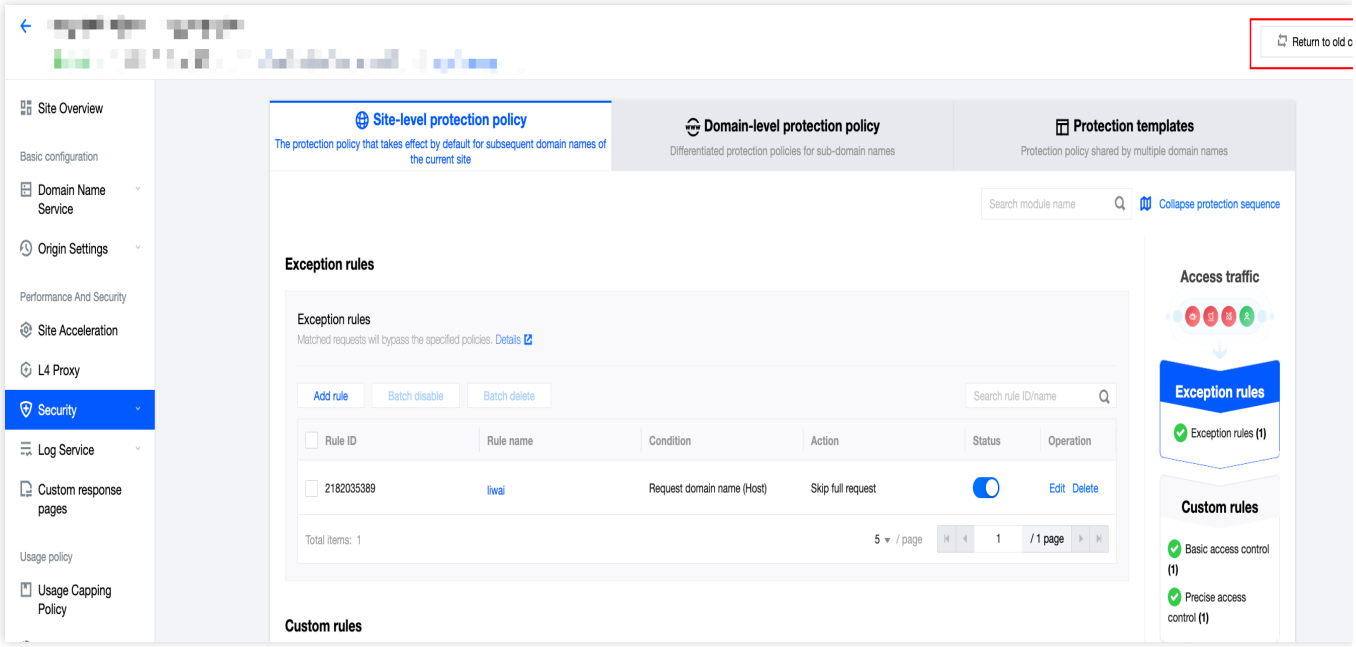


A new category **Advanced features** has been added to the secondary navigation of the new console, and **Edge Functions** and **Alias Domain Name** are included in this category, with no changes to their subdirectories and features.



Transition Plan

To prevent any disruption of your usage due to unfamiliarity with the new console, we have provided a button at the top right corner to return to the old console. You can switch back to the old console at any time without affecting your business configurations and data. Please feel free to operate.


Site Overview
Basic configuration
Domain Name Service
Origin Settings
Performance And Security
Site Acceleration
L4 Proxy
Security
Log Service
Custom response pages
Usage policy
Usage Capping Policy
Site-level protection policy
The protection policy that takes effect by default for subsequent domain names of the current site
Domain-level protection policy
Differentiated protection policies for sub-domain names
Protection templates
Protection policy shared by multiple domain names
Search module name
Collapse protection sequence
Exception rules
Exception rules
Matched requests will bypass the specified policies. Details
Add rule
Batch disable
Batch delete
Search rule ID/name
Rule ID
Rule name
Condition
Action
Status
Operation
2182035389
liwai
Request domain name (Host)
Skip full request
Edit Delete
Total items: 1
5 / page
1
/ 1 page
Custom rules
Access traffic
Exception rules
Exception rules (1)
Custom rules
Basic access control (1)
Precise access control (1)

【Tencent Cloud EdgeOne】Cloud API Change Notification

Last updated：2024-04-15 10:48:39

Due to CAM Authentication requirements, Tencent Cloud EdgeOne will change all cloud API parameters involving site ID (ZoneId/ZoneIds) from optional to mandatory after May 30, 2024. It is suggested that you adjust the API input parameters before this date to avoid API call errors. If you have already input the parameter or have not called the above API, this adjustment will not affect you.

The specific impact is as follows:
Taking the DescribePurgeTasks API as an example, the current ZoneId parameter of this API is optional, and you need to input the site to be queried when calling the API.

Parameter Name	Required	Type	Description
Action	Yes	String	Common Params. The value used for this API: DescribePurgeTasks.
Version	Yes	String	Common Params. The value used for this API: 2022-09-01.
Region	No	String	Common Params. This parameter is not required.
ZoneId	No	String	ZoneId. The parameter is required.

The list of specific APIs involved is as follows:
DescribePrefetchTasks
DescribePurgeTasks
DescribeDefaultCertificates
DescribeApplicationProxies
DescribeOriginProtection
DescribeOriginGroup
DescribeTimingL4Data
DownloadL7Logs
DownloadL4Logs
DescribeTimingL7AnalysisData
DescribeTopL7CacheData

DescribeTopL7AnalysisData
DescribeOverviewL7Data
DescribeTimingL7CacheData
DescribeDDoSAttackEvent
DescribeDDoSAttackTopData
DescribeDDoSAttackData