

# DDoS Protection

## Anti-DDoS Premium Service

# Anti-DDoS Premium Service

## Product Introduction

### 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.

## Features

### Protection functionalities

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.

**Important:** 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.

### High Quality Reporting

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.

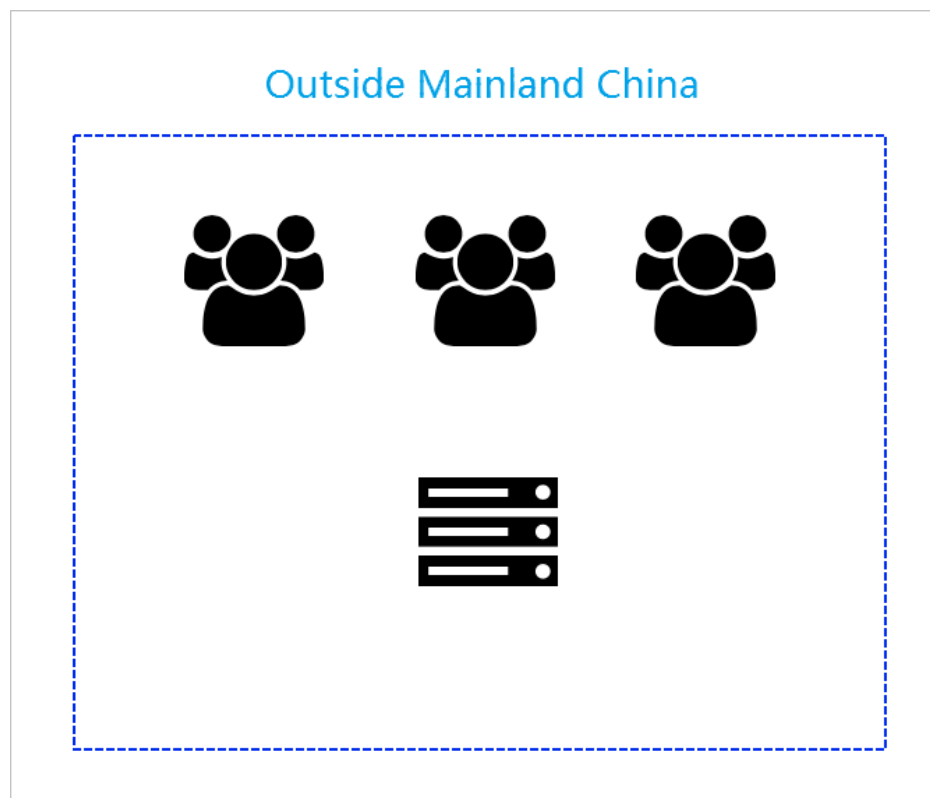
# Scenarios

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.

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:

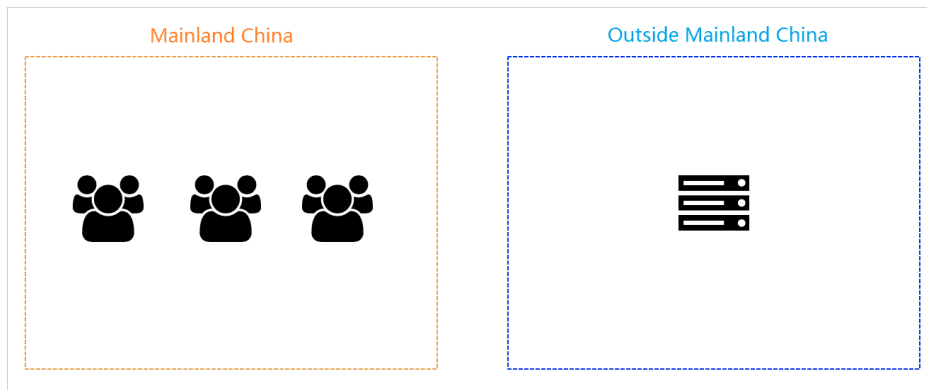
## Scenario 1: Servers deployed outside mainland China, while serving users outside mainland China



**Solution:**

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

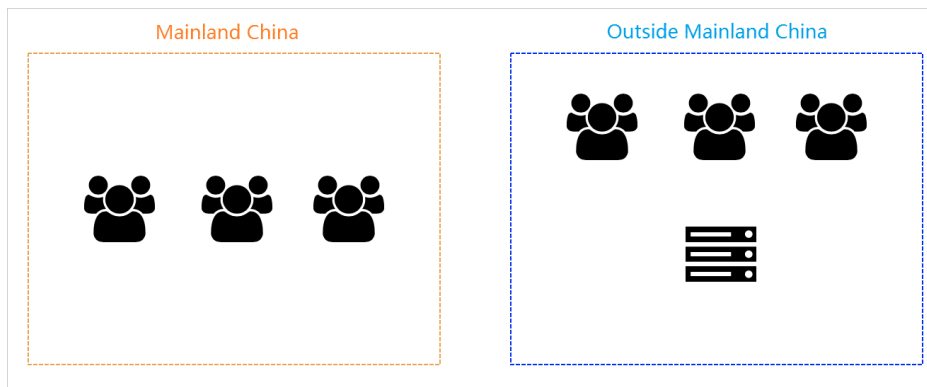
## Scenario 2: Servers deployed outside mainland China, while serving users in mainland China

**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](#).

## Pricing

## Billing method

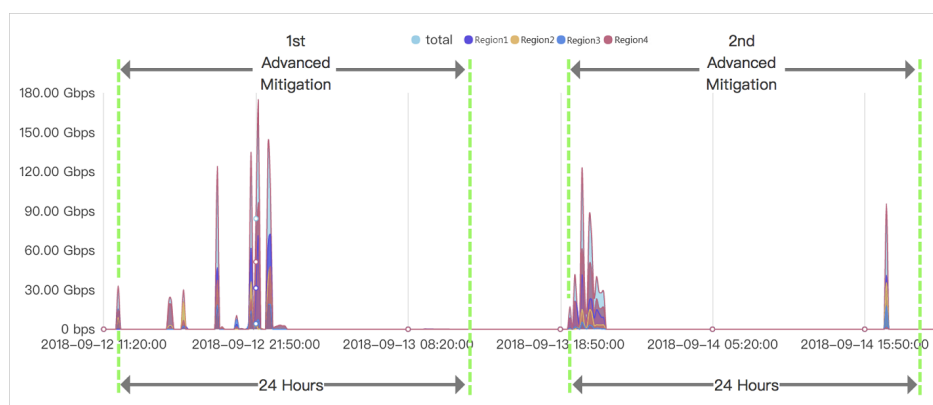
Anti-DDoS Premium offers two plans for your choices:

### Insurance Plan

Anti-DDoS Premium Insurance Plan provides two advanced mitigations (unlimited full-capacity protection) for each month. The advanced mitigation is enabled to provide

unlimited protection with full capacity within 24 hours for your business after it suffers DDoS attacks, and this consumes one advanced mitigation. The advanced mitigations is reset to two at the beginning of every month during the service period.

For example, from September 12th 11:20:00, a protected IP suffers DDoS attacks and advanced mitigation is triggered. Within 24 hours, Anti-DDoS Premium provides unlimited protection with full capacity for the IP. Then, from September 13th 18:50:00, the protected IP suffers DDoS attacks and advanced mitigation is triggered again. 24 hours later, the unlimited protection with full capacity stops and the two advanced mitigation opportunities of the Anti-DDoS Premium Insurance instance in September exhausts. The advanced mitigation opportunities are automatically reset to two at the beginning of next month, October 1st.



This plan is an entry-level solution of Anti-DDoS Premium, and applies to users who have relative low attack risk.

**Note:** Only when the DDoS attack against your business exceeds a specific threshold (basic protection threshold), the advanced mitigation of Anti-DDoS Premium is enabled.

### Unlimited Plan

Anti-DDoS Premium Unlimited Plan provides unlimited advanced mitigations (unlimited full-capacity protection). Purchasing the unlimited plan, no matter what attack frequency, Anti-DDoS Premium prevents your business from DDoS attacks.

## Notice about advanced protection

Anti-DDoS Premium aims to defend against every single DDoS attack by integrating all mitigation capacities of global Alibaba Cloud Anti-DDoS scrubbing centers to protect your business.

In most cases, the attack risk obviously decreases when you successfully defend against DDoS attacks by using Anti-DDoS services. Generally, malicious attackers launch DDoS attacks to cause losses of your business. If the attackers fail to achieve the purpose, the DDoS attack ends due to the cost of launching attacks. Therefore, the advanced mitigation of Anti-DDoS Premium does not have a limited

protection capacity.

**Important:** 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.

## Pricing

Anti-DDoS Premium uses the prepay billing method. It contains the following billing items:

- Clean business bandwidth (under no attack situation)
- Clean business QPS (under no attack situation)
- The number of ports to be protected
- The number of domains to be protected

Plan	Clean Bandwidth	Clean QPS	Advanced Mitigation	Port	Domain	Fee (USD)
Insurance	100 Mbps	500 QPS	2 times/month	50	20	3,200
Unlimited		1,000 QPS	Unlimited	50	20	12,000
Insurance	300 Mbps	500 QPS	2 times/month	50	20	5,600
Unlimited		1,000 QPS	Unlimited	50	20	16,000
Insurance	500 Mbps	500 QPS	2 times/month	50	20	8,000
Unlimited		1,000 QPS	Unlimited	50	20	20,000
Insurance	800 Mbps	500 QPS	2 times/month	50	20	11,600
Unlimited		1,000 QPS	Unlimited	50	20	26,000
Insurance	1,000 Mbps	500 QPS	2 times/month	50	20	14,000
Unlimited		1,000 QPS	Unlimited	50	20	30,000



# Quick Start

## 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 passes through global scrubbing centers first, and is forwarded back to the origin servers. In this situation, the unlimited full-capacity protection has been enabled for your business.

## 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.

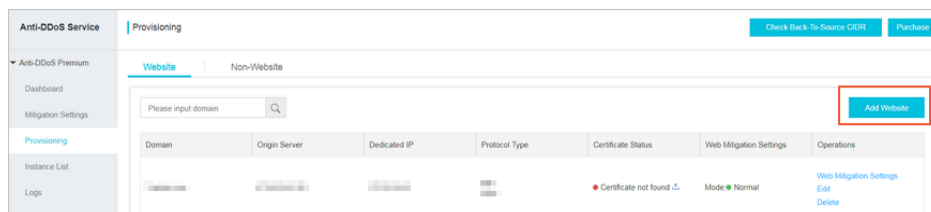
### Procedure

To add your website domain to the Anti-DDoS Premium instance, follow these steps:

**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](#).

Log on to the Anti-DDoS Premium Service console.

Go to **Provisioning>Website** page, and click **Add Website**.



On the **Website configuration** page, enter information for the website to be protected, and then click **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.
Protocol	Protocols that supported by the website.	If your website supports HTTPS or Websockets encryption, select <b>HTTPS</b> or <b>Websockets</b> accordingly, and upload the corresponding certificate and private key information after adding the website.
Origin server	Origin server of the website.	After add the website to the Anti-DDoS Premium instance, the system forwards clean traffic back to the origin server that you specified. - <b>(Recommended)</b> Select <b>IP</b> , 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

		<p>to the origin server IP after the configuration.</p> <p><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.</p> <p>- Select <b>Domain</b>, 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.</p> <p><b>Note:</b> The origin server domain must not be the same as the website domain to be protected.</p>
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.	By default, the HTTP and WebSocket protocols use Port 80, and the HTTPS and Websockets protocols use Port 433.
Choose Dedicated IP	Anti-DDoS Premium instance to protect the	For one website domain, you can set up to 8 Anti-

	website.	DDoS Premium Dedicated IPs.
--	----------	-----------------------------

Add Website
Back

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

Please input IP, separated with ",", cannot be repeated, up to 20.

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 0 IP)

<input type="checkbox"/>	
<input 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

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.

On the Anti-DDoS Premium Service console>**Instance List** page, locate the Anti-DDoS Premium instance that protects the website, and record the Dedicated IP of the instance.

Go to the DNS service provider of your website, and change the A record to point to the Dedicated IP.

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.

**(Optional)** Configure origin server protection, see [Protect origin server that enables Anti-DDoS Pro](#).

**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.

## Add 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.

**Note:** 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.

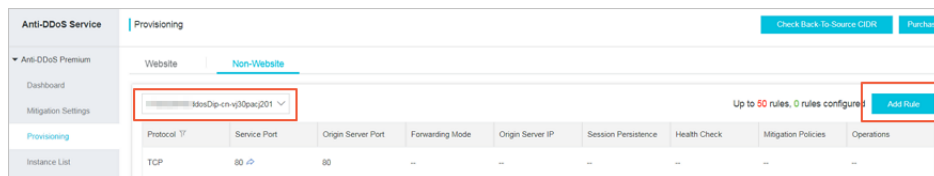
### Procedure

To add a non-website business to the Anti-DDoS Premium instance, follow these steps:

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

Log on to the Anti-DDoS Premium Service console.

Go to **Provisioning>Non-Website** page, select an Anti-DDoS Premium instance, and click **Add Rule**.



Configure the following rule, and click **Confirm**.

Parameter	Description	Note
Protocol	Protocol that to be forwarded.	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.
Origin Server Port	Origin server port that provides service for the business.	Any port from 1 to 65535 is supported.
Origin server 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.

**Add Rule**

\* Protocol: ☒ TCP ☐ UDP

\* Service Port:  + -  
Range 1- 65535

\* Origin Server Port:  + -  
Range 1- 65535

Forwarding Mode: Round Robin

\* Origin server IP   
Separated with ",", cannot be repeated, up to 20.

Confirm Cancel

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:** You can find the Dedicated IP of the Anti-DDoS Premium instance on the Anti-DDoS Premium Service console>**Instance List**page.

- 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 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.

## Configure Anti-DDoS Premium MCA

### What is Anti-DDoS Premium Mainland China Acceleration?

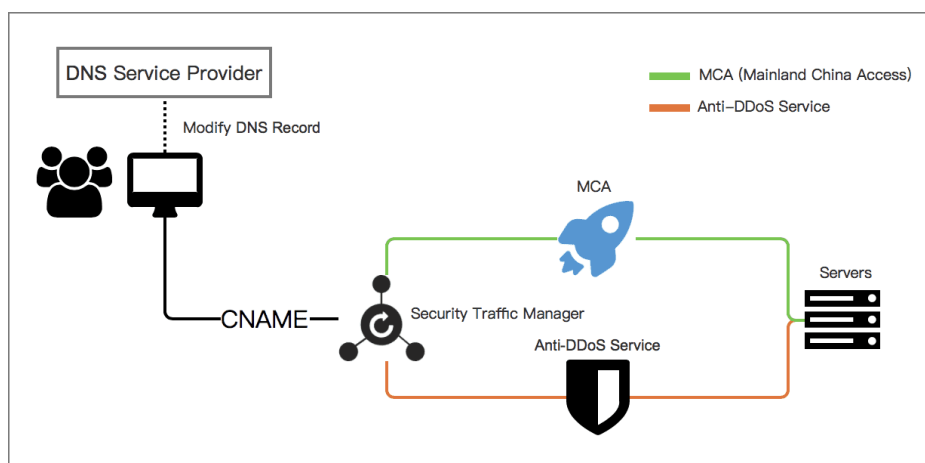
Anti-DDoS Premium mainland China acceleration (MCA) instance is used together with Anti-DDoS Premium Insurance/Unlimited instance, to realize quick access to your web service that deployed

outside mainland China, specially for your Mainland China users.

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 automatically 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.



## Configure Anti-DDoS Premium MCA

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.

To configure the Anti-DDoS Premium MCA instance for your website domain or service port, follow these steps:

1. Log on to the Anti-DDoS Premium Service console.

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.

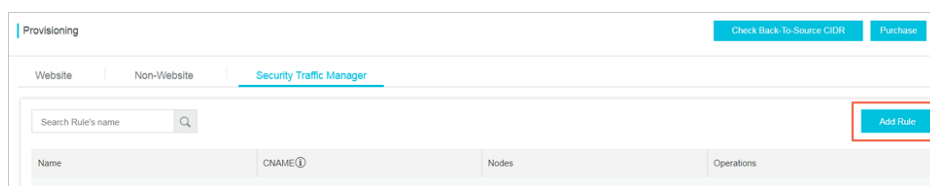


**For website domain:** Refer to Add website to Anti-DDoS Premium for protection to complete the provisioning configuration. During the configuration, choose both dedicated IPs of your Insurance/Unlimited and MCA instances when you choose dedicated IPs of Anti-DDoS Premium.

**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 are 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.

After the provisioning configuration completes, select the **Security Traffic Manager** tab of the **Provisioning** page, click **Add Rule**.



In the **Add Rule** dialog box, select the dedicated IP of the MCA instance as the High Priority node, select the dedicated IP of the Insurance/Unlimited instance as the Low Priority node, and then click **Confirm**. 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.

**Important :** 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.

**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.

Go to the DNS service provider of your service domain, and change the DNS record to the CNAME record that generated by the security traffic manager rule. 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.

## 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 use a domain as the origin site.

# Import provisioning settings of website domain

Log on to the Anti-DDoS Premium Service console.

Go to **Provisioning**, select the **Website** tab, and click **Import** at the bottom of the domain setting list to add provisioning settings for multiple domains.

In the **Add Multiple Rules** dialog box, enter the domain setting parameters in the specific XML format.

**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 starts with `<DomainConfig>` and ends with `</DomainConfig>`. For details about corresponding parameters for the domain provisioning setting, see the following table.

**Note:** For each domain provisioning setting, add a `<DomainConfig>...</DomainConfig>` structure data body.

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 <code>" , "</code> . 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>" , "</code> .
<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: - <code>&lt;ServerType&gt;0&lt;/ServerType&gt;</code> : For origin IP - <code>&lt;ServerType&gt;1&lt;/ServerType&gt;</code> : For origin domain 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 <code>" , "</code> . <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>
```

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

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

## Export provisioning settings of website domain

Go to **Provisioning**, select the **Website** tab, click **Export** at the bottom of the domain setting list, and then click **OK** to start an export task of current domain provisioning settings.

Click the Task List icon in the upper right corner of the Provisioning page, to view the progress of the export task.

After the task completes, click **Download** in the **Task List** dialog box, to download the domain provisioning 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.


## Import provisioning settings of non-website service (layer-4 forwarding rule)

Go to **Provisioning**, select the **Non-Website** tab, click **Add Multiple Rules** at the bottom and select **Add Forwarding Rules**, to import multiple forwarding rules.

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

Refer to the samples to enter information about the settings.

### Forwarding rules



The screenshot shows a dialog box titled "Add Rule" with a close button (X) in the top right corner. Inside the dialog, there is a large text area containing the following text:

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

Below this text area, there is a section titled "Sample of the file content:" with a red border. It contains the same text as the area above:

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

Below the sample content, there is a note:

Note: From left to right, the above fields are **Protocol**, **Forwarding Port**, **Origin site port**, and **Origin site IP**. Thus, in this sample, 2 rules are added. For the first rule, the protocol is **tcp**, the forwarding port is **90**, the origin site port is **91**, and the origin site IP address is **192.136.12.45**.

At the bottom right of the dialog, there are two buttons: "Add" (in blue) and "Cancel" (in gray).

### Session persistence/health-check settings

Session Persistence & Health-Check

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

Sample of the file content:  
8081 tcp 4000 tcp 22 5 5 3 3  
8080 tcp 4000 http 22 5 5 3 3 /search.php www.baidu.com

Note: 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. The "Health Check type" should be chosen from tcp(4 layer)/http(7 layer)/udp. For the UDP forwarding rules, the udp health check type is recommended, and the tcp or http type is recommended for the TCP forwarding rules.

AddCancel

## DDoS mitigation policies

DDoS Mitigation Policies

8081 tcp 2000 50000 20000 100000 1 1500 on on  
8080 udp 1000 50000 20000 100000 1 1500

Sample of the file content:  
8081 tcp 2000 50000 20000 100000 1 1500 on on  
8080 udp 1000 50000 20000 100000 1 1500

Note: 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).

"Forwarding Port" must be a forwarding port that has policies configured. Enter valid values in all other fields. To disable a configuration, enter a value of zero (0).

AddCancel

Click **Add** to import the settings.

## Export forwarding rules

Go to **Provisioning**, select the **Non-Website** tab, click **Export** at the bottom, select **Export Forwarding Rules** and click **OK**, to start an export task for current forwarding rules.

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

Click the Task List icon in the upper right corner of the Provisioning page, to view the progress of the export task.

After the task completes, click **Download** in the **Task List** dialog box, to download the domain provisioning 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.