Web Application Firewall

FAQs

©2013–2026 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2026 Tencent Cloud. All rights reserved.

The complete copyright of this document, including all text, data, images, and other content, is solely and exclusively owned by Tencent Cloud Computing (Beijing) Co., Ltd. ("Tencent Cloud"); Without prior explicit written permission from Tencent Cloud, no entity shall reproduce, modify, use, plagiarize, or disseminate the entire or partial content of this document in any form. Such actions constitute an infringement of Tencent Cloud's copyright, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Trademark Notice

Tencent Cloud

This trademark and its related service trademarks are owned by Tencent Cloud Computing (Beijing) Co., Ltd. and its affiliated companies("Tencent Cloud"). The trademarks of third parties mentioned in this document are the property of their respective owners under the applicable laws. Without the written permission of Tencent Cloud and the relevant trademark rights owners, no entity shall use, reproduce, modify, disseminate, or copy the trademarks as mentioned above in any way. Any such actions will constitute an infringement of Tencent Cloud's and the relevant owners' trademark rights, and Tencent Cloud will take legal measures to pursue liability under the applicable laws.

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

FAQs
- Product Consultation
- Integration
  - Real Server
  - Port Support
  - Domain Name
  - CNAME
  - Associated Product
- Usage
- Permissions
- Sandbox Isolation Status

©2013–2026 Tencent Cloud. All rights reserved.

FAQs
Product Consultation

Last updated: 2024-11-26 09:55:02

Can I use, migrate, and share WAF instances across accounts?

No, you cannot use, migrate, or share WAF instances across accounts.

Is WAF available to servers outside Tencent Cloud?

- SAAS-WAF supports access for data centers outside Tencent Cloud. It can protect any server in public networks, including but not limited to Tencent Cloud, clouds of other manufacturers, and IDCs.
- CLB-WAF only supports integration for CLB users on Tencent Cloud.

> **Note:**
> Domain names connected in the Chinese mainland must be ICP filed as required by the Ministry of Industry and Information Technology of China.

Does WAF support HTTPS protection?

SAAS-WAF and CLB-WAF fully support HTTPS services. Users just need to upload SSL Certificates and TLS private keys as instructed, or select Tencent Cloud-hosted certificates, to protect HTTPS traffic with WAF.

Does the WAF QPS limit apply to the entire instance, or to a single domain name?

The QPS limits for SAAS-WAF and CLB-WAF apply to the entire instance. For example, if protection is configured for three domain names, the total QPS for these three domains must not exceed the specified upper limit. If the purchased instance's QPS limit is exceeded, speed will be limited, resulting in packet loss.

Can Anti-DDoS Pro instances be used for WAF?

Yes, you can enable high defense capabilities for WAF by directly selecting the IP of either a SAAS-WAF instance or a CLB-WAF instance on the configuration page in the Anti-DDoS Pro console. For more details, refer to Combination of Anti-DDoS Pro and Web Application Firewall .

Are there any risks in uploading an SSL certificate's private key?

©2013-2026 Tencent Cloud. All rights reserved.

An SSL certificate's private key hosted on Tencent Cloud will enjoy extremely high security, in terms of:

Uploading stage

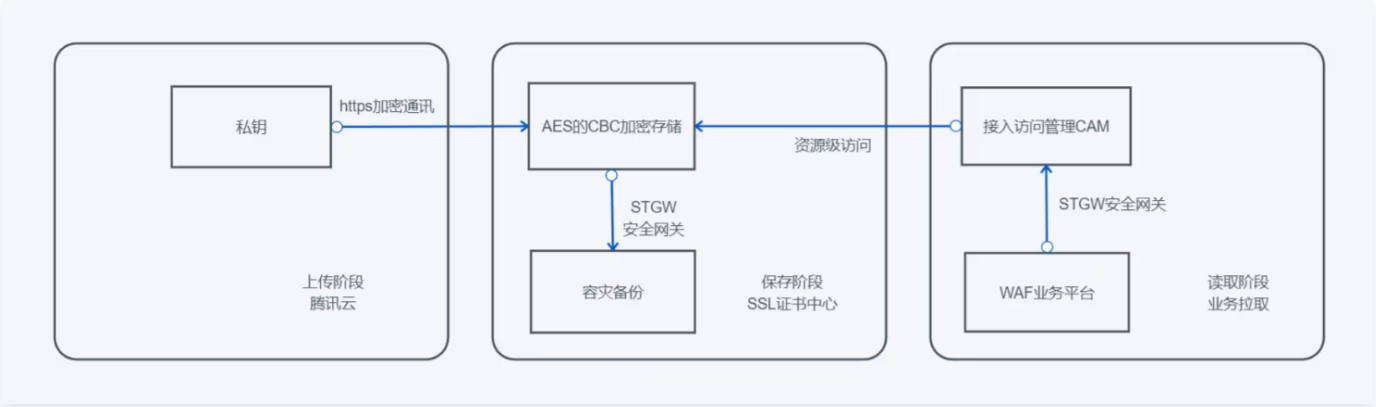
The process from uploading the private key to configuring the certificate on the Tencent Cloud certificate hosting platform is protected with HTTPS, an encrypted communication, and enterprise SSL certificates, ensuring the safety of communication data.

Saving stage

1. After uploading, the certificate is stored in the database. The certificate's private key will be encrypted using the AES CBC mode, which effectively prevents the private key from brute force attacks.
2. The certificate database will be backed up for disaster recovery. For high availability and high security of the certificate data, no external APIs will be used and the data will be protected by STGW.
3. There are multiple backend servers for SSL certificates, which are accessed via a load balancer to ensure API stability.

Managing and reading certificates

1. When customers manage certificates, Tencent Cloud SSL Certificates Center integrates with CAM (Cloud Access Management) at the "resource level", offering a comprehensive permission management system. Customers can grant different permissions to different subaccounts for various certificates, preventing malicious revocation and deletion operations.
2. The certificate pulling in WAF is protected by STGW. The business pulls the certificate on demand while identifying and authenticating the source of the request to avoid illegal and unnecessary access.



Is the SSL mutual authentication supported by both the SaaS WAF and CLB WAF?

©2013–2026 Tencent Cloud. All rights reserved.

It is supported by CLB WAF but not by SaaS WAF.

What are the differences between Web Application Firewall (WAF) and Tencent Cloud Firewall (CFW)?

The differences between WAF (Web Application Firewall) and CFW (Cloud Firewall) are as follows:

©2013–2026 Tencent Cloud. All rights reserved.

Type	Tencent Cloud WAF (Web Application Firewall)		Tencent Cloud CFW
	SaaS WAF	CLB WAF (Cloud Load Balancer WAF)	
Protection Object	Websites and API services.	Websites and API services.	All services exposed to the internet.
Applicable Scenario	Cybersecurity classified protection, intensifying protection, web and API security protection, application layer protection, and anti-cheating protection.	Cybersecurity classified protection, intensifying protection, web and API security protection, application layer protection, anti-cheating protection, and layer-7 CLB instance application.	Customers with classified protection or heavy duty protection needs, or those focused on CVM host and network security.
Core Protection Capability	• Web vulnerability and unknown threat prevention, and self-service false negative and false positive handling. • CC attack protection. • API security and business security. • Anti-leak and anti-tampering.	• Web vulnerability and unknown threat prevention, and self-service false negative and false positive handling. • CC attack protection. • API security and business security. • Protected IPv6 access to websites.	IPS virtual patching, which eliminates the needs for realistic CVM patches and restarting. The basic vulnerability defense for OWASP top 10 attacks is covered. Automatic detection for compromised hosts and automatically blocking CVM malicious external connections. Domain name-based active external connection control.
		It is a Tencent Cloud native service.	

©2013-2026 Tencent Cloud. All rights reserved.

Core Strength	The wide scenarios ranging the application needs of users both within and outside Tencent Cloud.	native service, which can be connected without adjusting the existing network architecture. Web business forwarding and security protection are separated, making it easy to bypass with one click, ensuring web business safety, stability, and reliability. It supports multi-region access and is only available to Tencent Cloud users.	The cloud-native firewall can be enabled with one click, without affecting your business. It integrates security capabilities, such as IPS, threat intelligence, and omission scanning, necessary for multi-level protection and cybersecurity assurance scenarios, which is only available to Tencent Cloud users.
How to Choose	For businesses requiring web and API security protection for both Tencent Cloud and local IDCs, we recommend using SaaS WAF.	For businesses using or planning to use layer-7 CLB instances, we recommend using CLB WAF.	CFW is recommended for those who have concerns over the security of CVM (whether it will be overwhelmed), and businesses exposed on the internet that expose public network businesses in addition to web businesses.

How does WAF prioritize hit rules?

The hit priorities for WAF rules are: precision allowlist > IP allowlist > API throttling > IP blocklist > regional blocking, mini program protection, access control, CC rules, BOT protection, web protection (rule engine), AI engine > tamper-proof, sensitive data prevention.

©2013-2026 Tencent Cloud. All rights reserved.

Integration
Real Server

Last updated: 2024-11-26 09:55:39

Can the real server IP added to WAF be the private IP of a Tencent Cloud CVM instance?

When adding a domain name to WAF, the real server address must be a domain name or a public IP, such as CVM public IP, CLB public IP, or Egress IP of other local IDCs, while a CVM private IP is not supported.

What is the purpose of an origin IP?

The origin-pulling IP is automatically assigned after configuring the protected domain in a SaaS-type WAF. When WAF forwards traffic to the customer origin server, it will use these origin-pulling IP addresses as the source address. Therefore, users need to set the WAF origin-pulling IP addresses as trusted IPs on the server. To achieve better protection, it is recommended that the origin server only allows access traffic from the WAF origin-pulling IPs.

How many real server IPs can be set for one protected domain name in WAF?

Up to 50 origin server IPs can be set for one protected domain name in WAF.

How does the traffic balancing work when multiple real servers are configured in WAF?

If multiple forwarding IPs are configured, WAF achieves load balancing for access requests by polling.

Does WAF automatically add a forwarding IP range to a security group?

WAF does not automatically add a high-defense forwarding IP range to a security group. Please refer to Getting Started to add the relevant forwarding IP to the security group.

©2013-2026 Tencent Cloud. All rights reserved.

Port Support

Last updated: 2024-11-26 09:56:17

Which ports does SaaS-type WAF support?

You can view and configure the ports supported by the SaaS-type WAF package in the console.

1. Log in to WAF Console, and in the left navigation, select **Asset Center** > **Access Management**. By default, you will enter the domain access page.
2. On the domain access page, click **Add Domain** to enter the page for adding domains.
3. In the **Server Configuration** section of the add domain page, select the appropriate protocol to view and configure the port. A maximum of 5 ports can be configured for each domain.
   - By default, WAF Premium supports HTTP (80/8080) and HTTPS (443/8443) standard ports but not non-standard ports.
   - WAF Enterprise and Ultimate support non-standard ports in addition to the default HTTP (80/8080) and HTTPS (443/8443) standard ports as listed below:

Protocol Name	Port
HTTP Protocol	80,81,82,83,84,85,86,87,88,89,97,800,805,808,1000,1090,2020,3333,3501,3601,5000,5222,6001,6666,7000,7001,7002,7003,7004,7005,7006,7007,7008,7009,7010,7011,7012,7013,7014,7015,7016,7018,7019,7020,7021,7022,7023,7024,7025,7026,7040,7070,7081,7082,7083,7088,7097,7510,7621,7777,7800,8000,8002,8003,8004,8005,8006,8007,8008,8009,8010,8011,8012,8020,8021 ,8022,8060,8025,8026,8060,8077,8078,8080,8081,8082,8083,8086,8087,8088,8089,8090,8106,8181,8182,8184,8210,8215,8334,8336,8445,8686,8800,8888,8889,8999,9000,9001,9002,9003,9021,9023,9027,9037,9080,9081,9082,9180,9182,9200,9201,9205,9207,9208,9209,9210,9211,9212,9213,9898,9908,9916,9918,9919,9928,9929,9939,10000,10001,10080,10083,12601,20080,20083,25060,28080,28080,33702,48800,52301
HTTPS Protocol	443,4443,5100,5200,5443,6443,7443,8084,8085,8091,8442,8443,8553,8663,9443,9550,9553,9663,10803,18980

Note:

- If you use Ultimate Edition and need to protect ports not included in the HTTP or HTTPS list, WAF offers the non-standard port customization service (for ports 1-65535). You can customize up to five non-standard ports for all

©2013-2026 Tencent Cloud. All rights reserved.

domain names in your plan. If you need this service, submit a ticket for assistance.

- Ports already in the HTTP or HTTPS list cannot be customized for other protocols.
- If you need HTTP and HTTPS non-standard ports, submit a ticket to have them added to the allowlist.

©2013-2026 Tencent Cloud. All rights reserved.

Domain Name

Last updated: 2024-11-26 09:56:38

How do I connect a domain name?

You can connect a domain name using the WAF Console. For more information, see Add a Domain Name.

Does WAF support wildcard domain names?

Yes. You can add a wildcard domain name directly in the WAF Console.

Note:

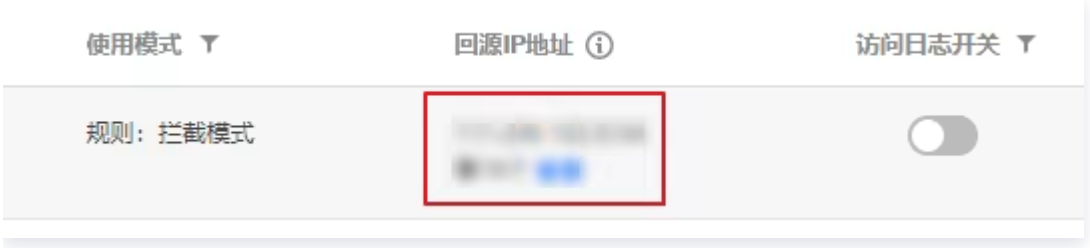
- If a wildcard domain (such as `*.test.com`) is accessed through Cloud WAF, subdomains of that wildcard domain can be accessed by other accounts.
- If you have added both a wildcard domain and a specific domain (for example: `*.test.com`, `a.test.com`), WAF will prioritize the protection policy configured for the specific domain.

How long does it take to update the DNS resolution (protection) status of my domain name?

Please check if your website's domain CNAME configuration is correct. After adding the CNAME record in DNS, the status update time is estimated to be 10 – 20 minutes, so please be patient. If you have completed the setup and the waiting time exceeds 30 minutes but the protection status has not been updated, you can submit a ticket to contact us for assistance.

Will the domain name origin-pull IP addresses change?

During maintenance, upgrades, or other such situations, WAF may change the domain's back-to-origin IP address. If there's a change, we will notify you in advance via SMS, email, or on-site messages. The specific back-to-origin IP addresses can be confirmed in the Domain List on the console.



Will the SaaS WAF-connected VIP address change?

©2013-2026 Tencent Cloud. All rights reserved.

The VIP address may change when WAF is maintaining and upgrading its in/cross-region disaster recovery capabilities. To ensure the service availability, WAF only supports configuring VIP addresses by adding the CNAME.

Can I modify the SaaS WAF-connected VIP address?

SaaS-based WAF instances do not support the request to change the service VIP address of a domain. If an anomaly occurs with the domain bound to an instance, please check if it is under a DDoS attack; meanwhile, you can submit a ticket to contact us, and we will address your issue promptly.

What are the requirements for connecting a domain name to WAF?

If the origin server domain for WAF protection belongs to Mainland China, the origin server business content must be valid and complete MIIT recordal.

- If the origin server does not have an ICP filing, you need to complete the ICP filing through Tencent Cloud. For the filing process, see How to Quickly File Your Website.
- If the origin server is on Tencent Cloud but the ICP filing was completed with another service provider, you need to re-submit the ICP filing through Tencent Cloud. For the filing process, see Filling in ICP Filing Information.

> **Note:**
> If the instance to which you add the domain name is a SaaS WAF instance, you also need to add a CNAME record at the DNS service provider of the domain name. Set the record value to the CNAME allocated by WAF.

What options does WAF offer for domain name origin-pull?

WAF performs origin-pull based on domain name or IP. You can choose either option to configure as needed. For more information, see Adding Domain Names.

How do I bind a CNAME to my domain name connected to WAF?

You can refer to modify DNS resolution to bind CNAME at your DNS service provider.

Will the CNAME change if my domain name is deleted and added again?

The domain name will change after being deleted and re-added in the console. Specific values can be found in the WAF console domain list, under instance information.

©2013-2026 Tencent Cloud. All rights reserved.

When adding a domain name to WAF, how should the origin domain be specified?

When you add a domain name to WAF, you must specify a forwarding domain name. It can be the CNAME of proxy or another domain name. The protocol type (HTTP or HTTPS) is not required.

©2013–2026 Tencent Cloud. All rights reserved.

CNAME

Last updated：2024-11-26 09:56:58

How do I configure CNAME?

- You cannot access the CNAME domain name directly. You need to complete the CNAME configuration at your domain name service provider. Once the configuration takes effect, WAF will protect your domain name. For detailed CNAME configuration steps, refer to Modifying DNS Resolution.
- If the CNAME configuration is completed, a CNAME domain name with a suffix like `.qcloud xxx.com` (e.g., `.qlcoudcjpj.com`, `qcloudwzgj.com`) will be automatically assigned to your domain after it is connected to WAF. You can view it in the instance information in the WAF Console Domain List.

Associated Product

Last updated：2024-11-26 09:57:54

How do I use WAF together with CDN or Anti-DDoS Pro services?

- You can use WAF with Anti-DDoS Pro directly, or use it with CDN by setting the CDN origin server IP as the IP of a WAF instance. Recommended deployment architecture: Client > CDN > WAF + Anti-DDoS Pro > CLB > Origin Server.
- If you need the CDN and Anti-DDoS capabilities, simply set the CNAME provided after the connection to WAF as the CDN origin server, and associate Anti-DDoS Pro with the WAF instance. In this way, the user traffic, after going through CDN, is forwarded to WAF, which has the capability of cleansing high-traffic DDoS attacks, and finally reaches the real server for full protection.

How do I connect a CDN domain name to WAF?

If the CDN domain name is already connected, simply set the CNAME address assigned by WAF as the CDN origin server. The traffic will flow according to the architecture of user > CDN > WAF > CLB > origin server. Additionally, you can log in to the WAF console, navigate to the Add Domain Name page, and select 'Yes' for the proxy option. WAF will then use the XFF field in the HTTP header to obtain the client's real IP, ensuring proper protection.

©2013-2026 Tencent Cloud. All rights reserved.

Usage

Last updated: 2024-11-26 10:04:09

How do I download access logs of the last 180 days?

The Access Log feature records the access log information of WAF-protected domains, providing access log queries and download features for the protection domains within the user-defined log retention period (up to 180 days). To download access logs for 180 days, please enable the respective domain's access log switch and set log storage to 180 days in the console. For more details, see Access Logs.

Does WAF support health check?

The SaaS-type WAF supports a Layer 4 health check mechanism and can be enabled upon domain integration for Enterprise editions and above, conducting proactive health status checks on all origin server IPs every 3 seconds. For more information about the health check mechanism, please Submit a Ticket to inquire.

Does WAF support session persistence?

WAF supports session persistence. To enable it, please submit a ticket to contact us for assistance.

Will logging still be available once WAF is disabled for the domain name list?

No. Once WAF is disabled, all its protection features are unavailable, and only the traffic forwarding mode starts to run instead, with no logs recorded.

When will a configuration change take effect?

Generally, the changed configuration takes effect within 10 seconds.

> **Note**
> This section is for modifying access configurations (e.g., origin server address, connection method, whether to enable HTTP2.0, etc.), and is not related to protection configurations.

The VIP of WAF-protected domain name is blocked due to DDoS attacks. What should I do?

©2013-2026 Tencent Cloud. All rights reserved.

WAF's VIP comes with the default Anti-DDoS Basic capability (protection capacity of 2Gb). In case of blockage in Anti-DDoS Basic and urgent restoration of service is needed, please purchase an Anti-DDoS Pro instance and bind it to the WAF's VIP address.

If uploading files is blocked, will uploading files using HTTPS or SFTP still be blocked?

If WAF is disabled, the file will not be blocked. If WAF is enabled and the blocking mode is set, WAF will block malicious files uploaded over HTTP or HTTPS, but will not block files uploaded over SFTP. SFTP is a non-HTTP or non-HTTPS protocol beyond the protection of WAF.

Will the persistent connection be disconnected when the WAF certificate is changed?

No. Updating the certificate will reload nginx, and the thread will not be recycled until the end of the old request session, so it will not be disconnected.

What cipher suites does the SaaS WAF support?

- In the SaaS WAF, the supported cipher suites and their corresponding TLS protocol versions are as follows:

©2013-2026 Tencent Cloud. All rights reserved.

Cipher Suite Name	Supported Protocol Version	Security Encryption Suite	General Encryption Suite
DES-CBC3-SHA	TLSv1.0 TLSv1.1 TLSv1.2	No	Yes
ECDHE-RSA-DES-CBC3-SHA		No	Yes
AES256-SHA		Yes	Yes
AES128-SHA		Yes	Yes
ECDHE-RSA-AES256-SHA		Yes	Yes
ECDHE-ECDSA-AES256-SHA		Yes	Yes
ECDHE-RSA-AES128-SHA		Yes	Yes
ECDHE-ECDSA-AES128-SHA		Yes	Yes
AES256-SHA256	TLSv1.2	Yes	Yes
AES256-CCM8		Yes	Yes
AES128-SHA256		No	Yes
AES256-CCM		Yes	Yes
AES256-GCM-SHA384		Yes	Yes
ECDHE-RSA-AES256-SHA		Yes	Yes
ECDHE-RSA-AES256-SHA384		Yes	Yes
ECDHE-RSA-AES256-GCM-SHA384		Yes	Yes
AES128-CCM8		Yes	Yes
AES128-CCM		Yes	Yes
AES128-GCM-SHA256		Yes	Yes

©2013-2026 Tencent Cloud. All rights reserved.

ECDHE-RSA-AES128-SHA256		Yes	Yes
ECDHE-RSA-CHACHA20-POLY1305		Yes	Yes
ECDHE-RSA-AES128-GCM-SHA256		Yes	Yes
TLS_AES_128_GCM_SHA256		Yes	Yes
TLS_CHACHA20_POLY1305_SHA256		Yes	Yes
TLS_AES_256_GCM_SHA384		Yes	Yes

- WAF supports the following TLS versions:
  - Protocol Versions: TLSv1, TLSv1.1, TLSv1.2, and TLSv1.3.
  - Cipher suites: EECDH+CHACHA20:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3DES:RSA+3DES:!MD5.

> **Note**
> - SaaS WAF supports ECDHE cipher suites by default (such as TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA).
> - The CLB WAF cipher suite depends on CLB, Cloud Native Gateway, and the user's definition of the gateway's own support for the TLS protocol.

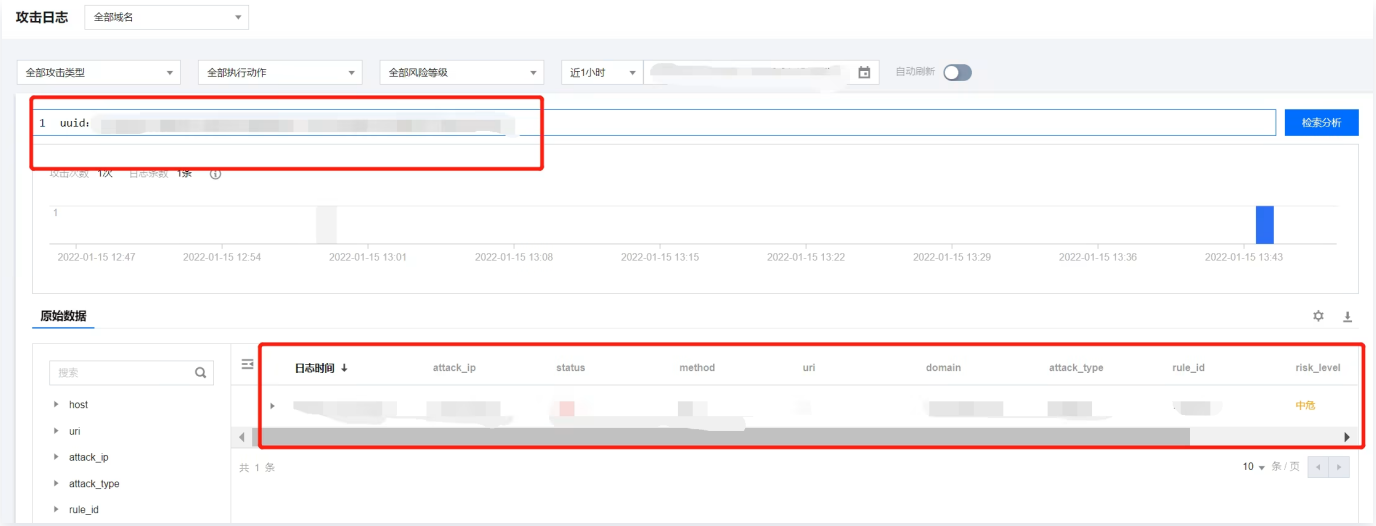
How do I query the module hit by a block page?

1. When a malicious request is detected, WAF blocks the request and returns a block page with a UUID.

©2013-2026 Tencent Cloud. All rights reserved.

2. Copy the current identification code and search for it on the Attack Log Page to view interception packet information.

> **Note**
>
> - Please check the time range during the retrieval.
> - Intercepted packages are mainly divided into several fields: "attack_type" for the type of attack, "rule_id" for the rule ID, and "attack_content" for the content of the attack field. Based on these fields, the rule that was hit can be identified, facilitating subsequent operations by users.



©2013–2026 Tencent Cloud. All rights reserved.

©2013–2026 Tencent Cloud. All rights reserved.

Permissions

Last updated: 2024-11-26 10:04:29

How to handle sub-account permission errors after enabling the log delivery service?

You can fix permission errors by creating a new custom policy in CAM > **Policies**. Specific examples are as follows:

Note:

- For more details, refer to Creating Custom Policies and Sub-account Authorization Guide.
- Please use the root account for authorization.

1. Log in to the CAM console, and in the left navigation menu, select **Policies**.
2. On the Policies page, click **New Custom Policy** and select **Create by policy syntax**.

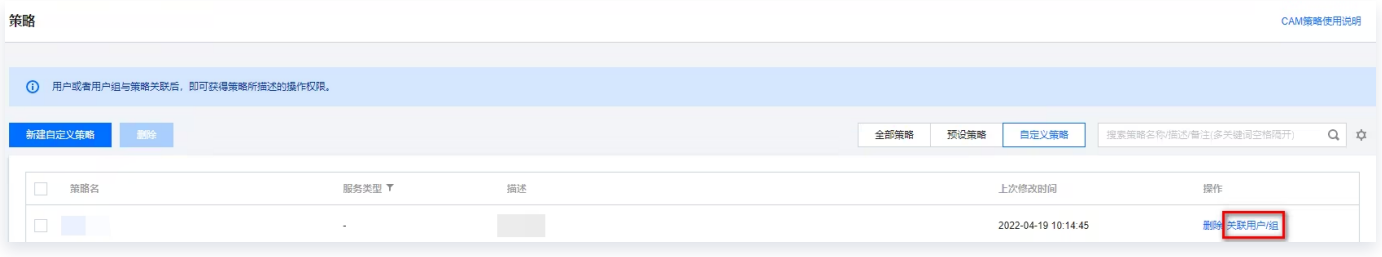
3. On the Select policy template page, select **Blank Template**, then click **Next**.

©2013-2026 Tencent Cloud. All rights reserved.

4. On the Edit Policy page, enter the policy name and description, and input the following code in the policy content:

```
{
  "version": "2.0",
  "statement": [
 {
   "action": [
     "cls:DescribeTopics",
     "ckafka:DescribeInstanceAttributes",
     "ckafka:DescribeTopic",
     "ckafka:DescribeRoute",
     "ckafka:DescribeInstances",
     "ckafka:DescribeInstancesDetail"
   ],
   "resource": "*",
   "effect": "allow"
 }
  ]
}
```

5. Click **Complete**, return to the policies page, select the newly created policy, and click **Associate Users/Groups** in the actions column.



©2013–2026 Tencent Cloud. All rights reserved.

6. In the Associate Users/Groups pop-up window, check the required users/groups, and click **Confirm**.

©2013-2026 Tencent Cloud. All rights reserved.

Sandbox Isolation Status

Last updated: 2026-03-11 17:13:07

On the same calendar day, if the business QPS peak of an instance exceeds the instance's specification value but does not reach the instance's sandbox isolation threshold a cumulative of 3 times (including 3 times), or if the QPS peak exceeds the instance's sandbox isolation threshold 1 time (including 1 time), the instance's business traffic will immediately enter the sandbox isolation status. Instances in sandbox isolation status will no longer have guaranteed SLA.

This document will introduce what sandbox isolation status is, the conditions for an instance to enter sandbox isolation status, and how to lift the sandbox isolation status of an instance.

1. Overview of Isolated Cluster

Isolated Cluster is a dedicated isolation space set up for abnormal instance traffic where the actual business QPS peak exceeds the QPS traffic specification value.

Instance QPS Traffic Specification Value

Instance QPS Traffic Specification Value is the sum of the internal QPS specification value of the version, the extended QPS specification value, and the Elastic Postpaid QPS value. The calculation method of the instance QPS traffic specification value is as follows:

Instances without Elastic Postpaid enabled

Instance QPS Specification Value = Purchased QPS Specification Value = Default QPS of Package Version + Extended QPS of Business Expansion Pack

Instances with Elastic Postpaid enabled

Instance QPS Specification Value = Purchased QPS Specification Value + Elastic QPS Specification Value = Default QPS of Package Version + Extended QPS of Business Expansion Pack + Elastic Postpaid QPS

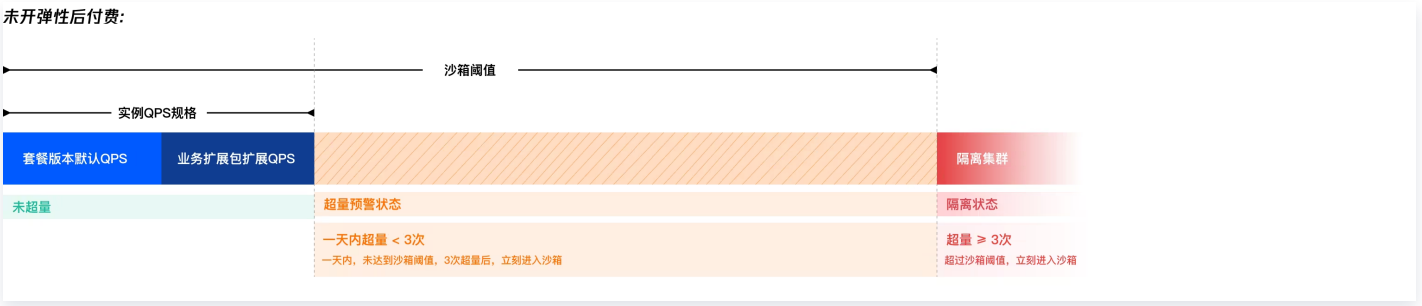
©2013-2026 Tencent Cloud. All rights reserved.

Sandbox Isolation Threshold

The Sandbox Isolation Threshold is the maximum protection QPS threshold that WAF instances of different QPS specifications can temporarily serve. Once the instance exceeds this QPS Sandbox Isolation Threshold, it will immediately enter the isolated cluster. The calculation of the instance QPS Sandbox Isolation Threshold is as follows:

Instances without Elastic Postpaid enabled and without custom purchased business expansion packs

Instance QPS Sandbox Isolation Threshold = Purchased QPS Specification Value * 3
Example: If a SaaS WAF instance of the Enterprise Edition in the Chinese mainland region purchased 3 expansion packs, the instance QPS Sandbox Isolation Threshold = (5000 + 3*1000) * 3.
Search for the required CAM policy as needed, and click to complete policy association.



Instances without Elastic Postpaid enabled and with custom purchased business expansion packs

Instance QPS Sandbox Isolation Threshold = Max[Instance QPS Specification Value, Instance Version Max QPS Sandbox Isolation Threshold]
Instance Version Max QPS Sandbox Isolation Threshold = (Default QPS Specification Value of Package Version + Max Expandable QPS Specification Value of Instance) * 3

- Example 1: If a SaaS WAF instance of the Enterprise Edition in the Chinese mainland region, after custom application, purchased 40 expansion packs. The instance QPS Specification Value = 5000 + 40*1000 = 45000, the Instance Version Max QPS Sandbox Isolation Threshold = (5000 + 30000) * 3 = 105000. Instance QPS Sandbox Isolation Threshold = Max[45000, 105000] = 105000 QPS.

©2013–2026 Tencent Cloud. All rights reserved.

- Example 2: If an Enterprise Edition WAF instance in the Chinese mainland region, after applying for customization, has purchased 150 expansion packages, the instance QPS specification limit = 5000 + 150*1000 = 155000 QPS. The maximum QPS Sandbox Isolation Threshold of the instance version = (5000 +30000)*3=105000 QPS. Finally, the instance QPS Sandbox Isolation Threshold = max[155000, 105000] = 155000 QPS.
- Example 3: More **instances that have not enabled post-paid elasticity and have customized business expansion packs purchased** are shown in the following data:

©2013-2026 Tencent Cloud. All rights reserved.

Region	Version	Default number of business expansion packages available for purchase	Actual number of business expansion packages purchased	Instance QPS specification limit	Maximum QPS Sandbox Isolation Threshold of the instance version	Instance QPS Sandbox Isolation Threshold
Regions in the Chinese Mainland	Advanced Edition	20	30	2500+30*1000=42500	(2500+20*1000)*3=67500	67500
	Enterprise Edition	30	80	5000+80*1000=85000	(5000+30*1000)*3=105000	105000
			120	5000+120*1000=125000		125000
	Flagship Edition	40	100	10000+100*1000=110000	(10000+40*1000)*3=150000	150000
			150	10000+150*1000=160000		160000
Non-Chinese Mainland Regions	Advanced Edition	5	10	2500+10*1000=12500	(2500+5*1000)*3=22500	22500
	Enterprise Edition	10	12	5000+12*1000=17000	(5000+10*1000)*3=45000	45000
			50	5000+50*1000=55000		55000
				10000+6		

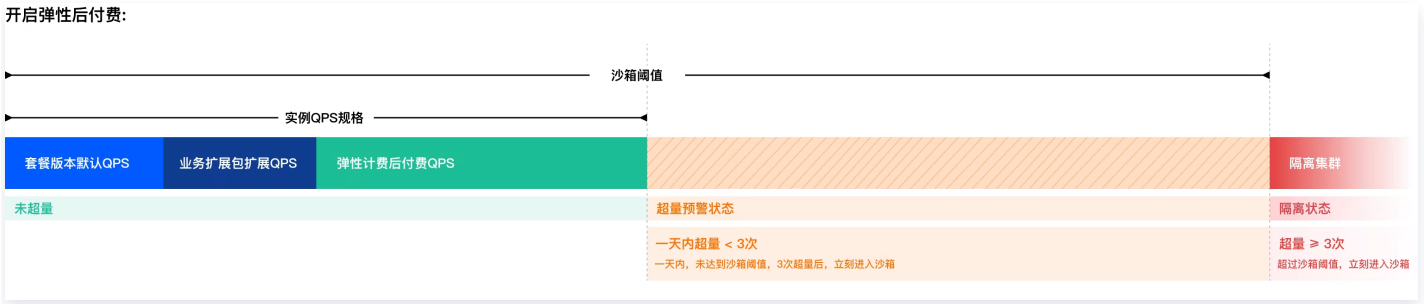
©2013–2026 Tencent Cloud. All rights reserved.

	Flagship Edition	20	60	0*1000= 70000	(10000+ 20*1000)*3=900 00	90000
			100	10000+1 00*1000 =110000		110000

Note:
For WAF instances in different regions and editions, the maximum number of business expansion packages (including the maximum scalable QPS specifications) varies. Refer to Plans and Editions for details.

Instances with Elastic Postpayment enabled and no custom business expansion package purchased

Instance QPS Sandbox Isolation Threshold = Purchased QPS specifications * 3 + Elastic QPS specifications
Example: If an Enterprise Edition WAF instance in the Mainland China Region has purchased 3 expansion packages, with Elastic Billing enabled and the specifications set to 50000, the instance QPS Sandbox Isolation Threshold = (5000 + 3*1000) * 3 + 50000.
Search for the required CAM policy as needed, and click to complete policy association.



Instances with Elastic Postpayment enabled and custom business expansion package purchased

Instance QPS Sandbox Isolation Threshold = Max[Instance QPS specifications, Maximum QPS Sandbox Isolation Threshold of the instance version]
Maximum QPS Sandbox Isolation Threshold of the instance version = (Default QPS specifications of the edition + Maximum scalable QPS specifications of the instance) * 3 + Elastic QPS specifications

- Example 1: If an Enterprise Edition WAF instance in the Chinese mainland Region, after applying for customization and purchasing 40 expansion packages, enabled Elastic Billing with the specifications set to 50000. The Instance QPS specifications = 5000 + 40*1000 + 50000 = 95000, the Maximum QPS Sandbox Isolation Threshold of the instance version =

©2013–2026 Tencent Cloud. All rights reserved.

(5000 + 30000) * 3 + 50000 = 155000. The Instance QPS Sandbox Isolation Threshold = Max[95000, 155000] = 155000 QPS.

- Example 2: If an Enterprise Edition WAF instance in the Chinese mainland Region, after applying for customization and purchasing 150 expansion packages, enabled Elastic Billing with the specifications set to 50000. The Instance QPS specifications = 5000 + 150*1000 + 50000 = 205000 QPS, the Maximum QPS Sandbox Isolation Threshold of the instance version = (5000 + 30000) * 3 + 50000 = 155000 QPS. The Instance QPS Sandbox Isolation Threshold = Max[205000, 155000] = 205000 QPS.
- Example 3: More instances with **Elastic Postpayment enabled and custom business expansion package purchased** sample data are as follows:

Region	Version	Default number of business expansion packages available for purchase	Default maximum Elastic QPS	Actual number of business expansion packages purchased	Elastic postpayment actual enabled specification value	Instance QPS specification limit	Maximum QPS Sandbox Isolation Threshold of the instance version	Instance QPS Sandbox Isolation Threshold
Regions in the Chinese Mainland	Advanced Edition	40	200000	10	200000	2500+10*1000+200000=212500	(2500+40*1000)*3+200000=287500	287500
	Enterprise Edition	60	300000	100	300000	5000+100*1000+300000=405000	(5000+60*1000)*3+300000= 435000	405000
				120		5000+120*1000+300000=425000		435000
	Flagship Edition	80	400000	100	400000	10000+100*1000+400000=510000	(10000+80*1000)*3 + 400000 =590000	590000
			400000	150	400000	10000+150*1000+400000=560000		590000
Non-Chinese Mainland Regions	Advanced Edition	10	Not involved	10	Not involved	2500+10*1000=12500	(2500+10*1000)*3=27500	27500
	Enterprise Edition	20		12		5000+12*1000=17000	(5000+20*1000)*3=55000	55000
				50		5000+50*1000=55000	(5000+20*1000)*3=55000	55000
	Flagship Edition	40		60		10000+60*1000=70000	(10000+40*1000)*3=110000	110000
				100		10000+100*1000=110000	(10000+40*1000)*3=110000	110000

2. Conditions for entering and ending isolation status

If the instance's QPS peak exceeds the instance's QPS specification limits but is less than the instance's QPS sandbox isolation threshold three times (inclusive) within the same calendar day, or exceeds the instance's QPS sandbox isolation threshold once (inclusive), the instance will immediately enter the isolation cluster. For instances in the isolation cluster, WAF will no longer guarantee service SLA.

©2013–2026 Tencent Cloud. All rights reserved.

> **Note:**
> - Rule for determining QPS overage frequency: WAF will obtain the QPS average at each time point in real-time (10s), then take the peak value at each time point as the instance's QPS peak.
> - If the instance's QPS peak exceeds the instance's QPS specification limits but does not exceed the instance's QPS sandbox isolation threshold, it is determined as one overage. Each 5-minute period, QPS overage circumstances are combined and counted as one overage. If the instance's QPS overage frequency reaches three times, the instance will immediately enter the isolation status.
> - If the instance's QPS peak exceeds the current instance's QPS sandbox isolation threshold once, the overage frequency for the day will no longer be calculated, and the instance will directly enter the isolation status.

After the instance enters the isolation status, you can expand the instance's QPS specification limits. Once the expanded instance's QPS specification limits exceed the maximum business peak, the isolation will automatically end, and normal protection and product service SLA will resume. If the instance's QPS specification limits are not expanded, the business QPS peak must continuously drop below the instance's QPS specification limits for three consecutive calendar days for the instance to exit the isolation status.

3. Impact of entering the isolation cluster on business

- The instances entering the isolation cluster will no longer guarantee the product SLA (i.e., regardless of whether the instance's QPS exceeds the specifications, WAF does not guarantee service availability). Domain names and instance protection objects connected to this instance may experience business access abnormalities at any time, including but not limited to packet loss, rate limiting, connection limiting, protection failure, abnormal logs or report data, access timeout, entering DDoS cleaning or black hole situations.
- After an instance enters the isolation cluster, the system will notify you via email, SMS, or station letter. You can also view QPS overrun warnings and alarm events at the top of the Security Overview and Instance Management pages in the console.
- After an instance enters the isolation cluster, if you enable elastic post-paid or purchase a business expansion package to extend the instance's QPS specification, and the extended instance's QPS specification is greater than the maximum business peak of the day's QPS overrun, the instance isolation status can be immediately lifted.

4. Viewing the isolation status instance

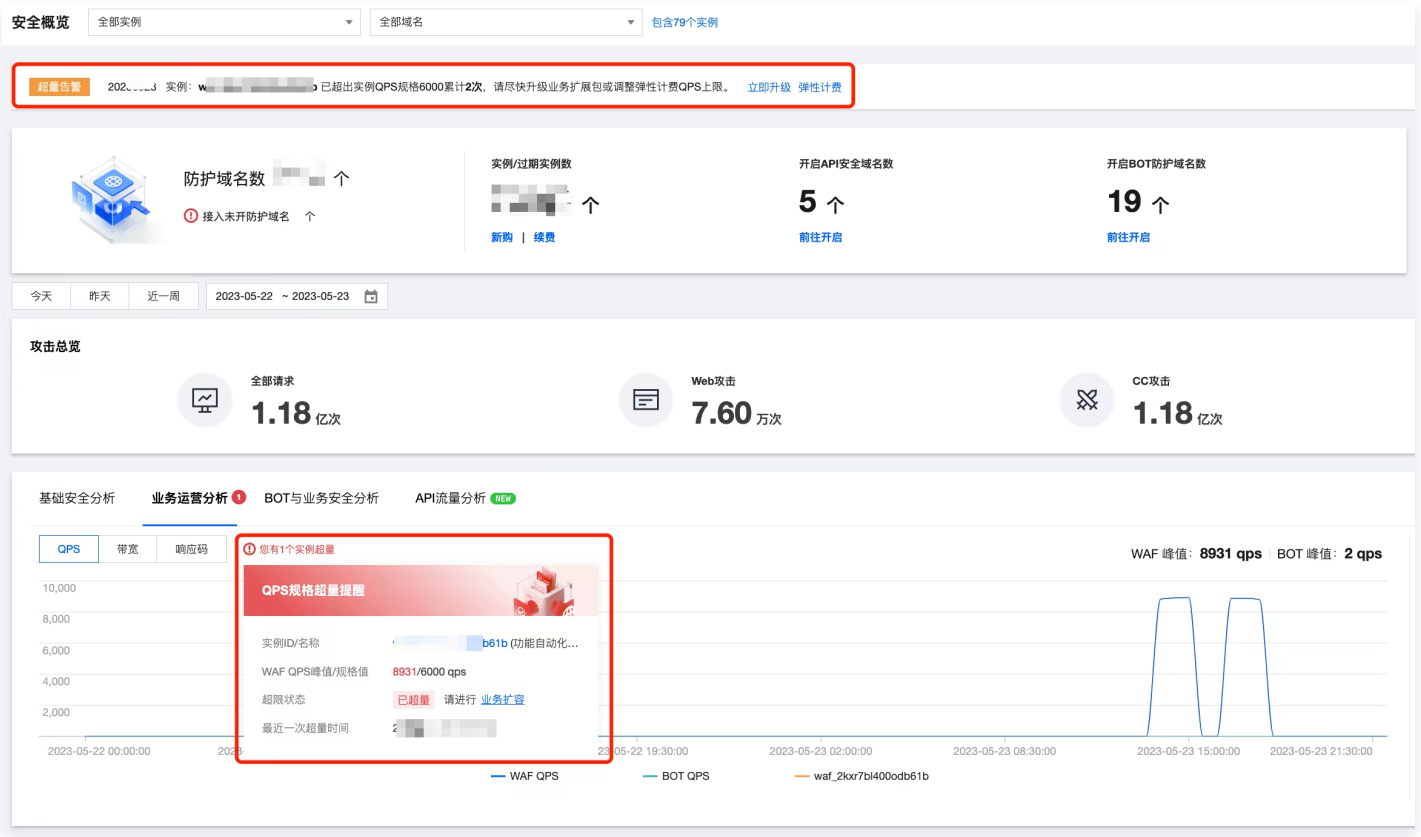
After exceeding the QPS usage limit, you will receive an alert event notification at the top of the Instance Management page in the WAF console (Illustration 1); at the same time, in the

©2013-2026 Tencent Cloud. All rights reserved.

instance list's specification section, you can view the peak QPS of the business and the QPS specification value of the instance within the last 30 days. If there has been an overage event in the past 30 days, it will be highlighted in red and support clicking to jump to the Security Overview page to view the QPS traffic trend of that instance within the last 30 days (Illustration 2).

Search for the required CAM policy as needed, and click to complete policy association.

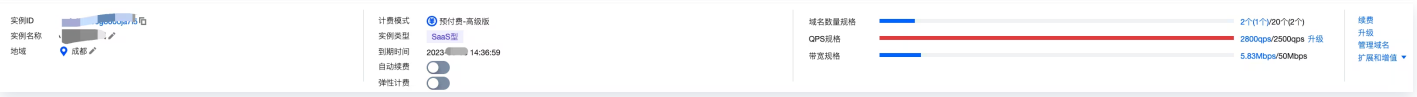
Search for the required CAM policy as needed, and click to complete policy association.



After exceeding the QPS limit and entering isolation status, the Security Overview page will show an isolation status alert; click **Business Operation Analysis**. In the QPS section, you can view the actual QPS usage through the QPS peak graph.

©2013–2026 Tencent Cloud. All rights reserved.

Search for the required CAM policy as needed, and click to complete policy association.



5. How to exit the sandbox isolation status of the instance

The isolation status of annual and monthly subscription instances will not be automatically lifted within the same day, even if the actual QPS usage has fallen below the instance's QPS specification value. You need to either expand the QPS specification value of the instance or have the business QPS peak value fall below the instance's QPS specification value for three consecutive natural days to lift the instance's isolation status. If, after upgrading, your instance's QPS again exceeds the limit and enters isolation status, you will need to expand the QPS specification value of the instance again.
You can end the instance isolation status in the following two ways:

Upgrade the package or business expansion package of the instance to expand the QPS specification value

On the Instance Management page, select the instance that has exceeded the limit, click **Upgrade** > **Domain Expansion Package/Business Expansion Package** to upgrade the package QPS specification, or click **Extensions and Add-ons** > **Business Expansion Package** to expand the instance's QPS specification value. Once the expanded instance QPS specification value exceeds the maximum business peak value at the time of QPS overage on that day, the product will automatically lift the instance's isolation status, and the instance will resume normal service SLA, while the QPS overage count will be reset to zero.
Search for the required CAM policy as needed, and click to complete policy association.

Enable elastic billing to expand the QPS specification value

1. For instances without elastic billing enabled, go to the Instance Management page and click on the target **Instance ID**.

©2013-2026 Tencent Cloud. All rights reserved.

2. On the instance details page, click to expand the QPS specification value.

   Search for the required CAM policy as needed, and click to complete policy association.

3. After enabling elastic billing, you can adjust and increase the elastic billing limit to expand the QPS specification value. Once the adjusted instance QPS specification value exceeds the maximum business peak value at the time of QPS overage on that day, the product will automatically lift the instance's isolation status, and the instance will resume normal service SLA, while the QPS overage count will be reset to zero.

©2013–2026 Tencent Cloud. All rights reserved.