

Alibaba Cloud

Web应用防火墙 Product Introduction

Document Version: 20220707

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
 Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings> Network> Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.What is WAF?	05
2.WAF deployment plans and editions	08

1. What is WAF?

provides end-to-end security protection for your websites or apps. WAF effectively identifies and filters out malicious web traffic, and then forwards normal traffic to your origin server. This protects your origin server from attacks and ensures data and service security.

Features

Feature		Description
Service configuration		WAF protects HTTP and HTTPS traffic of websites.
Web application protection	Protection against common web application attacks	<ul style="list-style-type: none">• Protection against common Open Web Application Security Project (OWASP) attacks: The common OWASP attacks include SQL injection, cross-site scripting (XSS), webshell upload, backdoors, command injection, unauthorized HTTP requests, common vulnerabilities of web servers, unauthorized access to core files, path traversal, and scan attacks.• Hiding of origin IP addresses: WAF prevents origin IP addresses from being exposed. Attackers cannot bypass to attack origin servers.• Regular and timely updates of patches for zero-day vulnerabilities: WAF updates patches at the earliest opportunity.• User-friendly monitoring mode: You can enable this mode to monitor new website services. WAF alerts rather than blocks suspicious attacks that match specified protection rules to help measure false positives.
	Precise protection	<ul style="list-style-type: none">• WAF parses HTTP data in common formats. The HTTP data includes header, form, multipart, JSON, and XML data.• WAF decodes data that is encoded by using the following methods: URL encoding, JavaScript Unicode encoding, HEX encoding, HTML entity encoding, Java serialization, PHP serialization, Base64 encoding, UTF-7 encoding, UTF-8 encoding, and nested encoding.• WAF preprocesses data to provide more fine-grained and accurate data sources for detection engines at the upper layer. The preprocessing mechanisms include space compression, comment pruning, and special character processing.• WAF detects data in complicated formats. WAF supports specific complexity in detection logic to prevent false positives caused by excessive detection operations. This reduces the false positive rate. WAF also supports adaptive decoding of data encoded in different formats. This prevents bypassing.

Feature		Description
	Protection against HTTP flood attacks	<ul style="list-style-type: none"> WAF restricts the frequency of requests from a specific IP address by using different methods, such as CAPTCHA verification and redirection for authentication. To protect against a large number of slow request attacks, WAF executes precise protection rules based on statistical data, such as the distribution of status codes, distribution of requested URLs, abnormal HTTP Referer headers, and User-Agent characteristics. WAF takes full advantage of Alibaba Cloud big data to build analysis models for threat intelligence and trusted access. These models help identify malicious requests.
	Precise access control	<ul style="list-style-type: none"> In the WAF console, you can combine different HTTP fields, such as IP, URL, Referer, and User-Agent fields, to configure protection rules and implement precise access control. You can configure custom protection rules to provide protection in different scenarios, such as hotlink protection and website background protection. The combination of different security modules, such as web security and HTTP flood protection, helps build a multi-layer protection architecture. This way, WAF can identify trusted and malicious traffic.
	Virtual patching	Before the patches for web application vulnerabilities are released or installed, you can adjust web protection rules to protect your services.
Attack event management		WAF allows you to manage attack events based on statistical data, such as attack events, attack traffic, and attack scales.
Reliability		<ul style="list-style-type: none"> Load balancing: WAF can provide services in cluster mode. WAF uses multiple servers to balance loads and supports different scheduling algorithms. Smooth and elastic scaling: You can add servers to or remove servers from a cluster to adjust the WAF service capability based on your business requirements. Preclusion of single points of failure (SPOFs): If a WAF node fails or is repaired, WAF can still provide services.

For more information, visit the [product page of Web Application Firewall](#).


Benefits

Benefit	Description
More than 10 years of web security experience	<ul style="list-style-type: none"> WAF is built on more than 10 years of web security experience of Alibaba Group and provides the same security experience as applications, such as Tmall, Taobao, and Alipay. WAF provides a professional security team. WAF defends against known OWASP vulnerabilities and constantly fixes disclosed vulnerabilities.

Benefit	Description
Protection against HTTP flood attacks and crawler attacks	<ul style="list-style-type: none">• WAF mitigates HTTP flood attacks.• WAF defends against web crawlers to prevent network resource consumption.• WAF detects and blocks malicious requests that may cause negative impacts, such as bandwidth consumption, exhaustion of database, SMS, or API resources, response latency, or even a breakdown.• WAF allows you to configure custom protection rules for various business scenarios.
Integration with big data capabilities	<ul style="list-style-type: none">• WAF can defend against hundreds of millions of attacks every day.• WAF provides an IP address library that contains a large number of IP addresses.• WAF provides a wide range of use cases to help obtain the patterns, methods, and signatures of various common network attacks.• WAF is continuously integrated with advanced technologies for big data analytics.
Ease of use and reliability	<ul style="list-style-type: none">• You can activate and configure WAF within 5 minutes.• You do not need to install software or hardware or adjust routing configurations.• Protection clusters are used to prevent SPOFs and redundancy.• WAF provides high traffic processing performance.

Scenarios

WAF is suitable for all users on and outside Alibaba Cloud. WAF helps protect web applications in industries such as finance, e-commerce, online-to-offline (O2O), Internet Plus, gaming, public service sectors, and insurance.

 **Note** If you use WAF to protect your services, you must add the domain names of your services to WAF. You cannot add IP addresses to WAF.

Use of WAF

After you purchase a WAF instance, you can add the domain name of your website to WAF in CNAME record mode. After you add the domain name, you can change the DNS record of the domain name to the CNAME that is assigned by WAF. This way, the web requests that are destined for the website are forwarded to WAF. For more information, see [Add a domain name](#).

Compliance certifications

WAF has passed various authoritative certifications. The certifications include ISO 9001, ISO 20000, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 29151, BS 10012, Cloud Security Alliance (CSA) STAR certification, China classified protection of cybersecurity-Level III, Service Organization Control (SOC) 1, 2, and 3, Cloud Computing Compliance Controls Catalog (C5), Green Finance Certification Scheme developed by Hong Kong Quality Assurance Agency (HKQAA), Outsourced Service Providers Audit Report (OSPAR), and Payment Card Industry Data Security Standard (PCI DSS).

2.WAF deployment plans and editions


This topic describes different deployment plans and editions supported by Web Application Firewall (WAF). This topic also describes the business scales and protection features supported by different WAF editions.

WAF deployment plans and editions

In subscription mode, WAF provides two deployment plans: On-cloud WAF and Hybrid Cloud WAF. **On-cloud WAF** supports the following editions: **Pro**, **Business**, **Enterprise**, and **Exclusive**. If you want to purchase an On-cloud WAF instance of the Exclusive edition, you must submit a ticket. **Hybrid Cloud WAF** supports only the **Exclusive** edition.

References

- [Billing method](#)
- [Best practices for WAF exclusive clusters](#)
- [Overview of Hybrid Cloud WAF](#)
- [Purchase a WAF instance](#)

 **Notice** If you want to purchase an On-cloud WAF instance of the Exclusive edition, you must submit a .

Editions and supported business scales

The following table lists the business scales supported by each edition. We recommend that you choose the Business or Enterprise edition for medium-sized enterprise websites.

Business specification	On-cloud WAF Pro	On-cloud WAF Business	On-cloud WAF Enterprise	On-cloud WAF Exclusive	Hybrid Cloud WAF Exclusive
Website scale	Small- and medium-sized websites that do not have special security requirements	Medium-sized enterprise-grade websites that provide services to all Internet users and have high data security requirements	Medium- and large-sized enterprise-grade websites that have custom security requirements	Large-sized enterprise-grade websites that require business-specific configurations	Medium- and large-sized enterprise-grade websites whose traffic cannot be protected by On-cloud WAF and that require the web protection capabilities of On-cloud WAF
Peak queries per second (QPS)	2,000	5,000	Higher than 10,000	5,000	0 Scalable

Business specification	On-cloud WAF Pro	On-cloud WAF Business	On-cloud WAF Enterprise	On-cloud WAF Exclusive	Hybrid Cloud WAF Exclusive
Number of nodes in an on-premises protection cluster and peak QPS	Not supported	Supported. Fees are charged.	Supported. Fees are charged.	Supported. Fees are charged.	2 and 10,000
Maximum bandwidth, in Mbit/s (The origin server is deployed on Alibaba Cloud.)	50	100	200	100	0 Scalable
Maximum bandwidth, in Mbit/s (The origin server is not deployed on Alibaba Cloud.)	10	30	50	30	
Default number of second-level domains that can be protected	1	1	1	1,000	200 (The domains are not limited to second-level domains. Each additional node can protect 100 more domains.)
Default number of domains that can be protected in total (Wildcard domains are supported.)	10	10	10	1,000	

Editions and supported features (in the Chinese mainland)

The following table describes the features supported by each edition of WAF in the **Chinese mainland**. A WAF instance uses the subscription billing method.

Symbol descriptions:

- √: indicates that the feature is supported by the edition.
- ×: indicates that the feature is not supported by the edition.
- : indicates that the feature is a value-added service. If you want to enable the feature, you must pay additional fees. You can enable the feature when you purchase or upgrade a WAF instance.

Feature	Description	On-cloud WAF Pro	On-cloud WAF Business	On-cloud WAF Enterprise	On-cloud WAF Exclusive	Hybrid Cloud WAF Exclusive
Website access						
HTTPS protection	Allows you to implement HTTPS protection for websites with a few clicks.	√	√	√	√	√
HTTP/2 protection	Protects websites that use HTTP/2.	×	√	√	√	√
Non-standard port protection	Protects traffic on ports other than standard ports 80, 8080, 443, and 8443.	×	√	√	√	√
IPv6 traffic protection	Detects and protects IPv6 traffic.	×	√	√	√	√
Intelligent load balancing	Connects to multiple Server Load Balancer (SLB) SLB service nodes to implement automatic disaster recovery and optimal routing with low latency.	○	○	○	○	○
Exclusive IP address	Provides exclusive IP addresses to protect specific domain names.	○	○	○	○	○
Exclusive cluster	Allows you to customize service access and protection capabilities based on business requirements.	×	×	×	√	√
On-premises protection cluster deployment	Deploys WAF protection clusters in data centers to protect web traffic that does not pass through Alibaba Cloud.	×	○	○	○	√
Website protection						
Protection Rules Engine	Protects your services against common web attacks, such as SQL injection and XSS attacks.	√	√	√	√	√
	Enables automatic update of protection rules against web zero-day vulnerabilities.	√	√	√	√	√

Feature	Description	On-cloud WAF Pro	On-cloud WAF Business	On-cloud WAF Enterprise	On-cloud WAF Exclusive	Hybrid Cloud WAF Exclusive
Custom protection rule group	Allows you to customize protection rule groups.	×	√	√	√	√
Big Data Deep Learning Engine	Detects web zero-day vulnerabilities.	×	√	√	√	×
Positive security model	Provides positive defense capabilities based on deep learning of website traffic.	×	×	√	√	√
Website tamper-proofing	Locks web pages to prevent content tampering.	√	√	√	√	√
Data leak prevention	Prevents the leak of sensitive data, such as ID card numbers, mobile numbers, and bank card numbers.	√	√	√	√	√
HTTP flood protection	Protects your services against common HTTP flood attacks in Prevention or Prevention-emergency mode.	√	√	√	√	√
Blacklist	Blocks access requests from specific IP addresses or CIDR blocks.	√	√	√	√	√
	Blocks access requests from specific IP addresses, specific CIDR blocks, or IP addresses in specific regions.	×	√	√	√	√
Scan protection	Blocks the IP addresses of scanners and blocks the IP addresses from which high-frequency web attacks and path traversal are initiated by using the default rules. This feature provides collaborative defense.	√	√	√	√	√
	Supports the above protection capabilities and allows you to customize rules to block high-frequency web attacks and path traversal.	×	√	√	√	√

Feature	Description	On-cloud WAF Pro	On-cloud WAF Business	On-cloud WAF Enterprise	On-cloud WAF Exclusive	Hybrid Cloud WAF Exclusive
Custom protection policy	Supports access control list (ACL)-based access control by using basic fields, such as IP, URL, Referer, User-Agent, and Params.	√	√	√	√	√
	Supports ACL-based access control by using basic fields and advanced fields. The advanced fields include Cookie, Content-Type, Header, and Http-Method.	×	√	√	√	√
	Allows you to configure throttling policies based on IP addresses and sessions. You can customize HTTP flood protection rules by adding match conditions and configuring throttling policies.	×	√	√	√	√
	Allows you to configure throttling policies based on IP addresses, sessions, and custom fields.	×	×	√	√	√
Data risk control	Protects crucial website services, such as registrations, logons, activities, and forums, against frauds.	○	○	○	○	×
Allowed crawlers	Maintains a whitelist that consists of authorized search engines. The crawlers of these search engines are allowed to access specified domain names.	○	○	○	○	○
Bot threat intelligence	Provides information about suspicious IP addresses that are used by dialers, data centers, and malicious scanners. This feature also maintains an IP address library of malicious crawlers and prevents these crawlers from accessing all pages under your domain name or specific directories.	○	○	○	○	○

Feature	Description	On-cloud WAF Pro	On-cloud WAF Business	On-cloud WAF Enterprise	On-cloud WAF Exclusive	Hybrid Cloud WAF Exclusive
App protection	Provides secure connectivity and anti-bot protection for native apps. This feature can identify requests from proxy servers and emulators and requests with invalid signatures.	○	○	○	○	○
Account security	Detects dictionary attacks, brute-force attacks, spam user registrations, weak passwords, and SMS flood attacks on service endpoints, such as registration and logon endpoints.	√	√	√	√	√
DDoS mitigation	Defends against DDoS attacks of up to 5 Gbit/s free of charge.	√	√	√	√	×
Security analysis and support						
Alert setting	Allows you to configure event monitoring and alerting for WAF.	√	√	√	√	√
Log Service for WAF	Collects and stores all logs, enables near-real-time query and analysis, and provides online reports.	×	○	○	○	○

Editions and supported features (outside the Chinese mainland)

The following table describes the features supported by each edition of WAF outside the Chinese mainland. A WAF instance uses the subscription billing method.

Symbol descriptions:

- √: indicates that the feature is supported by the edition.
- ×: indicates that the feature is not supported by the edition.
- ○: indicates that the feature is a value-added service. If you want to enable the feature, you must pay additional fees. You can enable the feature when you purchase or upgrade a WAF instance.

Feature	Description	On-cloud WAF Pro	On-cloud WAF Business	On-cloud WAF Enterprise	On-cloud WAF Exclusive	Hybrid Cloud WAF Exclusive
Website access						
HTTPS protection	Allows you to implement HTTPS protection for websites with a few clicks.	√	√	√	√	√
HTTP/2 protection	Protects websites that use HTTP/2.	×	√	√	√	√
Non-standard port protection	Protects traffic on ports other than standard ports 80, 8080, 443, and 8443.	×	√	√	√	√
IPv6 traffic protection	Detects and protects IPv6 traffic.	×	×	×	×	√
Intelligent load balancing	Connects to multiple SLB service nodes to implement automatic disaster recovery and optimal routing with low latency.	×	○	○	○	○
Exclusive IP address	Provides exclusive IP addresses to protect specific domain names.	○	○	○	○	○
Exclusive cluster	Allows you to customize service access and protection capabilities based on business requirements.	×	×	×	√	√
On-premises protection cluster deployment	Deploys WAF protection clusters in data centers to protect web traffic that does not pass through Alibaba Cloud.	×	○	○	○	√
Website protection						
Protection Rules Engine	Protects your services against common web attacks, such as SQL injection and XSS attacks.	√	√	√	√	√
	Enables automatic update of protection rules against web zero-day vulnerabilities.	√	√	√	√	√

Feature	Description	On-cloud WAF Pro	On-cloud WAF Business	On-cloud WAF Enterprise	On-cloud WAF Exclusive	Hybrid Cloud WAF Exclusive
Custom protection rule group	Allows you to customize protection rule groups.	×	×	√	√	√
Big Data Deep Learning Engine	Detects web zero-day vulnerabilities.	×	×	×	×	×
Positive security model	Provides positive defense capabilities based on deep learning of website traffic.	×	×	√	√	×
Website tamper-proofing	Locks web pages to prevent content tampering.	×	√	√	√	√
Data leak prevention	Prevents the leak of sensitive data, such as ID card numbers, mobile numbers, and bank card numbers.	×	√	√	√	√
HTTP flood protection	Protects your services against common HTTP flood attacks in Prevention or Prevention-emergency mode.	√	√	√	√	√
Blacklist	Blocks access requests from specific IP addresses or CIDR blocks.	√	√	√	√	√
	Blocks access requests from specific IP addresses, specific CIDR blocks, or IP addresses in specific regions.	×	×	√	√	√
Scan protection	Blocks the IP addresses of scanners and blocks the IP addresses from which high-frequency web attacks and path traversal are initiated by using the default rules. This feature provides collaborative defense.	√	√	√	√	√
	Supports the above protection capabilities and allows you to customize rules to block high-frequency web attacks and path traversal.	×	√	√	√	√

Feature	Description	On-cloud WAF Pro	On-cloud WAF Business	On-cloud WAF Enterprise	On-cloud WAF Exclusive	Hybrid Cloud WAF Exclusive
Custom protection policy	Supports ACL-based access control by using basic fields, such as IP, URL, Referer, User-Agent, and Params.	√	√	√	√	√
	Supports ACL-based access control by using basic fields and advanced fields. The advanced fields include Cookie, Content-Type, Header, and Http-Method.	×	√	√	√	√
	Allows you to configure throttling policies based on IP addresses and sessions. You can customize HTTP flood protection rules by adding match conditions and configuring throttling policies.	×	√	√	√	√
	Allows you to configure throttling policies based on IP addresses, sessions, and custom fields.	×	×	√	√	√
Data risk control	Protects crucial website services, such as registrations, logons, activities, and forums, against frauds.	×	×	×	×	×
Allowed crawlers	Maintains a whitelist that consists of authorized search engines. The crawlers of these search engines are allowed to access specified domain names.	○	○	○	○	○
Bot threat intelligence	Provides information about suspicious IP addresses that are used by dialers, data centers, and malicious scanners. This feature also maintains an IP address library of malicious crawlers and prevents these crawlers from accessing all pages under your domain name or specific directories.	○	○	○	○	○

Feature	Description	On-cloud WAF Pro	On-cloud WAF Business	On-cloud WAF Enterprise	On-cloud WAF Exclusive	Hybrid Cloud WAF Exclusive
App protection	Provides secure connectivity and anti-bot protection for native apps. This feature can identify requests from proxy servers and emulators and requests with invalid signatures.	○	○	○	○	○
Account security	Detects dictionary attacks, brute-force attacks, spam user registrations, weak passwords, and SMS flood attacks on service endpoints, such as registration and logon endpoints.	√	√	√	√	√
DDoS mitigation	Defends against DDoS attacks of up to 5 Gbit/s free of charge.	×	×	×	×	×
Security analysis and support						
Alert setting	Allows you to configure event monitoring and alerting for WAF.	√	√	√	√	√
Log Service for WAF	Collects and stores all logs, enables near-real-time query and analysis, and provides online reports.	×	○	○	○	○