Alibaba Cloud
Anti-Bot Service

Pricing

Issue: 20190527

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 due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information 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.
⚠	This warning information 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 restore business.
📋	This indicates warning information, supplementary instructions, and other content that the user must understand.	ⓘ Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	**It indicates that it is a required value, and only one item can be selected.**	`swich` *{stand | slave}*

Contents

1 Billing method

Anti-Bot Service employs a subscription-based billing method.

Billing method

Billing item: Depends on the subscription package.

Payment method: Subscription.

Billing period: The service is billed monthly or annually based on your order. A bill is generated each time you place an order.

Subscription period: Depends on the purchase date and subscription duration. You can select one of the following subscription durations: one month, three months, six months, one year, two years, and three years.

Expiration: The service stops automatically when the subscription period ends.

- You will receive reminder emails or texts seven days before the expiration date. If you do not renew your subscription before the expiration date, Anti-Bot Service will stop protecting your site when the subscription period ends.
- After the subscription period ends, your Anti-Bot Service configurations will be retained for seven days. If you renew your subscription within these seven days , you can continue to use the previous configurations. If you do not renew your subscription within these seven days, you must buy a new Anti-Bot instance and configure the instance from scratch to use Anti-Bot Service again.

Pricing

The prices of Anti-Bot instances depend on the region and protection module.

Req	Protecti module	Feature	Default specification	Pricing			
				Chinese mainland		International	
				USD/ Year	USD/ Month	USD/ Year	USD/ Month
Yes	Basic Defense	Provides basic protection against bot attacks for Web pages, HTML5, mobile apps, and API services. - You can create custom rules to filter requests based on specific parameters. - You can limit the number of requests to specific URLs based on the IP address, cookie, or header fields of the request. - You can use multiple actions to handle suspicious requests, such as JavaScript validation, slider captcha, block, and monitoring. - You can use data risk control	- Supports HTTP, HTTPS, HTTP/2, and WebSocket. - Supports ports 80/8080 and 443/8443, and more than 50 *non-standard ports*. - Domains: You can only add one TLD and up to 10 subdomains or wildcard domains. Note: If you add more TLDs, you are charged additional fees. For each *additional TLD*, Anti-Bot Service charges USD 236 per month. - Service request rate: 500 QPS Note: If your service request rate	8,490.57	707.55	12,735.85	1,061.32

Req	Protecti module	Feature	Default specification	Pricing			
				Chinese mainland		International	
				USD/ Year	USD/ Month	USD/ Year	USD/ Month
No	Bot Intelligence	Provides large amounts of cyber threat intelligence and updates protection policies against mass attacks. Intelligence sources: · The malicious IP library and fingerprint database maintained by Alibaba Group, which has years of experience in network security. · Threat intelligence such as information about data centers, Web crawler libraries, and harassing phone calls · Intelligence about bot attacks in the security industry.	-	8,490.57	707.55	12,735.85	1,061.32

Req	Protecti module	Feature	Default specification	Pricing			
				Chinese mainland		International	
				USD/ Year	USD/ Month	USD/ Year	USD/ Month
No	App Protection	Provides your app with enhanced protection against bot traffic through SDK integration. · You can integrate your app with the Anti-Bot SDK by following the integration guide. · You can establish secure connections between your app and the server, and ensure that only requests from legitimate devices are forwarded to the server. · You can access the fingerprint database maintained by Alibaba Group, which contains over 1 billion records of malicious devices	This feature supports only one app by default. If you add more apps for protection, you are charged additional fees. Anti-Bot Service charges USD XXX per month for each additional app. Note: The Android and iOS version of an app count as one app.	11,320.80	943.40	16,981.20	1,415.10

Req	Protection module	Feature	Default specification	Pricing			
				Chinese mainland		International	
				USD/ Year	USD/ Month	USD/ Year	USD/ Month
No	Customized algorithms	You can create a machine learning algorithm to analyze your business patterns and detect bot traffic accurately. You can customize your algorithm through deep learning and combine the algorithm with other protection modules to detect and handle bot traffic with more granularity. This helps improve protection capabilities.	-	188,679.24	15,723.27	283,018.86	23,584.91

Req	Protecti module	Feature	Default specification	Pricing			
				Chinese mainland		International	
				USD/ Year	USD/ Month	USD/ Year	USD/ Month
No	Managed Security Service	You can directly talk to our technical support professionals about anti-bot protection by joining an exclusive DingTalk group. · Basic service : Provides consultation and technical support to help you configure Anti-Bot instances, including configurations of domains and related products. · Value-added service: Helps you analyze traffic patterns of bot attacks and customize protection policies to minimize negative effects on your business. Note:	-	56,603.76	4,716.98	84,905.64	7,075.47

Recommended configurations

We recommend that you choose one of the following configurations based on your business type.

- Websites: Basic Defense + Bot Intelligence.
- Apps: Basic defense + App Protection
- Websites and apps: Basic defense + Bot Intelligence + App Protection

Note:

If your business requires a complex bot protection solution, we recommend that you use customized algorithms or Managed Security Service.

2 Activate Anti-Bot Service

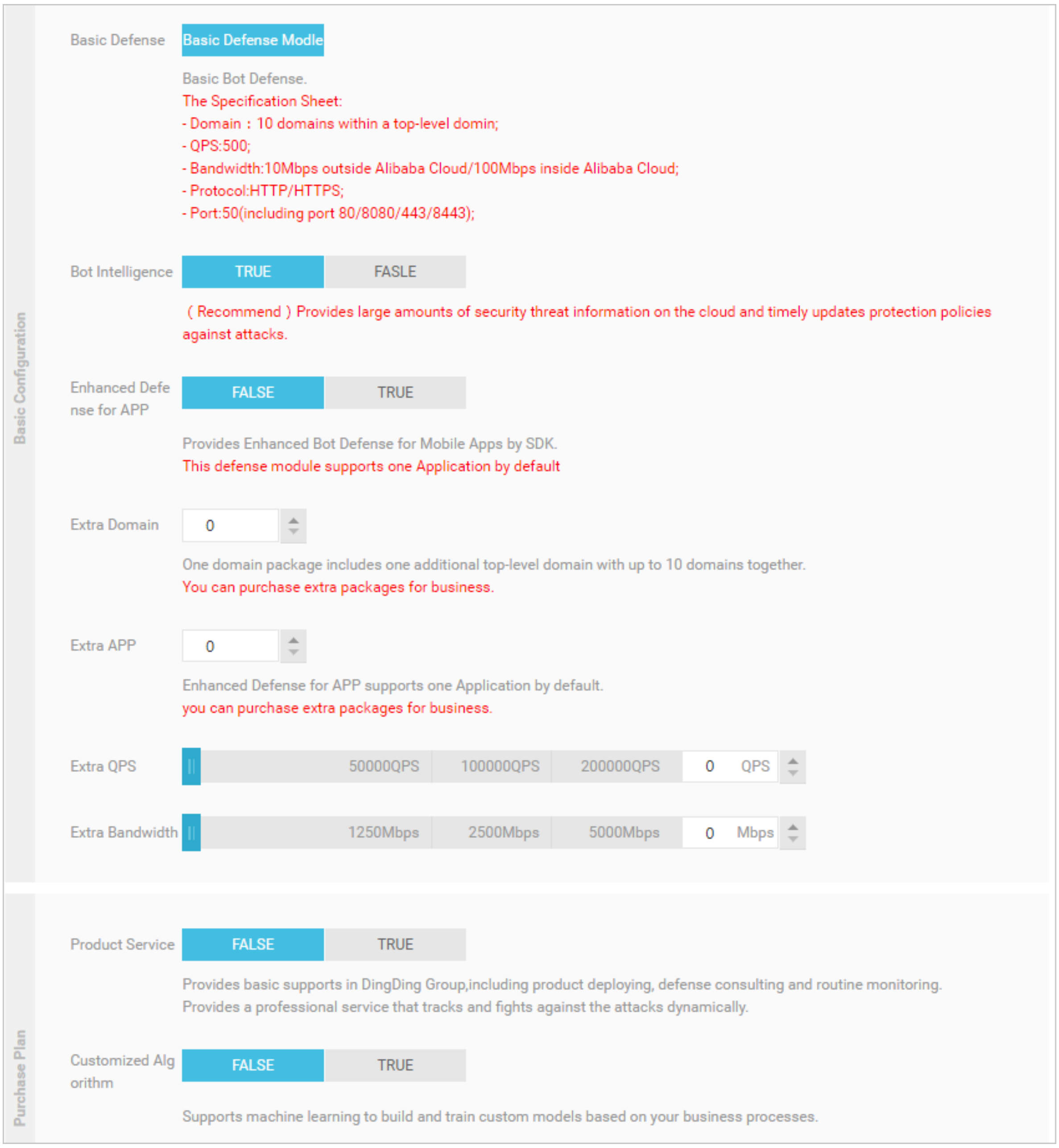
You can use Anti-Bot Service to defend against bot attacks.

Procedure

1. Go to the *Alibaba Cloud Anti-Bot Service buy page* and log on to your account.
2. Select the region.
3. Select the *Protection Module*.

   Note:

Specify the following fields based on your needs: *Extra Domain*, Extra App, *Extra QPS, and Extra Bandwidth*.



Basic Configuration

Basic Defense [✓ Basic Defense Modle]

Basic Bot Defense.
The Specification Sheet:
- Domain：10 domains within a top-level domin;
- QPS:500;
- Bandwidth:10Mbps outside Alibaba Cloud/100Mbps inside Alibaba Cloud;
- Protocol:HTTP/HTTPS;
- Port:50(including port 80/8080/443/8443);

Bot Intelligence [✓ TRUE] FASLE

（Recommend）Provides large amounts of security threat information on the cloud and timely updates protection policies against attacks.

Enhanced Defense for APP [✓ FALSE] TRUE

Provides Enhanced Bot Defense for Mobile Apps by SDK.
This defense module supports one Application by default

Extra Domain 0

One domain package includes one additional top-level domain with up to 10 domains together.
You can purchase extra packages for business.

Extra APP 0

Enhanced Defense for APP supports one Application by default.
you can purchase extra packages for business.

Extra QPS 50000QPS 100000QPS 200000QPS 0 QPS

Extra Bandwidth 1250Mbps 2500Mbps 5000Mbps 0 Mbps

Purchase Plan

Product Service [✓ FALSE] TRUE

Provides basic supports in DingDing Group,including product deploying, defense consulting and routine monitoring.
Provides a professional service that tracks and fights against the attacks dynamically.

Customized Algorithm [✓ FALSE] TRUE

Supports machine learning to build and train custom models based on your business processes.

Note:
You can upgrade your Anti-Bot instance specifications later.

4. Select the duration of the subscription.
5. Click Buy Now to make your payment.

Note:

Anti-Bot Service does not support full refunds within five days of purchase regardless of the reason.

3 Increase the limit on domains

Domains

By default, one Anti-Bot instance supports up to 10 domains. You can only add one TLD and up to 9 subdomains or wildcard domains for protection.

For example, you can add `abc . com` as the TLD and up to 9 subdomains or wildcard domains, such as `www . abc . com` , `\*. abc . com` , `mail . abc . com` , `user . pay . abc . com` , and `x . y . z . abc . com` . The total number of domains, including the `abc . com` TLD, cannot exceed 10.

Increase the limit on domains

If you want your Anti-Bot instance to protect two TLDs or their subdomains, you need to pay additional fees. Assume that you have added `abc . com` or its subdomains for protection, the following message appears when you try to add `xyz . com` or its subdomains to the same Anti-Bot instance:

```
You must upgrade your instance to enable protection for more TLDs or
 their subdomains.
```

In this case, you need to upgrade your Anti-Bot instance to increase the limit on domains.

You can click Upgrade in the Anti-Bot Service console to upgrade your Anti-Bot instance.

4 Increase the limits on the service bandwidth and request rate

By default, Anti-Bot Service supports up to 100 Mbit/s bandwidth for Alibaba Cloud-based services and up to 10 Mbit/s for non-Alibaba Cloud-based services. The default maximum service request rate is 500 QPS. You can increase the limits on service bandwidth and request rate based on your needs.

Service request rate

The service request rate is the number of concurrent requests per second that are sent to all domains protected by an Anti-Bot instance when no attack is in progress. Unit: QPS.

Each Anti-Bot instance supports a maximum request rate of 500 QPS by default.

Service bandwidth

The service bandwidth is the peak traffic that is sent to all domains protected by an Anti-Bot instance when no attack is in progress. Unit: Mbit/s.

> Note:
> The traffic that flows through Anti-Bot Service is measured independently of the bandwidth limits of other Alibaba Cloud services, such as CDN, SLB, and ECS.

By default, each Anti-Bot instance supports a maximum bandwidth of 100 Mbit/s for Alibaba Cloud-based services and a maximum bandwidth of 10 Mbit/s for non-Alibaba Cloud-based services. A higher bandwidth limit is provided for services that are deployed on Alibaba Cloud servers, such as ECS and SLB instances.

Increase the limits on service bandwidth and request rate

If your service expects to receive high-bandwidth traffic or a large number of concurrent requests, you need to purchase additional bandwidth to handle the traffic or requests.

For example, assume that your service is not deployed on Alibaba Cloud services , and your current service bandwidth is 30 Mbit/s and the request rate is 1,500 QPS. For non-Alibaba Cloud-based services, each Anti-Bot instance supports a maximum bandwidth of 10 Mbit/s and a maximum request rate of 500 QPS. To prevent service interruptions, you need to pay additional fees for the exceeding 20 Mbit/s of bandwidth and 1,000 QPS request rate.

To meet your growing needs, you can upgrade your Anti-Bot instance for higher specifications.

> Note:
> You can also increase the limits on service bandwidth and request rate when you buy the Anti-Bot instance.

What if the maximum service bandwidth or request rate is exceeded?

If your service bandwidth or request rate exceeds the limit of your Anti-Bot instance, you will receive an alert and traffic forwarding may be affected.

When the maximum service bandwidth or request rate is exceeded, bandwidth throttling and random packet losses are likely to occur, which may lead to issues such as service interruptions, slowdowns, and delays.

If you are experiencing these issues, we recommend that you increase the limits on service bandwidth and request rate as soon as possible.

Do I need to increase the QPS limit?

To see if you need to increase the QPS limit, you can estimate the combined peak request rate of your services that are protected by Anti-Bot Service. The maximum request rate supported by your Anti-Bot instance must be greater than the combined peak request rate of your services that are protected by the Anti-Bot instance.

Example

Assume that you are using an Anti-Bot instance to protect three websites, and the peak request rate of each website is no greater than 500 QPS. The combined peak request rate of the three websites is no greater than 1,500 QPS. In this case, you only need to purchase an Anti-Bot instance that provides a maximum service request rate of 1,500 QPS or above.

Do I need to increase the bandwidth limit?

To see if you need to buy more bandwidth, you can estimate the combined peak bandwidth of the inbound and outbound traffic that flows through the services protected by Anti-Bot Service. The maximum service bandwidth supported by your Anti-Bot instance must be greater than the combined peak bandwidth of the inbound and outbound traffic that flows through the services protected by the Anti-Bot instance.

Note:
Generally, the bandwidth of outbound traffic is greater than that of inbound traffic.

You can estimate the actual bandwidth by viewing the traffic statistics in the ECS console or other monitoring tools on your origin server.

Note:
The traffic described here refers to the normal traffic that flows through your services.

To use Anti-Bot Service to protect your services, you need to direct all incoming traffic to Anti-Bot Service. When your services are running normally and no attack is in progress, Anti-Bot Service forwards all normal traffic back to the origin server. When your services are experiencing attacks, Anti-Bot Service filters out malicious traffic, and only forwards normal traffic back to the origin server. Therefore, the inbound and outbound traffic in the ECS console is normal traffic. If your services are deployed on multiple origin servers, you need to calculate the combined bandwidth of inbound and outbound traffic that flows through all origin servers.

Example

Assume that you are using an Anti-Bot instance to protect three websites, and the peak bandwidth of outbound traffic from each website is no greater than 10 Mbit/s. The combined peak bandwidth of outbound traffic from all three websites is no greater than 30 Mbit/s. In this case, you only need to purchase an Anti-Bot instance that provides a maximum service bandwidth of 30 Mbit/s or above.

5 Support for non-standard ports

In addition to ports 80/8080 (HTTP) and 443/8443 (HTTPS), Anti-Bot Service also provides protection for specific non-standard ports.

Each Anti-Bot instance supports up to 50 ports, including standard ports 80, 8080, 443, and 8443.

Note:

Anti-Bot Service only provides protection for supported ports. Requests from unsupported ports are not accepted or forwarded. For example, when an Anti-Bot instance receives a request from port 4444, the request is discarded.

Supported HTTP ports

Anti-Bot Service supports the following HTTP ports:

80, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9999, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702

Supported HTTPS ports

Anti-Bot Service supports the following HTTPS ports:

443, 4443, 5443, 6443, 7443, 8443, 9443, 8553, 8663, 9553, 9663, 18980