

# **Alibaba Cloud Anti-DDoS Basic Anti-DDoS Premium Service**

Issue: 20190213

## 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.	 <b>Danger:</b> 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.	 <b>Warning:</b> 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.	 <b>Notice:</b> 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.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the <code>cd /d C:/windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
<b>1 Product Introduction.....</b>	<b>1</b>
1.1 What is Anti-DDoS Premium.....	1
1.2 Features.....	1
1.3 Scenarios.....	2
<b>2 Pricing.....</b>	<b>6</b>
2.1 Billing method.....	6
2.2 Global advanced mitigation.....	11
2.3 Mainland China Acceleration.....	14
<b>3 Quick Start.....</b>	<b>17</b>
3.1 Enable Anti-DDoS Premium.....	17
3.2 Add website to Anti-DDoS Premium for protection.....	17
3.3 Add a non-website business to Anti-DDoS Premium for protection.....	22
3.4 Configure Anti-DDoS Premium MCA.....	25
3.5 Import or export provisioning settings.....	29



# 1 Product Introduction

---

## 1.1 What is Anti-DDoS Premium

For users who have business servers deployed outside the mainland China, Alibaba Cloud provides the Anti-DDoS Premium service to mitigate DDoS attacks.

By enabling Anti-DDoS Premium for your server that deployed outside the mainland China, all attack traffic against your server is pulled to your Anti-DDoS Premium's dedicated IP. Then, the Anti-DDoS Premium service filters attack traffic that diverted to global distributed scrubbing centers by using Anycast technology, and forward clean traffic back to the origin server. This mostly improves the stability of your business.

## 1.2 Features

Anti-DDoS Premium defends against the following types of DDoS attacks for you.

Functionality	Description
Malformed packets filtering	Defends against Frag flood, Smurf attack, stream flood and Land attacks, and filters malformed IP packet, TCP packet and UDP packet.
Transport layer DDoS protection	Defends against SYN flood, ACK flood, UDP flood, ICMP flood, and RST flood attacks.
Web application layer DDoS protection	Defends against HTTP Get flood, HTTP Post flood, and connection flood attacks by using filtering rules based on HTTP characteristics, URI and Host.

### Core features

Anti-DDoS Premium has the following features:

- Global DDoS Mitigation

Anti-DDoS Premium integrates capacities of all Alibaba Cloud scrubbing centers over the world as protection resources by using Anycast technology. With

distributed technology, Anti-DDoS Premium automatically diverts DDoS attack traffic to the nearest scrubbing center to the attacking source for mitigation.

- **Unlimited Protection**

Anti-DDoS Premium provides unlimited protection with full capacity to each user by comprehensively utilizing global near-source mitigation abilities.

In 2018, the total protection capacity of Alibaba Cloud International Anti-DDoS scrubbing centers increases to over 2 Tbps. Anti-DDoS Premium aims to defend against every single DDoS attack for you.



**Notice:**

Alibaba Cloud keeps rights of actions when attacks against your business impact the infrastructure of Alibaba Cloud International Anti-DDoS scrubbing centers. Once the actions are triggered on your Anti-DDoS Premium instance, your protected business may be affected. The action includes but not limited to “black hole” of the IP addresses being attacked, or alteration to the routing of the traffic destined to the IP addresses being attacked.

- **Dedicated IP Resource**

Anti-DDoS Premium provides a dedicated Anycast IP for each user. Each IP is isolated to avoid any impact by DDoS attacks against other users. This provides you a safer DDoS mitigation service.

- **Security Report**

Anti-DDoS Premium provides detail traffic report and attack protection report in real time for you to have a clear view on the security of your business.

## 1.3 Scenarios

The Internet is interconnected by local network operators to achieve global access. However, due to different policies of network operators in different regions, the actual network access and communication is different. Therefore, you have to use an appropriate DDoS protection solutions according to your business scenarios.



**Note:**

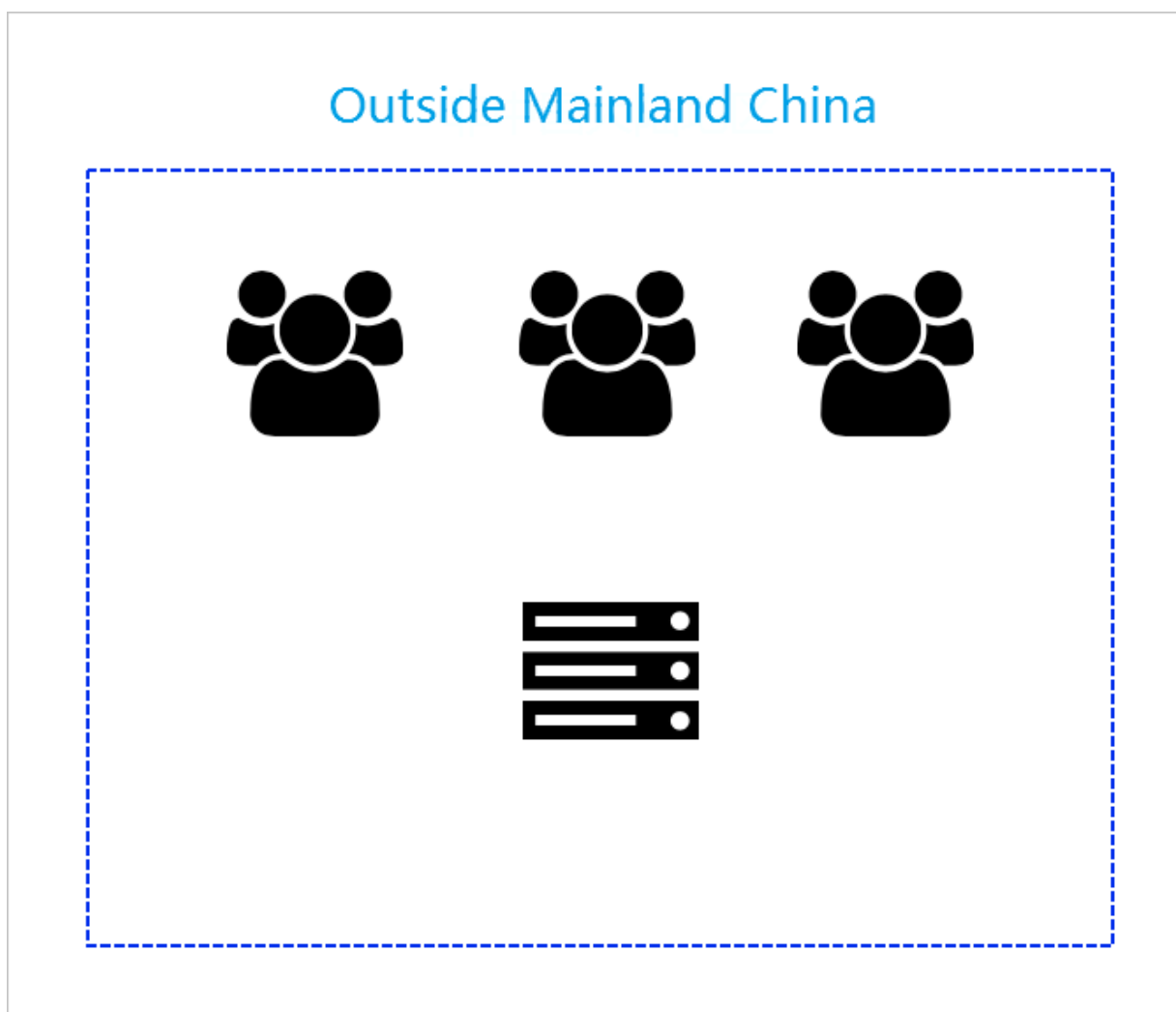
Because of the current routing and interconnection strategies of network operators, if only the Anti-DDoS Premium service is enabled, users in mainland China have to

access Anti-DDoS Premium resources deployed outside the mainland China, and the quality of the network link is affected.

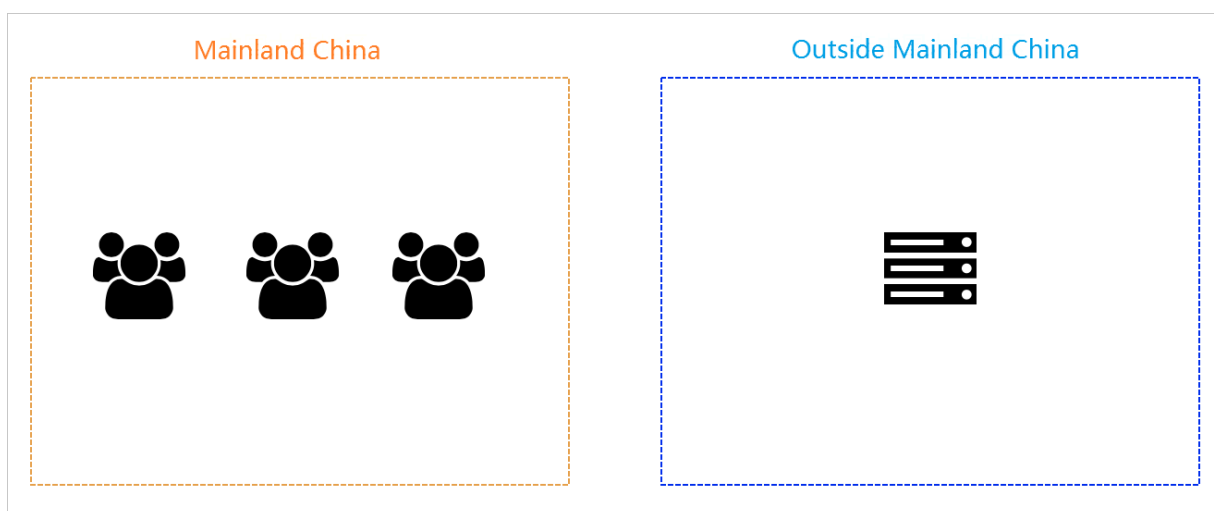
The average network delay time reaches 300 ms, and the network link is affected by international link congestion resulting in intermittent packet loss. Therefore, we strongly recommend that you deploy servers in mainland China to serve users in mainland China, use Anti-DDoS Pro service to mitigate DDoS attacks, and complete website registration and other compliance procedures to comply with relevant Chinese laws and regulations.

For servers that are deployed outside mainland China, see the following three scenarios:

Scenario 1: The Business Server is deployed in non-mainland China and mainly serves users from non-Mainland China



Purchase Anti-DDoS Premium, and add your business to the Anti-DDoS Premium instance for DDoS protection according to [Enable Anti-DDoS Premium](#).

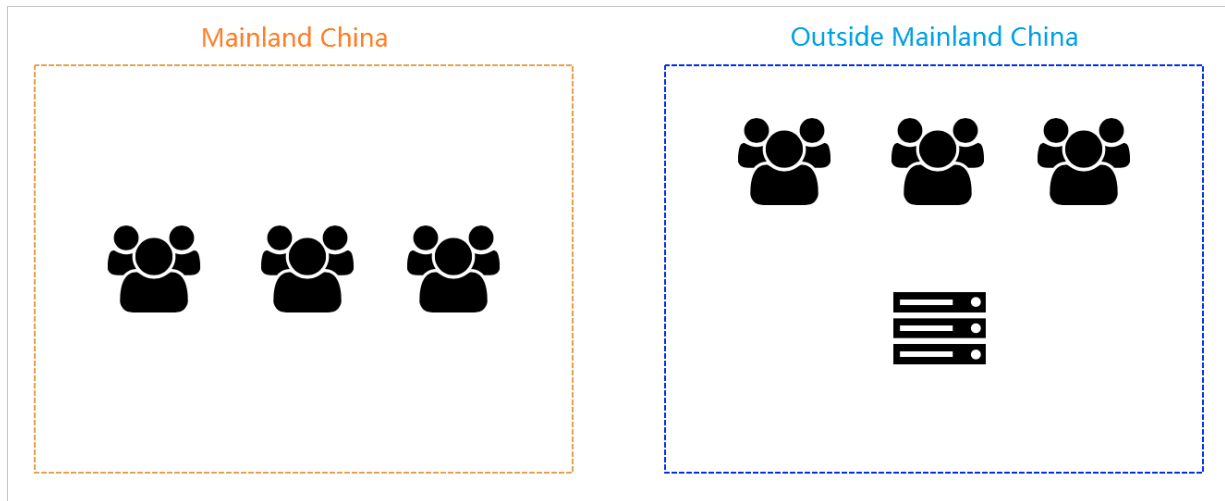
**Scenario 2: Servers deployed outside mainland China, while serving users in mainland China****Solutions:****· Solution A**

If your business has high requirements on network quality (for example, gaming servers), we recommend that you migrate your servers to the mainland China region that your major users located in, and purchase [the Anti-DDoS Pro service](#) to mitigate DDoS attacks.

**· Solution B**

If your business servers are not planned to be migrated to mainland China, contact our sales or submit a ticket to purchase the Mainland China Acceleration (MCA) plan of Anti-DDoS Premium. Then, our technical support helps you to deploy the Anti-DDoS Smart Switch solution to guarantee smooth access for users in mainland China by utilizing the acceleration lines when no DDoS attack happens. For more information about MCA, view [Configure Anti-DDoS Premium MCA](#).

**Scenario 3: Servers deployed outside mainland China, while serving users both in and outside mainland China**



**Solutions:**

- **Solution A**

We recommend that you deploy business servers separately for the two regions, using servers deployed in mainland China to serve users in mainland China and using servers deployed outside mainland China to serve users outside mainland China. Meanwhile, purchase [the Anti-DDoS Pro service](#) and the Anti-DDoS Premium service for businesses in and outside mainland China to mitigate DDoS attacks.

- **Solution B**

If you do not plan to deploy business servers in mainland China, contact our sales or submit a ticket to purchase the Mainland China Acceleration (MCA) plan of Anti-DDoS Premium. Then, our technical support helps you to deploy the Anti-DDoS Smart Switch solution to guarantee smooth access for users in mainland China by utilizing the acceleration lines when no DDoS attack happens. For more information about MCA, view [Configure Anti-DDoS Premium MCA](#).

## 2 Pricing

---

### 2.1 Billing method

Anti-DDoS Premium offers Insurance Plan and Unlimited Plan.

#### Advanced mitigation feature of Anti-DDoS Premium

Integrating all mitigation capacities of Alibaba Cloud Anti-DDoS scrubbing centers around the world, Anti-DDoS Premium defends against all DDoS attacks to secure your business.

In most cases, the chances of being attacked decrease significantly after you have successfully defended against DDoS attacks using the Anti-DDoS service. Typically, attackers launch DDoS attacks to cause financial losses to your business. Due to the cost of launching attacks, if the attackers fail to achieve this purpose, they will stop launching DDoS attack. Therefore, the advanced mitigation of Anti-DDoS Premium provides unlimited mitigation capacities and can integrate all mitigation capacities of Alibaba Cloud Anti-DDoS scrubbing centers around the world to secure your business.



#### Notice:

If the attacks against your business impact the infrastructure of Alibaba Cloud Anti-DDoS scrubbing centers, Alibaba Cloud has the right to control the traffic. Once the traffic control is triggered on your Anti-DDoS Premium instance, your protected business may be affected. The traffic control measures include but are not limited to black hole routing and limitations to the access traffic.

#### Plans of Anti-DDoS Premium

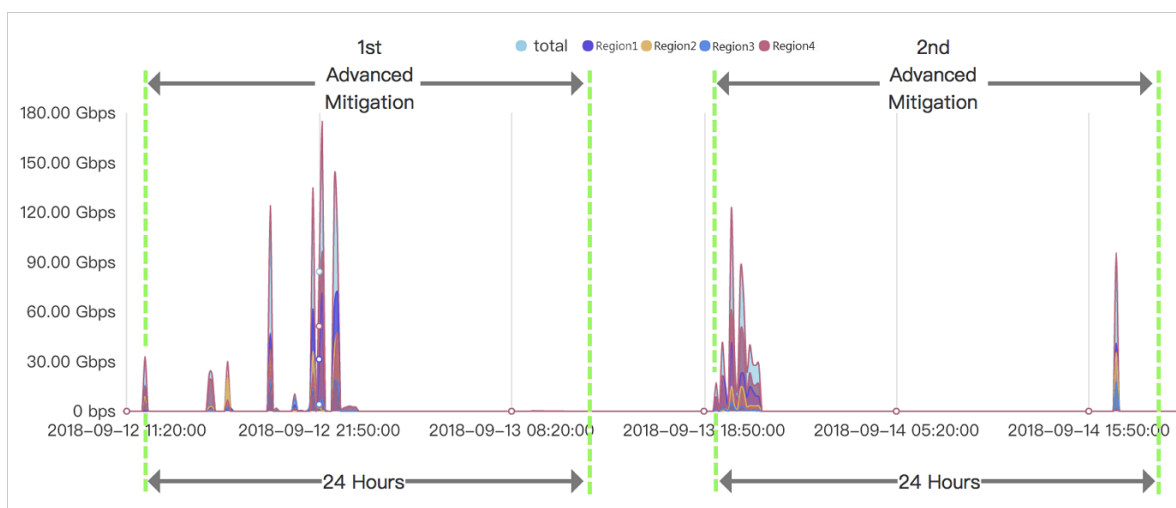
- Insurance Plan

Each month, Anti-DDoS Premium Insurance Plan offers two free advanced mitigations by default, featuring unlimited mitigation capabilities. This protects your businesses against DDoS attacks with full capacity within 24 hours after an attack has been detected, and consumes one advanced mitigation. The number of advanced mitigations is reset to two at the beginning of every month during the service period.

**Note:**

To purchase more advanced mitigations, see [Global advanced mitigation](#).

For example, a protected IP suffers DDoS attacks at 11:20:00 (UTC+8), September 12, and an advanced mitigation is triggered. Within 24 hours, Anti-DDoS Premium provides unlimited mitigation capacities for this IP. The protected IP suffers another DDoS attack at 18:50:00 (UTC+8), September 13, and an advanced mitigation is triggered again. 24 hours later, the advanced mitigation stops and the two advanced mitigation of the Anti-DDoS Premium Insurance Plan instance in September are exhausted. The number of advanced mitigations is automatically reset to two at the beginning of the following month, October 1.



Insurance Plan is a basic solution of Anti-DDoS Premium and applies to users who are less vulnerable to attacks.

**Note:**

Only when the DDoS attack against your business exceeds a specific threshold, namely the basic mitigation threshold, will the advanced mitigation of Anti-DDoS Premium be enabled.

- **Unlimited Plan**

Anti-DDoS Premium Unlimited Plan provides unlimited advanced mitigation capabilities for your business. After you purchase the Unlimited Plan instances, Anti-DDoS Premium provides unlimited mitigation to protect your business against all DDoS attacks.

## Pricing details of Anti-DDoS Premium

The pricing details of Anti-DDoS Premium instances are shown in the following table.

Plan	Business bandwidth	Advanced mitigation	Price (USD/month)
Insurance	100 Mbps	2/month	2,630
Unlimited		Unlimited	11,560
Insurance	150 Mbps	2/month	3,420
Unlimited		Unlimited	12,610
Insurance	200 Mbps	2/month	4,210
Unlimited		Unlimited	13,660
Insurance	250 Mbps	2/month	5,000
Unlimited		Unlimited	14,720
Insurance	300 Mbps	2/month	5,570
Unlimited		Unlimited	15,770

**Note:**

If you need a higher Clean bandwidth, contact Alibaba Cloud technical support.

**Note:**

Clean bandwidth refers to the maximum normal clean bandwidth that can be processed by Anti-DDoS Premium instances when your business is not under attack. Make sure that the Clean bandwidth of the instance is greater than the peak value of the inbound or outbound traffic of all services connected to the Anti-DDoS Premium instances. For more information about the Clean bandwidth, see [How to select a Clean bandwidth specification](#).



If the actual traffic volume exceeds the maximum Clean bandwidth, your business may be subject to traffic restrictions or random packet losses, and your normal business may be unavailable, slowed, or delayed for a certain period of time.

Anti-DDoS Premium instances provide the following business specifications by default:

**Note:**



If you need to expand the default business specifications based on actual needs, you can upgrade the instance or expand the corresponding specifications when purchasing the instance.

Business specifications	Descriptions	Default values	Price (USD/month)
Number of protected ports	The number of TCP/UDP ports that can be protected by the instance.	5	Every 5 ports: 150 USD/month
Number of protected domain names	The number of HTTP/HTTPS domain names that can be protected by the instance.	10  <b>Note:</b> Contains only one top-level domain and the subdomains or wildcard domains of this top-level domain.	Every 10 domain names: 150 USD/month  <b>Note:</b> Every 10 protected domain names contain only one top-level domain and the subdomains or wildcard domains of this top-level domain.
Clean QPS	The maximum concurrent HTTP/HTTPS requests per second supported when the system is not under attack.	<ul style="list-style-type: none"> <li>Insurance Plan: 500 QPS</li> <li>Unlimited Plan: 1,000 QPS</li> </ul>	Every 100 QPS: 150 USD/month

## More information

### How to select a Clean bandwidth specification

You can select an appropriate Clean bandwidth specification based on the daily inbound and outbound traffic peaks of all businesses that have or will be connected to the Anti-DDoS Premium instance. Make sure that the Clean bandwidth of the

instance is greater than the peak value of the inbound and outbound traffic of all businesses.



**Note:**

Typically, the outbound traffic is greater than the inbound traffic.

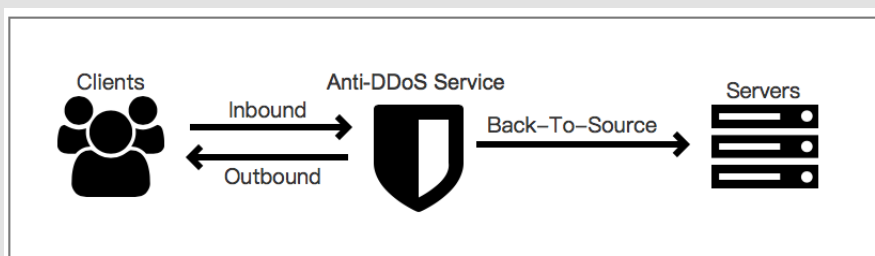
You can evaluate your business traffic by using ECS traffic statistics or other monitoring tools on your origin server.



**Note:**

The traffic here indicates the normal business traffic.

For example, you connect all access traffic of your external business to an Anti-DDoS Premium instance to secure your business. Anti-DDoS Premium will reroute the normal access traffic to the origin server when the business is normally accessed and without being attacked. When the business is attacked, Anti-DDoS Premium filters and blocks the malicious traffic, and only reroutes the normal traffic to the origin server. Therefore, the inbound and outbound traffic you view in the ECS console is normal traffic. If your business is deployed on multiple origin servers, you need to calculate the total traffic of all origin servers.



Assume that you need to connect the businesses of three websites to an Anti-DDoS Premium instance, the normal outbound traffic peak for each business does not exceed 50 Mbps, and the total business traffic does not exceed 150 Mbps. In this case, you only need to ensure that the maximum bandwidth of the purchased instance is greater than 150 Mbps.

### Domain name specifications

Anti-DDoS Premium instances support adding 10 domain names for protection by default, including one top-level domain and the subdomains or wildcard domains of the top-level domain.

Taking `abc.com` for example, you can add the top-level domain itself and a maximum of nine subdomains, such as `www.abc.com`, `*.abc.com`, `mail.abc.com`, `user.pay.abc.com`, and `x.y.z.abc.com`. Each domain name that you have added, including the top-level domain `abc.com` counts in the quota for protected domain names.

If you want to add two different top-level domains or their subdomains to connect to the Anti-DDoS Premium instance, you need to expand the quota for protected domain names. Assume that you have added `abc.com` or its subdomain for protection, when you try to add `xyz.com` (another top-level domain) or its subdomain, you will receive the following message:

The quota of top-level domains has been exceeded. Upgrade the instance to expand the quota for protected domain names.

In this case, you need to upgrade the Anti-DDoS Premium instance to expand the quota for domain name mitigation.



**Note:**

Adding 10 protected domain names each time allows you to have one more top-level domain in the quota for domain name mitigation. For example, you must set the number of protected domain names to 20 to protect the two top-level domains, `abc.com` and `xyz.com` in an Anti-DDoS Premium instance.

## 2.2 Global advanced mitigation

If the two free advanced mitigations for the month of an Anti-DDoS Premium Insurance Plan instance has been used up, you can purchase additional global advanced mitigations to achieve more unlimited mitigation capabilities.

Each month, Anti-DDoS Premium Insurance Plan provides two free advanced mitigations by default, featuring unlimited mitigation capabilities. This protects your businesses against DDoS attacks within 24 hours after an attack has been detected, and consumes one advanced mitigation.

If the business suffers from frequent large-traffic attacks, the two free advanced mitigations of Anti-DDoS Premium Insurance Plan may be not enough to guarantee the service availability. In this case, you can purchase global advanced mitigations to obtain more advanced mitigations for the Anti-DDoS Premium instances in your account.

## Notes

If the two free advanced mitigations for the month have been used up and your business still suffers from large-traffic attacks, with the traffic volume exceeding the basic mitigation threshold, the additional global advanced mitigations you have purchased will be consumed to provide unlimited mitigation capacities.

You do not need to bind the global advanced mitigation to a specific instance. You can use the global advanced mitigation for all Anti-DDoS Premium Insurance Plan instances that meet the usage requirements.

## Usage requirements

- The Insurance Plan instance is valid.
- The advanced mitigation feature of the account is not frozen.



### Note:

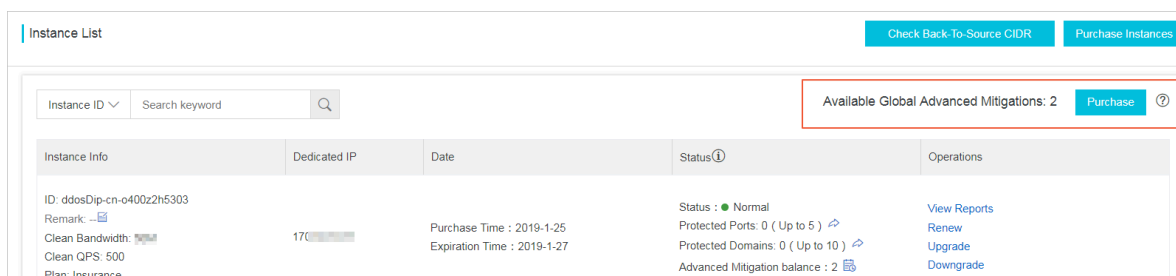
When the number of advanced mitigations, including the number of global advanced mitigation, consumed by all instances in your account in the current month exceeds 10, the advanced mitigation feature will be automatically frozen. You must wait until the next calendar month to use this feature.

If your business is subject to frequent large-traffic attacks, we recommend that you purchase Unlimited Plan instances to protect your business.

## Purchase global advanced mitigation

After you purchase an Anti-DDoS Premium instance, you can purchase additional global advanced mitigations in the Anti-DDoS Premium console at any time.

1. Log on to the [Anti-DDoS Premium console](#).
2. On the Instance List page, click **Purchase**.



3. On the Global Advanced Mitigation purchase page, select the quantity, and click **Buy Now**.

**Note:**

Make sure that the Product is selected as Anti-DDoS Premium.

**Pricing**

Pricing parameters	Description
Payment type	Subscription
Duration	3 Years
Unit price	1,580 USD

**Notice:**

Refund is not supported for the global advanced mitigation.

**More information****Global advanced mitigation and advanced mitigation of Anti-DDoS Premium instance**

Type	Scope	Period of Validity	Quantity
Advanced mitigation of Unlimited Plan	Instance	Based on instance validity period	Unlimited
Advanced mitigation of Insurance Plan	Instance	1 month <div> <b>Note:</b>            Advanced mitigation that is unconsumed in the current month will be cleared at the beginning of next month.         </div>	Twice each month
Global advanced mitigation	Account	3 years	Purchase separately

## 2.3 Mainland China Acceleration

If your business servers are deployed in regions outside mainland China, you can purchase Mainland China Acceleration (MCA) for your Anti-DDoS Premium instances to accelerate the access to your business for users in mainland China.

MCA provides users in mainland China with low-latency access to the businesses deployed in regions outside mainland China. This significantly improves the response time when the business is not under attack.



### Note:

MCA cannot be configured independently. MCA instances do not have any mitigation capabilities and must be used with Anti-DDoS Premium Insurance Plan or Unlimited Plan instances.

For more information about the applicable scenarios, see [Scenarios](#).

After purchasing MCA instances, you can use these instances with Anti-DDoS Premium Insurance Plan instances or Unlimited Plan instances to increase the access speed when your business is not under an attack, as shown in [Configure Anti-DDoS Premium MCA](#).

### Pricing

The pricing details of Anti-DDoS Premium MCA are shown in the following table.

Business bandwidth	Price (USD/month)
10 Mbps	1,548
20 Mbps	3,096
30 Mbps	4,643
40 Mbps	6,191
50 Mbps	7,739
60 Mbps	9,287
70 Mbps	10,834
80 Mbps	12,382
90 Mbps	13,930
100 Mbps	15,478

**Note:**

Business bandwidth refers to the maximum normal business bandwidth that can be processed by Anti-DDoS Premium MCA instances when your business is not under attack. Make sure that the business bandwidth of the instance is greater than the peak value of the inbound and outbound traffic of all services connected to the MCA instance.


If the actual traffic volume exceeds the maximum business bandwidth, your business may be subject to traffic restrictions or random packet losses, and your normal business may be unavailable, slowed, or delayed for a certain period of time.

Anti-DDoS Premium MCA instances provide the following business specifications by default:

**Note:**

The specification of the MCA instance must be consistent with the corresponding instance business specifications of Anti-DDoS Premium Insurance Plan or Unlimited Plan.

Business specifications	Descriptions	Default values
Number of protected ports	The number of TCP/UDP ports that can be protected by the instance.	The default number is 5. The number of ports must be the same as that of ports to be protected of the Anti-DDoS Premium Insurance Plan instances or the Unlimited Plan instances.

Business specifications	Descriptions	Default values
Number of protected domains	The number of HTTP/HTTPS domains that can be protected by the instance.	<p>The default number is 10. The number of protected domains must be the same as that of domains to be protected of the Anti-DDoS Premium Insurance Plan instances or the Unlimited Plan instances.</p> <div>  <b>Note:</b>            Every 10 protected domain names contain only one top-level domain and the subdomains or wildcard domains of this top-level domain.         </div>
Business QPS	The maximum concurrent HTTP/HTTPS requests per second supported when the system is not under attack.	500 QPS



## 3 Quick Start

---

### 3.1 Enable Anti-DDoS Premium

You can add configurations for your domains (Layer 7) and ports (Layer 4) in Anti-DDoS Premium for DDoS protection.

After purchasing an Anti-DDoS Premium instance, you can add configurations in the console to add forwarding rules of domains and ports to specify the origin servers where clean traffic is forwarded to after DDoS attack mitigation.

After completing the configurations in the console, you change the DNS resolution record for domain or change your business application's IP to the CNAME or IP assigned by your Anti-DDoS Premium instance, to switch all traffic to the Anti-DDoS Premium's dedicated IP. Then, all traffic firstly passes through global scrubbing centers and the clean traffic is forwarded back to the origin servers. In this situation, the unlimited full-capacity protection has been enabled for your business.

### 3.2 Add website to Anti-DDoS Premium for protection

After purchasing an Anti-DDoS Premium instance, you can add your website domain to the instance for DDoS protection.

#### Context



#### Note:

If you want to add a non-website business, such as client game, mobile game or APP to Anti-DDoS Premium, see [Add non-website business to Anti-DDoS Premium for protection](#).

#### Procedure

1. Log on to the [Anti-DDoS Premium Service console](#).
2. Go to Provisioning > Website page, and click Add Website.
3. On the Website configuration page, enter information for the website to be protected, and then click Add Website.

Website Configuration

Change DNS Records

\* Website domain:

Support Top Level Domain: e.g. "test.com" and Second Level Domain: e.g www.test.com

\* Protocol: ☒ HTTP ☒ HTTPS ☐ Websocket ☐ Websockets

\* Origin server: ☒ IP ☐ Domain

Origin server ports: HTTP 80 HTTPS 443

Service Ports: HTTP 80 HTTPS 443



Choose Dedicated IP:

☐ Instance ( Up to 8 IP for each domain, you have selected 1 IP)

<input checked="" type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

Add website

Parameter	Description	Note
Website domain	Domain of the website to be protected.	Top-level and second-level domains are supported. Additionally, wild-card domains are also supported, and the system automatically matches all second-level domain names of the wild-card domain.

Parameter	Description	Note
Protocol	Protocols supported by the website.	If your website supports https or websockets encryption authentication, you can check the HTTPS or Websockets protocol and upload the corresponding certificate and private key after adding the web site configuration.
Origin server	Origin server of the website.	<p>After adding the website to the Anti-DDoS Premium instance, the system forwards clean traffic back to the origin server that you specified.</p> <ul style="list-style-type: none"> <li>· (Recommended) Select IP, and input the origin server IP (For example, you can input a public IP of an ECS or SLB instance). Then, the Anti-DDoS Premium instance forwards traffic to the origin server IP after the configuration.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  <b>Note:</b>  You can set up to 20 origin server IPs. If multiple origin IPs are set, the system polls these IPs by IP-Hash to realize load balancing. </div> <ul style="list-style-type: none"> <li>· Select Domain, and input the origin server domain (For example, you can input a CNAME of an OSS bucket). Then, the Anti-DDoS Premium instance forwards traffic to the origin server domain after the configuration.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;">  <b>Note:</b>  The origin server domain must not be the same as the website domain to be protected. </div>

Parameter	Description	Note
Origin server ports	Ports of the website origin server. The Anti-DDoS Premium instance forwards clean traffic to the ports of the origin server after the configuration.	<ul style="list-style-type: none"><li>· By default, the HTTP and WebSocket protocols use Port 80,</li><li>· and the HTTPS and Websockets protocols use Port 433.</li></ul>
Choose Dedicated IP	Anti-DDoS Premium instance to protect the website.	For one website domain, you can set up to 8 Anti-DDoS Premium Dedicated IPs.

4. Go to the DNS service provider of your website,

and change the DNS record to the Dedicated IP of the Anti-DDoS Premium instance to enable Anti-DDoS service for your website.



**Note:**

Click Return to website list, if you want to test the forwarding rule of the Anti-DDoS Premium instance before switching business traffic to the Dedicated IP of Anti-DDoS Premium. After you verify that the forwarding rule works as expected, change the DNS record to switch business traffic to Anti-DDoS Premium.

- a) Log on to the [Anti-DDoS Premium Service console](#), go to the Instance List page, locate the Anti-DDoS Premium instance that protects the website, and record the Dedicated IP of the instance.
- b) Go to the DNS service provider of your website, and change the A record to point to the Dedicated IP.

The settings pages of the different DNS service providers are different. The following pictures are for reference only.

Add Record

Type:

A- IPV4 address

Host:

Enter ...

.com

ISP Line:

Default - Return to the default value when the query is not ...

\* Value:

Enter ...

\* TTL:

10 minute(s)

☐

Synchronize the Default Line

Cancel

OK

- c) After the DNS configuration is effective, all traffic to the website goes through the Anti-DDoS Premium instance for DDoS protection.

**Note:**

Generally, the DNS configuration takes about 10 minutes to be effective. We recommend that you change the DNS configurations during the low peak period.

5. Optional: Configure *origin server protection*.

**Note:**

The origin server protection can prevent your origin server against light-traffic HTTP flood and web attacks, but cannot defend against heavy traffic DDoS attacks. In addition, it does not prevent DDoS attacks directly targeting the origin server through traffic that bypasses Anti-DDoS Premium, which may even throw the origin IP address into the blackhole routing status.

### 3.3 Add a non-website business to Anti-DDoS Premium for protection

After purchasing an Anti-DDoS Premium instance, you can add your non-website business, such as client game, mobile game or APP, to the instance for DDoS protection.

#### Context



#### Notice:

Compared with website protection, non-website protection only provides layer 4 port protection, such as SYN, ACK, ICMP, and UDP floods. It cannot mitigate layer 7 attacks, such as HTTP floods, and web application attacks, such as SQL injection and XSS.



#### Note:


If you want to add a website domain to Anti-DDoS Premium, see [Add website to Anti-DDoS Premium for protection](#).


#### Procedure


1. Log on to the [Anti-DDoS Premium Service console](#).
2. Go to Provisioning > Non-Website page, select an Anti-DDoS Premium instance, and click Add Rule.

Provisioning

Website | **Non-Website** | Security Traffic Manager

Protocol 	Service Port	Origin Server Port	Forwarding Mod
--	--------------	--------------------	----------------

Add Multiple Rules 

Export 

3. On the Add Rule page, configure the following rule, and click Confirm.

## Add Rule

\* Protocol: ☒ TCP ☐ UDP

\* Service Port:

80



Range 1- 65535

\* Origin Server Port:

80



Range 1- 65535

Forwarding Mode: Round Robin

\* Origin Server IP

Separated with ",", cannot be repeated, up to 20.

Confirm

Parameter	Description	Note
Protocol	Protocols supported by the website.	The TCP and UDP protocols are supported.
Service Port	Port that used by the Anti-DDoS Premium instance to provide public service for the business. We recommend that you set the service port to the same port as the origin server port.	Any port from 1 to 65535 is supported.



Parameter	Description	Note
The port of the origin.	Origin server port that provides service for the business.	Any port from 1 to 65535 is supported.
Source station IP	IP address of the origin server.	You can set up to 20 origin server IPs. If multiple origin IPs are set, the system forwards traffic to these IPs by using the Round Robin mode to realize load balancing.

4. After you verify that the Anti-DDoS Premium forwarding rule works as expected, switch your business traffic to the Dedicated IP of the Anti-DDoS Premium instance.

**Note:**

Log on to the [Anti-DDoS Premium Service console](#). On the Instance Listpagepage, you can find the Dedicated IP of the Anti-DDoS Premium instance.

- If your business uses IP to access the origin server, change the business IP to the Dedicated IP of Anti-DDoS Premium.
- If your business also uses a domain to access the origin server (For example, you set the “aliyundemo.com” domain as the server address in the client program ), go the DNS service provider of the domain and change the A record to point to the Dedicated IP of Anti-DDoS Premium.

## 3.4 Configure Anti-DDoS Premium MCA

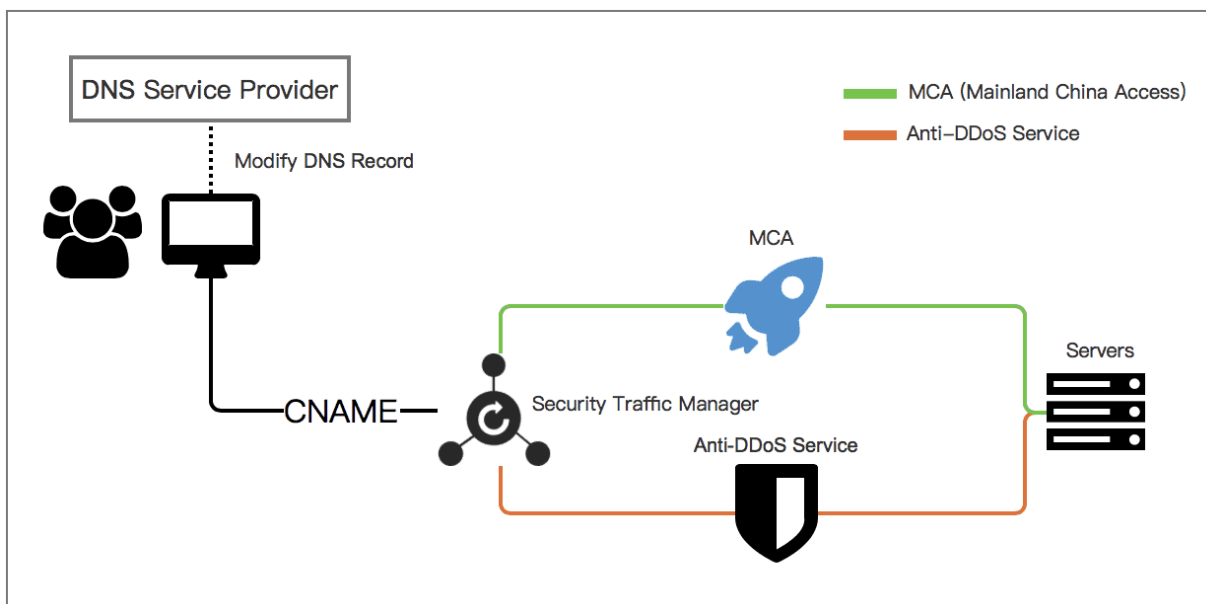
Anti-DDoS Premium mainland China acceleration (MCA) instance is used together with Anti-DDoS Premium Insurance/Unlimited instance, to realize quick access to your web service that deployed outside mainland China, especially for your Mainland China users.

### Context

After configuring MCA instance together with Anti-DDoS Premium Insurance/Unlimited instance, your web service can have the following features: Under no DDoS attack happens, Anti-DDoS Premium enables the MCA instance to accelerate web access to your service. When DDoS attack happens, Anti-DDoS Premium automatica

lly switches to the anti-DDoS instance (Insurance/Unlimited instance) to mitigate DDoS attacks for your web service.

For more information about recommended scenarios that require Anti-DDoS Premium MCA, refer to [Anti-DDoS Premium Use Cases](#).



You can configure an Anti-DDoS Premium MCA instance for domain (7-layer) or port (4-layer).

After purchasing Anti-DDoS Premium MCA and Insurance/Unlimited instances, complete provisioning of the instances for your website domain or service port on the Anti-DDoS Premium Management console, and then configure a Security Traffic Manager rule to enable the auto-switching between MCA and anti-DDoS instances. Finally, use the security service manager rule to forward non-attack traffic to the origin server of your web service.

## Procedure

1. Log on to the [Anti-DDoS Premium Service console](#).
2. Add your website or non-website service to both Anti-DDoS Premium Insurance/Unlimited and MCA instances.



### Note:

Only complete the provisioning configurations for your web service. Do not change the DNS resolution records of your domain at this step.

- For website domain: Refer to [Add website to Anti-DDoS Premium for protection](#) to complete the provisioning configuration. During the configuration, choose both dedicated IPs of your Insurance/Unlimited and MCA instances when you choose dedicated IPs of Anti-DDoS Premium.
- For service port: Refer to [Add non-website business to Anti-DDoS Premium for protection](#) to complete the provisioning configuration. Add forwarding rules under both Anti-DDoS Premium Insurance/Unlimited and MCA instances for your non-website service. Thus, you have to add a forwarding rule for your non-website service for each instance that is supposed to be used.

**Note:**

To configure Anti-DDoS Premium MCA for non-website service, your service must have a domain bound with the origin server instead of using the server IP directly. Otherwise, traffic cannot be automatically scheduled by Security Traffic Manager.

3. After the provisioning configuration completes, select the Provisioning > Security Traffic Manager page, click Add Rule.

Website   Non-Website   <u>Security Traffic Manager</u>			
Search Rule's name <input type="text"/>		<input type="button" value="Add Rule"/>	
Name	CNAME①	Nodes	Operations
jiasu1		Low Priority <input type="text"/>	<a href="#">Edit</a>
		High Priority <input type="text"/>	<a href="#">Delete</a>

4. In the Add Rule dialog box, configure rule and then click Confirm.

### Add Rule

Name :

Nodes :

High Priority :

Select

Select the Dedicated IP of MCA instance

Low Priority :

Select

Select the Dedicated IP of Insurance/Unlimited instance

Important: Please make sure the Web/Non-Web provisioning settings have been done before using Security Traffic Manager.

Confirm

Cancel

- The High Priority node: select the dedicated IP of the MCA instance.
- The Low Priority node: select the dedicated IP of the Insurance/Unlimited instance.

With this configuration, MCA instance is enabled with a high priority to accelerate web access when no DDoS attack happens, and the Security Traffic Manager automatically switch traffic to the anti-DDoS instance for DDoS attack mitigation when under DDoS attacks.

The system generates a CNAME record when the security traffic manager rule is added. After you change the DNS records of your service domain to resolve to the CNAME, the service traffic manager enables the traffic auto-scheduling for your service.

**Note:**

For those dedicated IPs that you select in the security traffic manager rule, make sure that you have completed the provisioning configurations for the dedicated IPs of the MCA and Insurance/Unlimited instances.

5. In the domain name resolution service provider, modify the DNS resolution record for that domain name.

After the DNS configuration is effective, all traffic to your web service is handled by the security traffic manager for auto-scheduling.



**Note:**

The traffic auto-scheduling is based on the CNAME record. Therefore, the DNS resolution of the service domain must use the CNAME record.

## 3.5 Import or export provisioning settings

If you have multiple provisioning settings of website domain or layer-4 forwarding, and you want to back up or migrate the service provisioning settings, you can quickly complete such operations through the import/export functionalities of the provisioning settings.

- The import/export of layer-4 forwarding rule settings supports the TXT format.
- The import/export of website domain provisioning settings supports the XML format with high compatibility.

The XML format has more parameter extensibility and readability than the TXT format. Additionally, the import/export also supports the provisioning setting that uses a domain as the origin site.

### Bulk import website domain name Configuration

1. Log on to the [Anti-DDoS Premium Service console](#).
2. Go to Provisioning > Website, click Import at the bottom of the domain setting list to add provisioning settings for multiple domains.
3. In the Add Multiple Rules dialog box, enter the domain setting parameters in the specified XML format.

Add Multiple Rules

View the Sample

```

<DomainList>
<DomainConfig>
<Domain>a.com</Domain>
<ProtocolConfig>
<ProtocolList>http,https</ProtocolList>
</ProtocolConfig>
<InstanceConfig>
<InstanceList>ddosDip-cn-v0h0v9a3x07</InstanceList>
</InstanceConfig>
<RealServerConfig>
<ServerType>0</ServerType>
<ServerList>1.2.3.4</ServerList>
</RealServerConfig>
</DomainConfig>
<DomainConfig>
<Domain>b.com</Domain>
<ProtocolConfig>
<ProtocolList>http,websocket,websockets</ProtocolList>
</ProtocolConfig>
<InstanceConfig>
<InstanceList>ddosDip-cn-v0h0v9a3x07,ddosDip-cn-0pp0u9slr01</InstanceList>
</InstanceConfig>
<RealServerConfig>
<ServerType>1</ServerType>
<ServerList>q840a82zf2j23afs,qfvip05al</ServerList>
</RealServerConfig>
</DomainConfig>
</DomainList>

```

Next
Cancel





#### Note:

You can copy and paste the content in the text box.

#### Parameter definition

The domain setting parameter content must start with `<DomainList>`, and end with `</DomainList>`. Between these two tags, there is the domain provisioning setting parameters to be imported. The parameters of each domain provisioning setting start with `<DomainConfig>` and end with `</DomainConfig>`. For details about corresponding parameters for the domain provisioning setting, see the following table.

Parameter	Description
<code>&lt;Domain&gt;a.com&lt;/Domain&gt;</code>	Domain name to be provisioned. You can enter only one domain in this parameter.
<code>&lt;ProtocolConfig&gt;</code> <code>&lt;ProtocolList&gt;http,https&lt;/ProtocolList&gt;</code> <code>&lt;/ProtocolConfig&gt;</code>	Protocol type. Separate multiple protocols with “,”. In this example, the protocols of the website domain are HTTP and HTTPS.
<code>&lt;InstanceConfig&gt;</code> <code>&lt;InstanceList&gt;ddoscoo-cn-4590lwcny001&lt;/InstanceList&gt;</code> <code>&lt;/InstanceConfig&gt;</code>	Anti-DDoS Premium instance ID.   <b>Note:</b> Since each Anti-DDoS Premium instance has one dedicated anycast IP, just specify the Anti-DDoS Premium instance ID. Separate multiple Anti-DDoS Premium instance IDs with “,”.
<code>&lt;RealServerConfig&gt;</code> <code>&lt;ServerType&gt;0&lt;/ServerType&gt;</code> <code>&lt;ServerList&gt;1.2.3.4&lt;/ServerList&gt;</code> <code>&lt;/RealServerConfig&gt;</code>	Origin site : <ul style="list-style-type: none"> <li>- <code>&lt;ServerType&gt;0&lt;/ServerType&gt;</code>: For origin IP</li> <li>- <code>&lt;ServerType&gt;1&lt;/ServerType&gt;</code>: For origin domain</li> </ul> In the <code>&lt;ServerList&gt;1.2.3.4&lt;/ServerList&gt;</code> tags, specify the origin site address. Separate multiple origin site addresses with “,”.   <b>Note:</b> For one domain, you cannot set both IP and domain addresses as the origin site.

#### • Sample

```

<DomainList>
  <DomainConfig>
    <Domain>a.com</Domain>
    <ProtocolConfig>
      <ProtocolList>http,https</ProtocolList>
    </ProtocolConfig>
    <InstanceConfig>
      <InstanceList>ddosDip-cn-v0h0v9a3x07</InstanceList>
    </InstanceConfig>
    <RealServerConfig>
      <ServerType>0</ServerType>
      <ServerList>1.2.3.4</ServerList>
    </RealServerConfig>
  </DomainConfig>

```

```

<DomainConfig>
<Domain>b.com</Domain>
<ProtocolConfig>
<ProtocolList>http,websocket,websockets</ProtocolList>
</ProtocolConfig>
<InstanceConfig>
<InstanceList>ddosDip-cn-v0h0v9a3x07,ddosDip-cn-0pp0u9slr01</
InstanceList>
</InstanceConfig>
<RealServerConfig>
<ServerType>1</ServerType>
<ServerList>q840a82zf2j23afs.gfvip05al.com</ServerList>
</RealServerConfig>
</DomainConfig>
</DomainList>

```



#### 4. Click Next.

After the XML content passes the validation, it is resolved to the domain provisioning settings to be imported.

#### 5. Select the domain provisioning settings to be added, and click OK to import these settings.

### Export provisioning settings of website domain

1. Go to Provisioning > Website, click Export at the bottom of the domain setting list.
2. Click OK to start an export task of current domain provisioning settings.
3. Click the Task List icon in the upper right corner of the Provisioning page, to view the progress of the export task.
4. After the task completes, click Download in the Task List dialog box, to download the domain provisioning settings to your local computer.

Task List			
Task	Status	Start Time	Operations
Conf Export: Webs...	 Preparing	01/07/2019 15:32:20	Delete
Conf Export: Webs...	 Done	12/27/2018 14:44:56	Delete Download



#### Note:

If the status of the tasks is Preparing, please be patient and wait for the export task to complete.



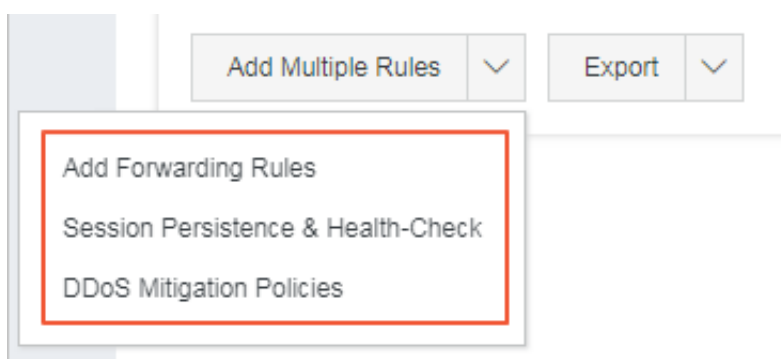
## Import forwarding rules

1. Go to Provisioning > Non-Website page.
2. Click Add Multiple Rules > Add Forwarding Rules at the bottom, to import multiple forwarding rules.



### Note:

You can also select Session Persistence/Health-Check or DDoS Mitigation Policies to import corresponding settings.



3. Refer to the samples to enter information about the settings.

- Forwarding rules

```
tcp 90 91 192.136.12.41
udp 22 13 12.14.1.23,10.23.4.12
```

From left to right, the above fields are Protocol, Forwarding Port, Origin site port, and Origin site IP.

- Session persistence/health-check settings

```
8081 tcp 4000 tcp 22 5 5 3 3
8080 tcp 4000 http 22 5 5 3 3 /search.php www.baidu.com
```

From left to right, the above fields are Forwarding Port, Forwarding Protocol, Session Persistence Timeout, Health Check Type, Ports, Response Timeout, Check Interval, Unhealthy Threshold, Healthy Threshold, URI (Required when the health check type is http), domain (Optional when the health check type is http). "Forwarding Port" must be a forwarding port that has policies configured.

- DDoS mitigation policies

```
8081 tcp 2000 50000 20000 100000 1 1500 on on
```

```
8080 udp 1000 50000 20000 100000 1 1500
```

From left to right, the above fields are Forwarding Port, Forwarding Protocol, New Connection Speed Limits for Source IP, Concurrent Connection Speed Limits for Source IP, New Connection Speed Limits for Destination IP, Concurrent Connection Speed Limits for Destination IP, Minimum Length of Packets, Maximum Length of Packets, and False Sources and Null Session Connections (This value is only effective for the TCP protocol. To enable the Null Session Connection setting, you must have the False Sources setting enabled).

4. Click Add to import the settings.

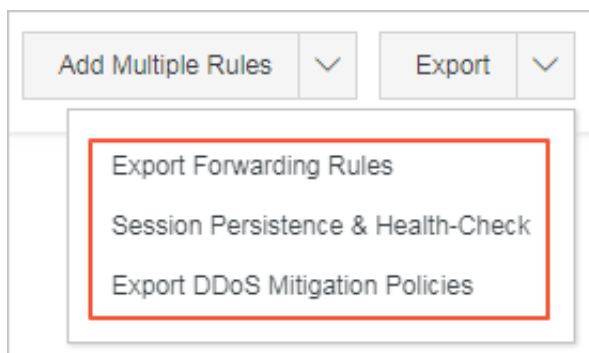
#### Export forwarding rules

1. Go to Provisioning > Non-Website page.
2. Click Export > Export Forwarding Rules at the bottom.



#### Note:

You can also select Session Persistence/Health-Check or DDoS Mitigation Policies to export corresponding settings.



3. In the prompt box, click OK, to start an export task for current forwarding rules.
4. Click the Task List icon in the upper right corner of the Provisioning page, to view the progress of the export task.
5. After the task completes, click Download in the Task List dialog box, to download the forwarding rule settings to your local computer.



#### Note:

If the status of the tasks is Preparing, please be patient and wait for the export task to complete.