

# **Alibaba Cloud Anti-DDoS**

Anti-DDoS

Issue: 20200529

# 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please contact Alibaba Cloud directly if you discover any errors in this document.



## Document conventions

Style	Description	Example
	A danger notice 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.
	A warning notice 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 restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click <b>Settings &gt; Network &gt; Set network type</b> .
<b>Bold</b>	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
Courier font	Courier font is used for commands.	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
{ } or {a b}	This format is used for a required value, where only one item can be selected.	switch {active stand}



# Contents

---

<b>Legal disclaimer.....</b>	<b>I</b>
<b>Document conventions.....</b>	<b>I</b>
<b>1 Migrate to the latest Anti-DDoS Pro.....</b>	<b>1</b>
<b>2 Product Introduction.....</b>	<b>10</b>
2.1 What are Anti-DDoS Pro and Anti-DDoS Premium?.....	10
2.2 Anti-DDoS Pro.....	13
2.3 Anti-DDoS Premium.....	16
2.4 DDoS cost protection.....	20
<b>3 Pricing.....</b>	<b>22</b>
3.1 Anti-DDoS Pro billing method.....	22
3.2 Anti-DDoS Premium.....	28
3.2.1 Anti-DDoS Premium billing method.....	28
3.2.2 Mainland China Acceleration.....	32
3.2.3 Global advanced mitigation.....	33
3.3 Instance specification.....	36
3.3.1 Function plan.....	36
3.3.2 Clean bandwidth.....	40
3.3.3 Domains.....	41
<b>4 Quick Start.....</b>	<b>43</b>
4.1 Set up Anti-DDoS Pro using domains.....	43
4.1.1 Overview.....	43
4.1.2 Step 1: Add forwarding rules.....	44
4.1.3 Step 2: Configure service traffic forwarding.....	49
4.1.4 Step 3: Configure protection policies.....	51
4.1.5 Step 4: View the protection data of your website services.....	53
4.2 Set up Anti-DDoS Pro using IPs and ports.....	56
4.2.1 Overview.....	56
4.2.2 Step 1: Create a port forwarding rule.....	57
4.2.3 Step 2: Configure port forwarding and anti-DDoS protection policies.....	60
4.2.4 Step 3: View the protection data of a port.....	64
<b>5 Resource management.....</b>	<b>68</b>
5.1 Purchase Anti-DDoS Pro or Anti-DDoS Premium instances.....	68
5.2 Upgrade the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance.....	74
5.3 Manage instance tags.....	75
<b>6 Check security overview.....</b>	<b>78</b>
<b>7 View security reports.....</b>	<b>86</b>
<b>8 Deploy Anti-DDoS Pro.....</b>	<b>90</b>



8.1 Use domains.....	90
8.1.1 Add a website.....	90
8.1.2 Edit a website configuration.....	97
8.1.3 Delete a website configuration.....	99
8.1.4 Export multiple website configurations at a time.....	100
8.1.5 Specify non-standard ports for protection.....	102
8.1.6 Upload an SSL certificate.....	103
8.1.7 Create a custom TLS policy.....	107
8.1.8 Website configurations in an XML file.....	109
8.2 Use ports.....	111
8.2.1 Create forwarding rules.....	111
8.2.2 Edit forwarding rules.....	116
8.2.3 Delete forwarding rules.....	118
8.2.4 Export multiple port configurations.....	119
8.2.5 Configure a health check.....	122
8.2.6 Configure session persistence.....	126
8.3 Provisioning settings.....	130
8.3.1 Modify DNS records to protect websites.....	130
8.3.2 Enable NS Mode Access to protect a website.....	134
8.3.3 Modify the CNAME record to protect a non-website service.....	136
8.3.4 Modify the CNAME record to reroute traffic by using Sec-Traffic Manager.....	141
8.4 Sec-Traffic Manager.....	143
8.5 CNAME reuse.....	158
8.6 Allow back-to-origin IP addresses to access the origin server.....	164
8.7 Verify the forwarding configuration on your local machine.....	166
8.8 Change the public IP address of an ECS origin server.....	168
8.9 Configure Anti-DDoS Premium MCA.....	169
<b>9 Protection settings.....</b>	<b>174</b>
9.1 Protection for infrastructure.....	174
9.1.1 Configure a blacklist or whitelist for destination IP addresses.....	174
9.1.2 Configure diversion from the origin server.....	180
9.1.3 Configure blocked regions.....	183
9.1.4 Deactivate a black hole.....	185
9.2 Protection for website services.....	187
9.2.1 Configure intelligent protection.....	187
9.2.2 Configure blacklists and whitelists for domain names.....	191
9.2.3 Configure blocked regions for domain names.....	194
9.2.4 Configure accurate access control rules.....	197
9.2.5 Configure frequency control.....	204
9.3 Protection for non-website services.....	210
9.3.1 Configure Layer 4 intelligent protection.....	210
9.3.2 Create an anti-DDoS protection policy.....	212
9.3.3 Configure the speed limit for source IP addresses.....	223
9.4 Configure static page caching.....	226

9.5 Create custom policies for specific scenarios.....	228
<b>10 Query and analysis.....</b>	<b>233</b>
10.1 Full log.....	233
10.2 Fields supported by full log.....	239
10.3 Operation logs.....	243
<b>11 Best Practices.....</b>	<b>244</b>
11.1 Create an Anti-DDoS Pro alert rule.....	244
11.2 Monitor black hole events and traffic scrubbing events on Anti-DDoS Pro.....	252
11.3 Create an Anti-DDoS Pro dashboard.....	259
<b>12 API Reference.....</b>	<b>266</b>
12.1 List of operations by function.....	266
12.2 Make API requests.....	276
12.3 Request signatures.....	278
12.4 Common parameters.....	282
12.5 Obtain an AccessKey pair.....	284
12.6 Instances.....	286
12.6.1 DescribeInstanceIds.....	286
12.6.2 DescribeInstances.....	289
12.6.3 DescribeInstanceDetails.....	295
12.6.4 DescribeInstanceSpecs.....	297
12.6.5 DescribeInstanceStatistics.....	300
12.6.6 ModifyInstanceRemark.....	303
12.6.7 DescribeElasticBandwidthSpec.....	304
12.6.8 ModifyElasticBandWidth.....	306
12.6.9 DescribeDefenseCountStatistics.....	308
12.7 Website configuration.....	310
12.7.1 DescribeDomains.....	310
12.7.2 DescribeWebRules.....	312
12.7.3 CreateWebRule.....	318
12.7.4 ModifyWebRule.....	321
12.7.5 DeleteWebRule.....	324
12.7.6 DescribeWebInstanceRelations.....	326
12.7.7 DescribeCerts.....	329
12.7.8 AssociateWebCert.....	332
12.7.9 DescribeWebCustomPorts.....	336
12.7.10 ModifyTlsConfig.....	338
12.7.11 ModifyHttp2Enable.....	341
12.7.12 DescribeWebAccessMode.....	343
12.7.13 ModifyWebAccessMode.....	345
12.7.14 DescribeCnameReuses.....	347
12.7.15 ModifyCnameReuse.....	349
12.8 Port configuration.....	351
12.8.1 DescribeNetworkRules.....	351
12.8.2 CreateNetworkRules.....	355

12.8.3	ConfigNetworkRules.....	357
12.8.4	DeleteNetworkRule.....	360
12.8.5	DescribeHealthCheckList.....	362
12.8.6	ModifyHealthCheckConfig.....	366
12.8.7	DescribeHealthCheckStatus.....	369
12.9	Sec-Traffic manager.....	372
12.9.1	DescribeSchedulerRules.....	372
12.9.2	CreateSchedulerRule.....	377
12.9.3	ModifySchedulerRule.....	382
12.9.4	DeleteSchedulerRule.....	387
12.10	Protection for infrastructure.....	388
12.10.1	DescribeAutoCcListCount.....	388
12.10.2	DescribeAutoCcBlacklist.....	390
12.10.3	AddAutoCcBlacklist.....	394
12.10.4	DeleteAutoCcBlacklist.....	396
12.10.5	EmptyAutoCcBlacklist.....	398
12.10.6	DescribeAutoCcWhitelist.....	399
12.10.7	AddAutoCcWhitelist.....	402
12.10.8	DeleteAutoCcWhitelist.....	404
12.10.9	EmptyAutoCcWhitelist.....	406
12.10.10	DescribeUnBlackholeCount.....	408
12.10.11	DescribeBlackholeStatus.....	409
12.10.12	ModifyBlackholeStatus.....	412
12.10.13	DescribeNetworkRegionBlock.....	414
12.10.14	ConfigNetworkRegionBlock.....	430
12.10.15	DescribeBlockStatus.....	447
12.10.16	ModifyBlockStatus.....	449
12.10.17	DescribeUnBlockCount.....	451
12.11	Protection for website services.....	453
12.11.1	DescribeWebCcProtectSwitch.....	453
12.11.2	ModifyWebAIProtectSwitch.....	457
12.11.3	ModifyWebAIProtectMode.....	460
12.11.4	ModifyWebIpSetSwitch.....	462
12.11.5	ConfigWebIpSet.....	465
12.11.6	EnableWebCC.....	467
12.11.7	DisableWebCC.....	469
12.11.8	ConfigWebCCTemplate.....	471
12.11.9	EnableWebCCRule.....	473
12.11.10	DisableWebCCRule.....	475
12.11.11	DescribeWebCCRules.....	477
12.11.12	CreateWebCCRule.....	480
12.11.13	ModifyWebCCRule.....	483
12.11.14	DeleteWebCCRule.....	486
12.11.15	ModifyWebPreciseAccessSwitch.....	488
12.11.16	DescribeWebPreciseAccessRule.....	490

12.11.17 ModifyWebPreciseAccessRule.....	494
12.11.18 DeleteWebPreciseAccessRule.....	504
12.11.19 ModifyWebAreaBlockSwitch.....	506
12.11.20 DescribeWebAreaBlockConfigs.....	509
12.11.21 ModifyWebAreaBlock.....	516
12.12 Protection for non-website services.....	519
12.12.1 DescribePortAutoCcStatus.....	519
12.12.2 ModifyPortAutoCcStatus.....	522
12.12.3 DescribeNetworkRuleAttributes.....	524
12.12.4 ModifyNetworkRuleAttribute.....	531
12.13 Custom scenario policy.....	533
12.13.1 DescribeSceneDefensePolicies.....	533
12.13.2 CreateSceneDefensePolicy.....	539
12.13.3 ModifySceneDefensePolicy.....	541
12.13.4 DeleteSceneDefensePolicy.....	543
12.13.5 DescribeSceneDefenseObjects.....	545
12.13.6 AttachSceneDefenseObject.....	548
12.13.7 DetachSceneDefenseObject.....	550
12.13.8 EnableSceneDefensePolicy.....	552
12.13.9 DisableSceneDefensePolicy.....	553
12.14 Static page caching.....	555
12.14.1 ModifyWebCacheSwitch.....	555
12.14.2 ModifyWebCacheMode.....	557
12.14.3 ModifyWebCacheCustomRule.....	560
12.14.4 DeleteWebCacheCustomRule.....	563
12.14.5 DescribeWebCacheConfigs.....	565
12.15 Investigation.....	568
12.15.1 DescribeDDoSEvents.....	568
12.15.2 DescribePortFlowList.....	572
12.15.3 DescribePortConnsList.....	577
12.15.4 DescribePortConnsCount.....	581
12.15.5 DescribePortMaxConns.....	584
12.15.6 DescribePortAttackMaxFlow.....	588
12.15.7 DescribePortViewSourceCountries.....	590
12.15.8 DescribePortViewSourceIps.....	605
12.15.9 DescribePortViewSourceProvinces.....	610
12.15.10 DescribeDomainAttackEvents.....	615
12.15.11 DescribeDomainQPSList.....	618
12.15.12 DescribeDomainStatusCodeList.....	622
12.15.13 DescribeDomainOverview.....	627
12.15.14 DescribeDomainStatusCodeCount.....	630
12.15.15 DescribeDomainTopAttackList.....	634
12.15.16 DescribeDomainViewSourceCountries.....	636
12.15.17 DescribeDomainViewSourceProvinces.....	652
12.15.18 DescribeDomainViewTopCostTime.....	657

12.15.19 DescribeDomainViewTopUrl.....	660
12.15.20 DescribeDomainQpsWithCache.....	663
12.16 Log analysis.....	668
12.16.1 DescribeSlsOpenStatus.....	668
12.16.2 DescribeSlsAuthStatus.....	670
12.16.3 DescribeLogStoreExistStatus.....	672
12.16.4 DescribeSlsLogstoreInfo.....	674
12.16.5 ModifyFullLogTtl.....	676
12.16.6 DescribeWebAccessLogDispatchStatus.....	678
12.16.7 DescribeWebAccessLogStatus.....	680
12.16.8 EnableWebAccessLogConfig.....	683
12.16.9 DisableWebAccessLogConfig.....	685
12.16.10 DescribeWebAccessLogEmptyCount.....	687
12.16.11 EmptySlsLogstore.....	688
12.17 System configuration and logs.....	690
12.17.1 DescribeStsGrantStatus.....	690
12.17.2 DescribeBackSourceCidr.....	693
12.17.3 DescribeOpEntities.....	694
12.17.4 DescribeDefenseRecords.....	701
12.17.5 DescribeAsyncTasks.....	705
12.17.6 CreateAsyncTask.....	710
12.17.7 DeleteAsyncTask.....	713
12.18 Tag.....	715
12.18.1 DescribeTagKeys.....	715
12.18.2 DescribeTagResources.....	718
12.18.3 CreateTagResources.....	722
12.18.4 DeleteTagResources.....	724
12.19 Error codes.....	726



# 1 Migrate to the latest Anti-DDoS Pro

---

## Overview

It has been three years since Alibaba Cloud released the previous version of Anti-DDoS Pro. To meet your needs for more reliable networking, Alibaba Cloud has been consistently improving Anti-DDoS Pro services.

Currently, Alibaba Cloud has released the latest version of [Anti-DDoS Pro](#).

The latest version is built on a new network infrastructure that connects Anti-DDoS Pro with Alibaba Cloud BGP data centers. This version reduces the average latency between Anti-DDoS Pro and any Chinese mainland region to less than 20 ms and offers more reliable networking than China Telecom or China Unicom networks alone. Anti-DDoS Pro adopts an architecture that requires attack traffic to be filtered in the same ISP network where the traffic was first detected. This significantly improves disaster recovery and protection capabilities offered by Anti-DDoS Pro.

### Anti-DDoS Pro instance configurations

- Basic bandwidth: The minimum basic bandwidth is 30 Gbit/s, which only costs RMB 20,800 per month.
- Burstable bandwidth: The maximum burstable bandwidth is 600 Gbit/s. Contact customer service if you need more burstable bandwidth.

## Migrate to the latest Anti-DDoS Pro

We recommend that you migrate to the latest version of Anti-DDoS Pro for a more reliable, secure, and faster service. Note the following details:

- The China Telecom data center in Suzhou and China Unicom data center in Dalian will stop providing services after December 30, 2018. If your Anti-DDoS Pro instances are deployed in any of these data centers, you must migrate your service to the latest version of Anti-DDoS Pro before December 30, 2018. If you need help with service migration, contact customer service.



### Note:

You must migrate to the latest Anti-DDoS Pro if your Anti-DDoS Pro instances meet the criteria.

- You can keep using your current Anti-DDoS Pro instances if they are not deployed in the China Telecom data center in Suzhou or China Unicom data center in Dalian. To experience the latest version of Anti-DDoS Pro now, you can purchase new Anti-DDoS Pro instances and migrate your service to new instances.

## Procedure

You can perform the following steps to migrate your service.

### Before you begin

Contact customer service to check whether your Anti-DDoS Pro instances meet the preceding criteria.

If your Anti-DDoS Pro instances meet the criteria, you can contact customer service to create new Anti-DDoS Pro instances for you. The expiration time of new instances is no earlier than that of old instances.

New instances have the same configurations as old instances.



#### Note:

We recommend that you migrate your service to new Anti-DDoS Pro instances once the new instances are created. During the migration process, both old and new Anti-DDoS Pro instances can forward your traffic and protect the security of your business.



#### Notice:

We recommend that you back up your configurations in advance. You can read [Import and export configurations](#) to learn how to import and export domain configurations and forwarding rules in the Anti-DDoS Pro console. After you migrate domain configurations to the new Anti-DDoS Pro instances, you cannot view these configurations on old Anti-DDoS Pro instances.

1. Log on to the [Anti-DDoS Pro console](#).



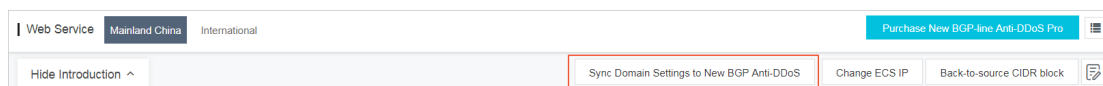
## 2. Migrate domain configurations and forwarding rules to new Anti-DDoS Pro instances.

- **Migrate domain configurations to new Anti-DDoS Pro instances**

### Notes:

- Do not add forwarding rules on port 80 or 443. Anti-DDoS Pro uses port 80 or 443 by default. If the ports are already in use, you cannot associate your domain to new Anti-DDoS Pro instances.
- If you submitted a ticket to redirect HTTP/2 or HTTPS requests to HTTP, you must disable the redirect feature before you migrate domain configurations to new Anti-DDoS Pro instances.
- If a wildcard subdomain that matches your domain is already configured in other accounts, you cannot associate your domain to new Anti-DDoS Pro instances. If you have multiple Alibaba Cloud accounts, make sure to avoid this conflict.

**a.** In the left-side navigation pane, choose **Access > Web Service**, and click **Sync Domain Settings to New BGP Anti-DDoS**.



**b.** Enter the IP address of the new Anti-DDoS Pro instance and select the domains to be migrated.



### Note:

You can select up to 5 domains. If the old Anti-DDoS Pro instance is associated with more than 5 domains, synchronize domain configurations between the old and new instance in batches.

Sync Domain Settings to New BGP Anti-DDoS

Please view corresponding [documentation](#) before doing the synchronization.

IP:

12

Please enter a New BGP Anti-DDoS IP

Select Domain:

☐ Select All

☐ adf.test.com

Synchronize

Cancel

- c. Click **Synchronize** to migrate domain configurations to the new Anti-DDoS Pro instance. To view the domain configurations that are already migrated to new Anti-DDoS Pro instances, log on to the [New BGP Anti-DDoS console](#) and select **Management > Websites**.

**Note:**

At this point, your traffic is still forwarded by the old Anti-DDoS Pro instance.

**Domain synchronization notes:**

- If you have only one old Anti-DDoS Pro instance, perform the preceding steps to synchronize all domain configurations between the old and new Anti-DDoS Pro instance.
- If you have multiple old Anti-DDoS Pro instances and some domains are associated with multiple instances, you must identify the domains to be

synchronized and the Anti-DDoS Pro instances associated with these domains . If you want to keep using some of the old Anti-DDoS Pro instances, we recommend that you dissociate the domains to be synchronized from these instances and perform the preceding steps to synchronize domain configurations between old and new Anti-DDoS Pro instances.

**Notice:**

After you synchronize domain configurations, you cannot view these configurations on old Anti-DDoS Pro instances. However, the domains are still associated with old Anti-DDoS Pro instances. You can choose **Management > Websites** in the New BGP Anti-DDoS console to view domain configurations that are already migrated to new Anti-DDoS Pro instances. To prevent mistakes to these domain configurations, you cannot view these configurations in the old Anti-DDoS Pro console.

- d. After you synchronize domain configurations, we recommend that you log on to the [New BGP Anti-DDoS console](#), choose **Management > Websites**, and compare the domain configurations in the Websites list with your backup configurations. If you find any differences, you can manually change the domain configurations according to your backup configurations.

**Notes:**

- The new and old Anti-DDoS Pro instances use different CIDR blocks to forward traffic back to your origin server. If you set access control rules on your origin server, make sure to add the back-to-origin CIDR blocks used by new Anti-DDoS Pro instances to the whitelist. You can select **Management > Websites** and click

**View Back-to-origin CIDR Blocks** to view all back-to-origin CIDR blocks used by new Anti-DDoS Pro instances.

- If your domain has not obtained an ICP license, you can submit a ticket or contact customer service for help. We recommend that you obtain an ICP license as soon as possible.

- **Migrate forwarding rules to the new Anti-DDoS Pro instances**

- a. In the left-side navigation pane, choose **Access > Non-Web Service** and select an Anti-DDoS Pro instance and IP address.
- b. Click **Export Rules** and select **Export rules** to export forwarding rules in a TXT file to your local computer.
- c. In the [New BGP Anti-DDoS console](#), choose **Management > Port Settings**, select an Anti-DDoS Pro instance, click **Batch Operations**, and select **Create Rule**.
- d. Copy the contents of the TXT file to the edit area in the Create Rule dialog box, and click **Create** to migrate the forwarding rules to the selected Anti-DDoS Pro instance.

**Note:**

For more information about importing and exporting multiple forwarding rules, see [Import and export configurations](#). After you migrate forwarding rules to the new instance, you can follow a similar procedure to migrate session persistence and health check settings to the new instance.

3. You can modify the hosts file on your machine to test if the domain configurations and forwarding rules work as expected. For more information, see [Test configurations on local machines](#).
4. After you pass the tests, change DNS resolution settings and modify A record values through your DNS provider to forward traffic to your Anti-DDoS Pro instances.

**Note:**

If you use IPs and ports to set up the Anti-DDoS Pro instance, replace your service IP with the IP address of the Anti-DDoS Pro instance to forward traffic to Anti-DDoS Pro.

5. After you migrate your service to new Anti-DDoS Pro instances, your old Anti-DDoS Pro instances will be released when their subscription period ends. You can also submit a ticket or contact customer service to release your old instances.

**Note:**

When both old and new Anti-DDoS Pro instances are in use, you cannot delete the domain configurations that were migrated from the old instances in the new BGP Anti-DDoS console. You can only delete these domain configurations when the associated old Anti-DDoS Pro instances are released.

## Notes

- The migration process will not affect your service. If you need to roll back the configurations, submit a ticket or contact customer service.
- To avoid additional fees during the migration process and when both new and old Anti-DDoS Pro instances are in use, we recommend that you set the basic bandwidth and burstable bandwidth to the same value on your old Anti-DDoS Pro instances.
- If your Anti-DDoS Pro instances do not meet the preceding criteria, you can purchase new Anti-DDoS Pro instances by yourself and follow the preceding steps to migrate your service to new Anti-DDoS Pro instances. After the migration process is complete, and your old Anti-DDoS Pro instances have subscription time left, you can submit a ticket to request a refund.



### Note:

If your Anti-DDoS Pro instances meet the preceding criteria, you cannot request a refund because your new Anti-DDoS Pro instances are created by Alibaba Cloud free of charge.

## FAQ

### What benefits does the latest Anti-DDoS Pro have?

For more information about the benefits offered by Anti-DDoS Pro, see [What is Anti-DDoS Pro](#).

### Where can I find detailed pricing information?

For more information about pricing, see [Billing methods](#).

### How fast is the network used by Anti-DDoS Pro?

You can use third-party testing tools to test the latency of Anti-DDoS Pro instances. For example, <http://ping.chinaz.com/203.107.32.57>.

Test IP address: 203.107.32.57

### Do I need to buy new Anti-DDoS Pro instances during the migration process?

No. After you confirm the configurations of your new Anti-DDoS Pro instances with customer service, Alibaba Cloud creates new Anti-DDoS Pro instances for you free of charge .

**How can I tell where my Anti-DDoS Pro instance is deployed?**

Your Anti-DDoS Pro instance is deployed in the China Telecom data center in Suzhou or China Unicom data center in Dalian if its IP address is within one of the following CIDR blocks:

- 180.97.164.128/26
- 180.97.164.0/25
- 180.97.163.0/24
- 180.97.162.0/24
- 180.97.161.0/24
- 180.97.89.0/24
- 180.101.207.0/24
- 180.101.208.0/24
- 218.94.232.0/24
- 218.60.113.0/24
- 218.60.114.0/24
- 218.60.115.0/25
- 218.60.115.128/26
- 218.60.112.0/24
- 218.60.121.0/24
- 218.60.82.0/24
- 218.60.83.0/24
- 211.93.149.0/24

**How long does it take to migrate my service to new Anti-DDoS Pro instances?**

- If you use domains to set up Anti-DDoS Pro instances, it takes one to three days because you need to update DNS records through your DNS provider.
- If you use IPs and ports to set up Anti-DDoS Pro instances, it depends on your service status.

**Will my service be interrupted during the migration process?**

In most situations, migrating to new Anti-DDoS Pro instances does not affect your service. The actual situation may vary according to the service status. Alibaba Cloud allows you to keep both old and new Anti-DDoS Pro instances in use for a period of time. Old Anti-DDoS Pro instances are not released until Alibaba Cloud confirms that all your traffic is forwarded to your new Anti-DDoS Pro instances.

Your service availability is the highest priority of Alibaba Cloud during the entire migration process.

**What else do I need to know when migrating to the latest Anti-DDoS Pro?**

- The latest version of Anti-DDoS Pro is based on BGP networks and supports quick disaster recovery. This version provides faster and more reliable networks compared with older versions. To set up the latest Anti-DDoS Pro to protect your business, you need to change A records instead of CNAME records.
- The latest Anti-DDoS Pro uses different back-to-origin CIDR blocks than older versions of Anti-DDoS Pro. You need to manually update back-to-origin CIDR blocks if you have set access control rules to protect your origin server.

## 2 Product Introduction

---

### 2.1 What are Anti-DDoS Pro and Anti-DDoS Premium?

Anti-DDoS Pro and Anti-DDoS Premium provide proxy protection services to protect against distributed denial of service (DDoS) attacks. They protect network servers from volumetric DDoS attacks. Anti-DDoS Pro and Anti-DDoS Premium forward traffic to the Alibaba Cloud anti-DDoS network by using DNS resolution, and then connect services to the Anti-DDoS Service system in DNS proxy mode. This protects against volumetric and resource exhaustion DDoS attacks.

#### Anti-DDoS Pro and Anti-DDoS Premium

Anti-DDoS Pro and Anti-DDoS Premium provide effective solutions for scenarios where your servers are deployed inside and outside mainland China.

- [Anti-DDoS Pro](#): provides bandwidth resources of eight BGP lines at the Tbit/s level. It protects servers that are deployed in **mainland China** and serve **mainland China** users from volumetric DDoS attacks.
- [Anti-DDoS Premium](#): relies on the state of the art distributed near-source traffic scrubbing capability. It provides unlimited protection capability for servers that are deployed **outside mainland China** and serve users **outside mainland China**.

#### How Anti-DDoS Pro and Anti-DDoS Premium work

Anti-DDoS Pro and Anti-DDoS Premium forward traffic based on DNS resolution records or IP addresses to protect the services connected by using domain names and ports. The results of DNS resolutions or the service IP addresses are mapped to the IP addresses or CNAME records of Anti-DDoS Pro or Anti-DDoS Premium instances based on forwarding rules configured by users.

All inbound traffic from the Internet first passes through the anti-DDoS data center. Attack traffic is scrubbed and filtered in the traffic scrubbing center, and clean traffic is forwarded back to the origin server by using forwarding ports. This ensures stable access to the origin server.



## Benefits

Compared with traditional anti-DDoS security solutions, Anti-DDoS Pro and Anti-DDoS Premium are more stable and easier to deploy. They rely on high-quality BGP networks and intelligent protection technologies to provide stronger protection with higher availability.

- Five-minute deployment

You can protect domain names and ports by mapping either the results of DNS resolutions or service IP addresses to the IP addresses of Anti-DDoS Pro and Anti-DDoS Premium instances. This way, you can enable Anti-DDoS Pro or Anti-DDoS Premium protection for your assets without any hardware or software installation, or router and switch configuration.

- Massive protection bandwidth

Anti-DDoS Pro provides a protection bandwidth of more than 8 Tbit/s in mainland China , and Anti-DDoS Premium provides a protection bandwidth of more than 2 Tbit/s outside mainland China.

- Intelligent protection

Anti-DDoS Pro and Anti-DDoS Premium automatically optimize protection algorithms and learn service traffic baselines from the protection analysis of volumetric and resource exhaustion DDoS attacks. This enables the services to identify malicious IP addresses, and scrub and filter attack traffic.

- Protection against volumetric DDoS attacks

Volumetric DDoS attacks at the transport layer congest networks, leave data centers unavailable, and interrupt or paralyze your services. Anti-DDoS Pro and Anti-DDoS Premium adopt conventional technologies, such as proxy, detection, rebound, authentication, blacklist and whitelist, and packet compliance. They also employ IP reputation investigation, near-source scrubbing, and in-depth packet analysis based on network fingerprints, user behaviors, and content characteristics. These technologies block and filter threats based on user-defined rules, which ensures that the protected services provide external services even under sustained attacks.

- Protection against resource exhaustion DDoS attacks (HTTP flood attacks)

Anti-DDoS Pro and Anti-DDoS Premium integrate intelligent protection engines to protect against resource exhaustion DDoS attacks when application-layer services are interrupted under attacks. They also support URL-level threat filtering at a custom

frequency to improve protection efficiency, protection success rate, and work efficiency of O&M personnel. Intelligent protection engines provide effective protection by:

- Learning your traffic to obtain traffic characteristics.
- Dynamically generating normal service baselines.
- Quickly discovering exceptions of traffic and characteristics.
- Participating the attack characteristics analysis.
- Automatically generating a combination of multi-dimensional policies.
- Dynamically executing or canceling protection policy instructions.
- High stability and reliability
  - Anti-DDoS Pro and Anti-DDoS Premium use high-availability network protection clusters to avoid single-point failure and redundancy. The processing capabilities of Anti-DDoS Pro and Anti-DDoS Premium can be scaled up.
  - Anti-DDoS Pro and Anti-DDoS Premium monitor the inbound traffic forwarded to the traffic scrubbing center and CPU and memory resources of all servers to ensure the availability of the data center. They also monitor the availability of server engines and bring or take servers online or offline based on monitoring results.
  - Anti-DDoS Pro and Anti-DDoS Premium monitor the availability of back-to-origin links and automatically switch to secondary links when primary links are unstable, which ensures link availability.
  - Anti-DDoS Pro and Anti-DDoS Premium perform health checks on protected origin servers and switch service traffic to another healthy origin server when an origin server is unhealthy. They also monitor the HTTP status codes of origin servers and initiate back-to-origin or switchover operations when errors are detected.

- Traffic rerouting

Anti-DDoS Pro and Anti-DDoS Premium forward traffic based on cloud product-specific security events and DNS resolution records. They keep DDoS protection disabled for secure cloud products and enable DDoS protection for vulnerable cloud products by connecting the cloud products to themselves. You can customize forwarding templates as required for Anti-DDoS Pro and Anti-DDoS Premium to automatically schedule DDoS protection based on the security states of cloud products. The templates contain Cloud Service Interaction, Tiered Protection, and Network Acceleration.

## Scenarios

Anti-DDoS Pro and Anti-DDoS Premium are suitable for finance websites, e-commerce websites, portal websites, Internet egress of government departments, portals, and open platforms. They provide DDoS protection for important live streaming and sales promotions. Anti-DDoS Pro and Anti-DDoS Premium protect against malicious attacks and blackmailing by competitors, and prevent mobile apps from malicious registration, empty box scams, and fraud traffic.

We recommend that you use Anti-DDoS Pro and Anti-DDoS Premium to mitigate the following security risks in the preceding industries and scenarios:

- Ransom-driven DDoS attacks occur.
- DDoS attacks have frozen your services and urgent protection is required to recover it.
- DDoS attacks occur frequently. Continuous protection against DDoS is required to ensure service stability.

## 2.2 Anti-DDoS Pro

Anti-DDoS Pro provides eight BGP lines at the Tbit/s level to protect your servers deployed in mainland China against volumetric DDoS attacks. Compared with anti-DDoS service based on Internet Data Center (IDC), Anti-DDoS Pro now supports more reliable networks with lower latency. This enables quicker disaster recovery.

### Benefits

Anti-DDoS Pro provides the following benefits:

- Maximum BGP bandwidth resources in mainland China. It provides a maximum protection bandwidth of 1.5 Tbit/s to protect your services against volumetric DDoS attacks.
- Top-quality bandwidth resources in mainland China. Its BGP lines cover most Internet service provider (ISP) networks in mainland China, such as China Telecom, China Unicom, China Mobile, and China Education and Research Network. The average latency is about 20 ms.
- Only one IP address is required to access different ISP networks in mainland China.

**Differences between IDC-based anti-DDoS service and Anti-DDoS Pro**

Item	IDC-based anti-DDoS service (China Telecom, China Unicom, and China Mobile networks)	IDC-based anti-DDoS service (BGP lines)	Anti-DDoS Pro
ISP networks	Only supports China Telecom, China Unicom, and China Mobile networks.	Supports multiple small and medium-sized ISP networks in addition to China Telecom, China Unicom, and China Mobile networks.	Supports multiple small and medium-sized ISP networks in addition to China Telecom, China Unicom, and China Mobile networks.
Network latency	Average latency is 30 ms in mainland China. Cross-network access may occur if you use networks provided by small-sized ISPs.	Average latency is 20 ms in mainland China. No cross-network access is required.	Average latency is 20 ms in mainland China. No cross-network access is required.
Dedicated back-to-origin line	Not supported. Traffic is forwarded back to the origin server with a latency over the Internet.	If the origin server is deployed on Alibaba Cloud, traffic is forwarded back to the origin server with a negligible latency by using dedicated connections. Otherwise, traffic is forwarded back to the origin server over the Internet.	If the origin server is deployed on Alibaba Cloud, traffic is forwarded back to the origin server with a negligible latency by using dedicated connections. Otherwise, traffic is forwarded back to the origin server over the Internet.

Item	<b>IDC-based anti-DDoS service</b>  <b>(China Telecom , China Unicom, and China Mobile networks)</b>	<b>IDC-based anti-DDoS service</b>  <b>(BGP lines)</b>	<b>Anti-DDoS Pro</b>
Disaster recovery	If a server fault occurs, transport-layer traffic cannot be automatically scheduled. Due to DNS resolution limits, automatic scheduling for application-layer traffic cannot take effect immediately.	Supports automatic scheduling for all traffic based on BGP routing. The switchover is completed within several seconds.	Supports automatic scheduling for all traffic based on BGP routing. The switchover is completed within several seconds.
IP addresses	Needs more than two IP addresses , which requires a larger configuration workload.	Needs only one IP address.	Needs only one IP address.
Maximum protection capability	Provides a maximum protection bandwidth of 1 Tbit/s against volumetric DDoS attacks based on China Telecom or China Unicom networks.	Provides a maximum protection bandwidth of 100 Gbit/s against volumetric DDoS attacks.	Provides a maximum protection bandwidth of 1.5 Tbit /s against volumetric DDoS attacks.
Attack mitigation for the transport layer	Supports protection against flood attacks such as SYN floods, ACK floods, and ICMP floods. Filters out malformed packets , empty requests, and requests from zombies.	The same.	The same.

Item	IDC-based anti-DDoS service (China Telecom, China Unicom, and China Mobile networks)	IDC-based anti-DDoS service (BGP lines)	Anti-DDoS Pro
Attack mitigation for the application layer	Supports protection against HTTP flood attacks.	Supports protection against HTTP flood attacks.	Supports protection against HTTP flood attacks.

## Scenarios

We recommend that you use Anti-DDoS Pro as required:

- A reliable network that has a minimal latency, provides quick disaster recovery, and covers multiple ISP networks.
- Basic protection that offers 20 Gbit/s or more of BGP bandwidth.
- Protection against volumetric DDoS attacks over 300 Gbit/s.

## References

- [Anti-DDoS Pro billing method](#)
- [#unique\\_11](#)

## 2.3 Anti-DDoS Premium

Alibaba Cloud provides Anti-DDoS Premium to protect against DDoS attacks for servers deployed outside mainland China.

After you set up an Anti-DDoS Premium instance to protect your services, Anti-DDoS Premium forwards all attack traffic directed toward your servers to a dedicated IP address. Anti-DDoS Premium relies on the state of the art distributed near-origin traffic scrubbing to scrub malicious traffic and forward normal traffic to origin servers. This ensures the stability of your services.

## Features

The following table describes the features provided by Anti-DDoS Premium.

Feature	Description
Malformed packet filtering	Anti-DDoS Premium protects your services against attacks, such as frag flood, smurf, stream flood, and land flood attacks , and filters out malformed packets, such as IP packets, TCP packets, and UDP packets.
Protection against transport-layer DDoS attacks	Anti-DDoS Premium protects your services against attacks, such as SYN flood, ACK flood, UDP flood, ICMP flood, and RST flood.
Protection against web application DDoS attacks	Anti-DDoS Premium protects your services against HTTP GET flood, HTTP POST flood, and high-frequency attacks. It also supports user-defined rules for access control, such as specific HTTP header field, URIs, and host rules.

## Benefits

Anti-DDoS Premium provides the following benefits:

- Global near-origin traffic scrubbing

Anti-DDoS Premium uses the anycast mode and the traffic scrubbing centers of Alibaba Cloud around the world to forward DDoS attack traffic to the nearest traffic scrubbing center. It also supports backup and disaster recovery among multiple data centers.

- Unlimited protection

Different from Anti-DDoS Pro, Anti-DDoS Premium relies on global near-source scrubbing to provide unlimited and continuous protection.



### Notice:

If the attacks that target your services impact the infrastructure of anti-DDoS scrubbing centers, Alibaba Cloud reserves the right to throttle the traffic. Traffic throttling on your Anti-DDoS Premium instances may affect your services. For example, user traffic may also be throttled or even routed to a black hole.

- Dedicated IP resources

Anti-DDoS Premium provides a dedicated anycast IP address. Each IP address is isolated to avoid any impact on your services caused by DDoS attacks on other customers. This provides you with more secure anti-DDoS services.

- Security reports

Anti-DDoS Premium provides detailed traffic reports and attack prevention reports in real time. This provides you a clear view of your service security.

## Scenarios

The Internet connects operators in different regions to enable global users to establish connections with each other. However, the network access and ability to communicate vary with the policies of these operators. Therefore, you must select an appropriate DDoS protection solution based on your service requirements.

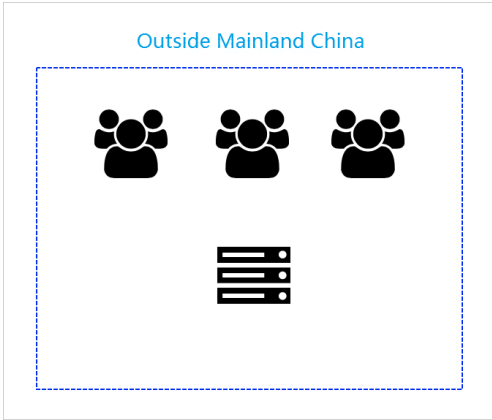


### Note:

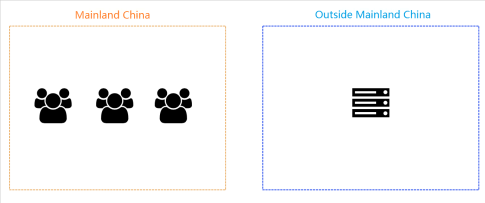
When customers in mainland China want to access Anti-DDoS Premium resources deployed outside mainland China, the network quality cannot be guaranteed if only Anti-DDoS Premium is enabled due to the current routing and interconnection strategies of network operators.

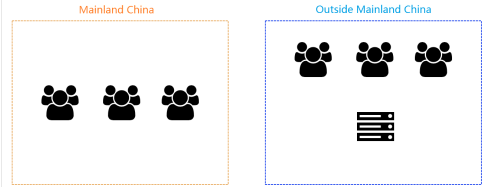
In this case, the average network latency reaches 300 ms, and intermittent packet loss caused by the congestion of international links may occur. Therefore, we recommend that you deploy servers in mainland China to serve users in mainland China, use Anti-DDoS Pro to protect against DDoS attacks, and comply with relevant China laws and regulations to complete website registration and other compliance procedures.

The following table describes the scenarios where servers are deployed outside mainland China.

Scenario	Solution
<p>Servers are deployed <b>outside mainland China</b> to serve users <b>outside mainland China</b>.</p> 	<p>Deploy Anti-DDoS Premium to protect against DDoS attacks.</p>



Scenario	Solution
<p>Servers are deployed <b>outside mainland China</b> to serve users in <b>mainland China</b>.</p>  <p>The diagram consists of two rectangular boxes. The left box is labeled 'Mainland China' in orange text at the top and contains three black icons of people. The right box is labeled 'Outside Mainland China' in blue text at the top and contains one black icon of a server rack.</p>	<ul style="list-style-type: none"><li>• Solution 1</li></ul> <p>If your services require a low network latency, such as that required for games, migrate your servers to mainland China where your users are located and deploy Anti-DDoS Pro to protect against DDoS attacks.</p> <ul style="list-style-type: none"><li>• Solution 2</li></ul> <p>If you do not plan to migrate your servers to mainland China, contact sales personnel or submit a ticket to purchase an Anti-DDoS Premium MCA instance. After you submit a ticket, technical support personnel can help you deploy the smart Anti-DDoS service that automatically switches between Anti-DDoS Pro or Anti-DDoS Premium and MCA. This guarantees smooth access for users in mainland China by using MCA if no attacks are detected. For more information about MCA configurations for Anti-DDoS Premium, see <a href="#">Configure Anti-DDoS Premium MCA</a>.</p>

Scenario	Solution
<p>Servers are deployed <b>outside mainland China</b> to serve users both <b>in mainland China</b> and <b>outside mainland China</b>.</p>  <p>The diagram illustrates two regions: 'Mainland China' (outlined in orange) and 'Outside Mainland China' (outlined in blue). In the 'Mainland China' region, there are three user icons. In the 'Outside Mainland China' region, there are three user icons and one server icon.</p>	<ul style="list-style-type: none"> <li>• <b>Solution 1</b> Deploy servers separately for mainland China and outside mainland China. Servers deployed in mainland China serve users in mainland China, and servers deployed outside mainland China serve users outside mainland China. Deploy both Anti-DDoS Pro and Anti-DDoS Premium to protect your services in and outside mainland China against DDoS attacks.</li> <li>• <b>Solution 2</b> If you do not plan to migrate your servers to mainland China, contact sales personnel or submit a ticket to purchase an Anti-DDoS Premium MCA instance. After you submit a ticket, technical support personnel can help you deploy the smart Anti-DDoS service that automatically switches between Anti-DDoS Pro or Anti-DDoS Premium and MCA. This guarantees smooth access for users in mainland China by using MCA if no attacks are detected. For more information about MCA configurations for Anti-DDoS Premium, see <a href="#">Configure Anti-DDoS Premium MCA</a>.</li> </ul>

## References

- [Anti-DDoS Premium billing method](#)
- [#unique\\_11](#)
- [Configure Anti-DDoS Premium MCA](#)

## 2.4 DDoS cost protection

Both Anti-DDoS Pro and Anti-DDoS Premium support DDoS cost protection. The service safeguards against the scaling of cost due to usage spikes on the protected Elastic Compute Service (ECS) instances or Server Load Balancer (SLB) instances caused by a DDoS

attack. If the costs of any protected resources increase due to DDoS attacks, you can submit a ticket to obtain a voucher.

## 3 Pricing

### 3.1 Anti-DDoS Pro billing method

This topic describes the billing methods, instance specifications, and expiration of Anti-DDoS Pro instances.



#### Basic protection (monthly subscription)

Basic protection bandwidth	Line	Price (standard function plan)	Price (enhanced function plan)
30 Gbit/s	Eight BGP lines	USD 3,120/month	USD 4,320/month
60 Gbit/s	Eight BGP lines	USD 7,020/month	USD 8,220/month
100 Gbit/s	Eight BGP lines	USD 49,230/year (discount price)	USD 63,630/year (discount price)
300 Gbit/s	Eight BGP lines	USD 79,260/year (discount price)	USD 93,660/year (discount price)
400 Gbit/s	Eight BGP lines	USD 145,300/year (discount price)	USD 159,700/year (discount price)
500 Gbit/s	Eight BGP lines	USD 563,430/year (discount price)	USD 577,830/year (discount price)
600 Gbit/s	Eight BGP lines	USD 670,610/year (discount price)	USD 685,010/year (discount price)

**Note:**

- For more information about the differences between the standard and enhanced function plans, see [Function plan](#).
- If you need higher protection bandwidth, you can submit a ticket.

The following table shows the default specifications of Anti-DDoS Pro instances. If the default specifications cannot meet your service needs, you can upgrade the instance or scale up the specifications when you purchase instances.

Item	Description	Default value	Price for extra specifications
Ports	The number of TCP and UDP ports that the instance can protect.	50	Every 5 additional ports: USD 7.5/ month
Domains	The number of HTTP and HTTPS domain names that the instance can protect.	50 <div>  <b>Note:</b>            The domain names that you add to an instance can belong to no more than five top-level domain names.         </div>	<ul style="list-style-type: none"> <li>Standard function plan : USD 4.5 per month for every 10 additional domain names</li> <li>Enhanced function plan : USD 7.5 per month for every 10 additional domain names</li> </ul> <div>  <b>Note:</b>            For every 10 additional domain names, the total number of supported top-level domain names increases by one.         </div>

Item	Description	Default value	Price for extra specifications
Clean Bandwidth	The maximum bandwidth of your services if no attacks are detected	100 Mbit/s	<ul style="list-style-type: none"> <li>100 Mbit/s &lt; Bandwidth ≤ 600 Mbit/s: You are charged USD 15 per Mbit/s for the bandwidth over the default bandwidth. The additional fees are added onto your regular monthly fee.</li> <li>600 Mbit/s &lt; Bandwidth ≤ 5,000 Mbit/s: You are charged USD 11 per Mbit/s for the bandwidth over 600 Mbit/s. The additional fees are added onto your regular monthly fee.</li> </ul>
QPS	The maximum number of HTTP and HTTPS requests that the instance can concurrently process per second if no attacks are detected.	3,000	Every 100 additional QPS: USD 1.5/month

**Note:**

- For more information about clean bandwidth, see [Clean bandwidth](#).
- For more information about domain names, see [Domains](#).

### Burstable protection (pay-as-you-go on a daily basis)

Burstable protection of Anti-DDoS Pro is provided to protect your services when the highest peak bandwidth of DDoS attacks exceeds the basic protection bandwidth. Burstable protection is charged based on the difference between the peak bandwidth of DDoS attacks and the basic protection bandwidth during a day.

**Note:**

If you set the burstable bandwidth and basic protection bandwidth to the same value, no additional fees are incurred but your Anti-DDoS Pro instance provides no burstable protection.

For example, the basic protection bandwidth of your Anti-DDoS Pro instance is 30 Gbit/s and the burstable bandwidth is 100 Gbit/s. Two DDoS attacks are launched at the instance on the same day. The peak bandwidths of the two DDoS attacks are 80 Gbit/s and 40 Gbit/s. Burstable protection is charged based on the higher peak bandwidth (80 Gbit/s). The difference between the peak bandwidth and basic protection bandwidth (30 Gbit/s) is 50 Gbit/s. Based on the price tier table in the following table, Anti-DDoS Pro charges USD 960 for burstable protection.

**Note:**

- No fees are incurred for burstable protection if the highest peak bandwidth of DDoS attacks in a day is lower than the basic protection bandwidth.
- No fees are incurred for burstable protection if the highest peak bandwidth of DDoS attacks on the current day is higher than the burstable bandwidth. Therefore, if the domain names protected by an Anti-DDoS Pro instance enter the black hole state, no additional fees are incurred.
- Bill statements for the burstable protection of a day are generated between 8:00 to 9:00 the next day.

Bandwidth difference	Price
0 Gbit/s < Bandwidth difference ≤ 5 Gbit/s	USD 120/day
5 Gbit/s < Bandwidth difference ≤ 10 Gbit/s	USD 180/day
10 Gbit/s < Bandwidth difference ≤ 20 Gbit/s	USD 330/day

Bandwidth difference	Price
20 Gbit/s < Bandwidth difference ≤ 30 Gbit/s	USD 540/day
30 Gbit/s < Bandwidth difference ≤ 40 Gbit/s	USD 730/day
40 Gbit/s < Bandwidth difference ≤ 50 Gbit/s	USD 960/day
50 Gbit/s < Bandwidth difference ≤ 60 Gbit/s	USD 1,170/day
60 Gbit/s < Bandwidth difference ≤ 70 Gbit/s	USD 1,380/day
70 Gbit/s < Bandwidth difference ≤ 80 Gbit/s	USD 1,590/day
80 Gbit/s < Bandwidth difference ≤ 100 Gbit/s	USD 1,770/day
100 Gbit/s < Bandwidth difference ≤ 150 Gbit/s	USD 2,190/day
150 Gbit/s < Bandwidth difference ≤ 200 Gbit/s	USD 3,240/day
200 Gbit/s < Bandwidth difference ≤ 300 Gbit/s	USD 4,200/day
300 Gbit/s < Bandwidth difference ≤ 400 Gbit/s	USD 6,000/day
400 Gbit/s < Bandwidth difference ≤ 500 Gbit/s	USD 7,510/day
500 Gbit/s < Bandwidth difference ≤ 600 Gbit/s	USD 9,010/day
600 Gbit/s < Bandwidth difference ≤ 700 Gbit/s	USD 10,510/day
700 Gbit/s < Bandwidth difference ≤ 800 Gbit/s	USD 12,010/day
800 Gbit/s < Bandwidth difference ≤ 900 Gbit/s	USD 13,510/day
900 Gbit/s < Bandwidth difference ≤ 1,000 Gbit/s	USD 15,010/day
1,000 Gbit/s < Bandwidth difference ≤ 1,100 Gbit/s	USD 16,510/day
1,100 Gbit/s < Bandwidth difference ≤ 1,200 Gbit/s	USD 18,010/day
1,200 Gbit/s < Bandwidth difference ≤ 1,300 Gbit/s	USD 19,510/day



Bandwidth difference	Price
1,300 Gbit/s < Bandwidth difference ≤ 1,400 Gbit/s	USD 21,010/day
1,400 Gbit/s < Bandwidth difference ≤ 1,500 Gbit/s	USD 22,520/day

## Refunding

The subscription fees paid for your Anti-DDoS Pro instances are non-refundable.

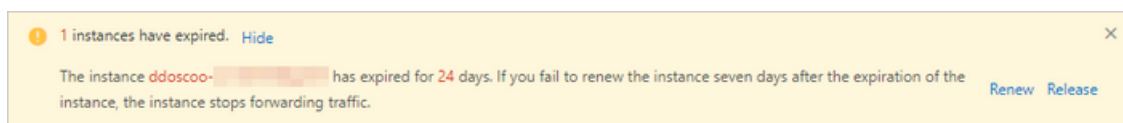
## Instance expiration

- When an Anti-DDoS Pro instance expires, the protection bandwidth immediately reduces to 5 Gbit/s and burstable protection becomes unavailable. However, Anti-DDoS Pro still forwards your traffic for **seven days** after the expiration.
- Seven days after the expiration**, the instance stops forwarding traffic.
  - After you renew an instance, it continues to forward traffic, and Anti-DDoS Pro is available.
  - Alibaba Cloud reclaims instance resources regularly. If you do not renew the instance within seven days after it expires, the instance may be automatically released.



### Note:

Your services may be interrupted if Anti-DDoS Pro stops forwarding traffic. We recommend that you read the notifications on instance expiration and renew instances as soon as possible or enable automatic renewal.



- Alibaba Cloud sends you notifications through SMS, emails, and internal messages when an instance is about to expire, expires, and is to be released.
  - You receive a notification seven, three, and one day before your instance expires to remind you of instance expiration and renewals.
  - After your instance expires, Alibaba Cloud notifies you that your instance is still available for seven days. If you want to renew it within seven days, you must renew it promptly.
  - If you do not renew your instance within seven days after it expires, Alibaba Cloud notifies you that the instance has stopped forwarding traffic.

## 3.2 Anti-DDoS Premium

### 3.2.1 Anti-DDoS Premium billing method

This topic describes the billing methods, instance specifications, and expiration of Anti-DDoS Premium instances.

#### Advanced protection with unlimited capabilities

The advanced protection of Anti-DDoS Premium integrates all protection capacities of anti-DDoS scrubbing centers of Alibaba Cloud from around the world to protect against DDoS attacks for your service security.

Services protected by Anti-DDoS Premium are less likely to be attacked. Attackers launch DDoS attacks to cause financial loss to the target services. Due to the cost of resources to launch DDoS attacks, attackers stop DDoS attacks if they continuously fail. The advanced protection of Anti-DDoS Premium provides unlimited protection and integrates all protection capacities of anti-DDoS scrubbing centers of Alibaba Cloud from around the world to secure your services.



#### Notice:

If the attacks that target your services impact the infrastructure of anti-DDoS scrubbing centers, Alibaba Cloud reserves the right to throttle the traffic. Traffic throttling on your Anti-DDoS Premium instances may affect your services. For example, user traffic may also be throttled or even routed to a black hole.

#### Mitigation plan

Anti-DDoS Premium provides **Insurance** and **Unlimited** mitigation plans.

- **Insurance**

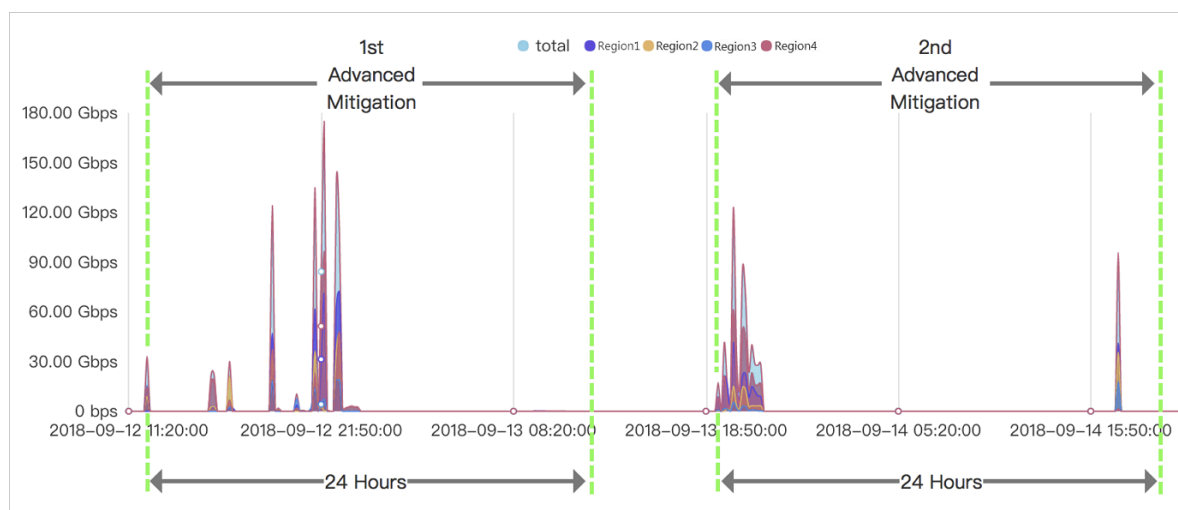
Each month, Anti-DDoS Premium Insurance Plan offers two free advanced protection sessions with unlimited protection capabilities. If your services suffer a volumetric DDoS attack, Anti-DDoS Premium provides unlimited protection capabilities to protect your services for the following 24 hours. This consumes one protection session. The number of advanced protection sessions is reset to two at the beginning of every month during the service period.



#### Note:

You can purchase more sessions of global advanced mitigation as required. For more information, see [Scenarios](#).

For example, a protected IP address suffers a volumetric DDoS attack at 11:20:00 (UTC +8), September 12, 2019, and an advanced protection is triggered. Anti-DDoS Premium provides unlimited protection capabilities to protect this IP address for the following 24 hours. Then, the IP address suffers another volumetric DDoS attack at 18:50:00 (UTC+8), September 13, 2019, and an advanced protection is triggered again. After 24 hours, the advanced protection stops. The two advanced protection sessions of Anti-DDoS Premium Insurance Plan for September are exhausted. The number of advanced protection sessions is automatically reset to two at the beginning of the following month, which in the case of the preceding example is October 1, 2019.



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

- **Unlimited**

Anti-DDoS Premium Unlimited Plan provides advanced protection with unlimited sessions and capabilities for your services. If you purchase the unlimited mitigation plan, Anti-DDoS Premium provides unlimited protection sessions to protect your services against DDoS attacks.

## Pricing

The following table lists the prices for different Anti-DDoS Premium specifications.

Mitigation plan	Clean bandwidth	Advanced protection	Price
Insurance	100 Mbit/s	Two sessions/month	USD 2,630/month

Mitigation plan	Clean bandwidth	Advanced protection	Price
Unlimited		Unlimited	USD 11,560/month
Insurance	150 Mbit/s	Two sessions/month	USD 3,420/month
Unlimited		Unlimited	USD 12,610/month
Insurance	200 Mbit/s	Two sessions/month	USD 4,210/month
Unlimited		Unlimited	USD 13,660/month
Insurance	250 Mbit/s	Two sessions/month	USD 5,000/month
Unlimited		Unlimited	USD 14,720/month
Insurance	300 Mbit/s	Two sessions/month	USD 5,570/month
Unlimited		Unlimited	USD 15,770/month

**Note:**



Clean bandwidth refers to the maximum bandwidth that an Anti-DDoS Premium instance can use to handle services if no attacks are detected. The clean bandwidth of an instance must be greater than the highest peak bandwidth of the inbound and outbound traffic of the services that you plan to run on the instance. If the actual bandwidth exceeds the clean bandwidth that the instance can handle, traffic throttling and random packet loss may occur. This may make your services unavailable or slow for a period of time.

For more information about the clean bandwidth and how to select appropriate clean bandwidth, see [Clean bandwidth](#).

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

The following table describes the default specifications of Anti-DDoS Premium instances. If the default specifications cannot meet your service needs, you can upgrade instance or scale up the specifications when you purchase instances.

Item	Description	Default value	Price for extra specifications
Ports	The number of TCP and UDP ports that the instance can protect.	5	Every five additional ports: USD 150/month

Item	Description	Default value	Price for extra specifications
Domains	The number of HTTP and HTTPS domain names that the instance can protect.	10  <b>Note:</b> Only one top-level domain can be added. The domain names that you add to an instance must belong to the same top-level domain name.	<ul style="list-style-type: none"> <li>Standard function plan : USD 45 per month for every 10 additional domain names</li> <li>Enhanced function plan : USD 75 per month for every 10 additional domain names</li> </ul>  <b>Note:</b> For every 10 additional domain names, the total number of supported top-level domain names increases by one.
QPS	The maximum number of HTTP and HTTPS requests that the instance can concurrently process per second if no attacks are detected.	<ul style="list-style-type: none"> <li>Insurance plan: 500</li> <li>Unlimited plan: 1,000</li> </ul>	Every 100 additional QPS: USD 150/month

**Note:**

For more information about domain names, see [Domains](#).

**Refunding**

The subscription fees paid for your Anti-DDoS Premium instances are non-refundable.

**Instance expiration**

- You receive SMS messages or emails 29, 27, 3, and 1 day before your instance expires to remind you of instance expiration and renewals.

- If you do not renew an instance after it expires, the instance provides only the default protection capability.
- After an instance expires, Anti-DDoS Premium retains the configurations for 30 days. If you renew the instance within a month, you can continue to use the instance. Otherwise, the instance is released and unavailable.

### 3.2.2 Mainland China Acceleration

Mainland China Acceleration (MCA) provides users in mainland China with low-latency access to servers deployed outside mainland China. This reduces response time if no attacks are detected. If your servers are deployed outside mainland China, you can purchase the MCA service for your Anti-DDoS Premium instances to accelerate access to your services for users in mainland China.

**Note:**

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

For more information about uses of MCA, see [Scenarios](#).

After you purchase MCA instances, you can use these instances with Anti-DDoS Premium Insurance or Unlimited Plan instances to accelerate access to your services for users in mainland China if no attacks are detected. For more information, see [Configure Anti-DDoS Premium MCA](#).

#### Pricing

The following table lists the prices for different MCA specifications.

Clean bandwidth	Price
10 Mbit/s	USD 1,548/month
20 Mbit/s	USD 3,096/month
30 Mbit/s	USD 4,643/month
40 Mbit/s	USD 6,191/month
50 Mbit/s	USD 7,739/month
60 Mbit/s	USD 9,287/month
70 Mbit/s	USD 10,834/month
80 Mbit/s	USD 12,382/month

Clean bandwidth	Price
90 Mbit/s	USD 13,930/month
100 Mbit/s	USD 15,478/month

**Note:**

Clean bandwidth refers to the maximum bandwidth that an MCA instance can use to handle services if no attacks are detected. The clean bandwidth of an MCA instance must be greater than the highest peak bandwidth of the inbound and outbound traffic of the services that you plan to run on the instance. If the actual bandwidth exceeds the clean bandwidth, traffic throttling and random packet loss may occur. This may cause your services to be unavailable, slow, or delayed for a period of time.

**Instance expiration**

- You will receive SMS messages or emails 29, 27, 3, and 1 day before your instance expires to remind you of instance expiration and renewals.
- If you do not renew your MCA instance after it expires, the MCA instance stops access acceleration.
- After your MCA instance expires, Anti-DDoS Premium retains the configurations for a month. If you renew the MCA instance within a month, you can continue to use the MCA instance. Otherwise, the MCA instance is released and becomes unavailable.

### 3.2.3 Global advanced mitigation


If the two advanced mitigation sessions for the month of an Anti-DDoS Premium Insurance Plan instance are used, you can purchase global advanced mitigation sessions to obtain unlimited protection capabilities.

**Context**

Each month, Anti-DDoS Premium Insurance Plan provides two free advanced mitigation sessions, which support unlimited protection capabilities. After a DDoS attack is detected, Anti-DDoS Premium Insurance Plan protects your services with unlimited capabilities in the following 24 hours. This consumes your quota of free advanced mitigation sessions.

If your services suffer frequent volumetric DDoS attacks, the two advanced mitigation sessions may fail to guarantee service availability. In this case, you can purchase global advanced mitigation sessions to provide unlimited protection capabilities for the Anti-DDoS Premium Insurance Plan instances under your account.

The following table describes the differences between global advanced mitigation and advanced mitigation of Anti-DDoS Premium instances.

Type	Scope	Validity period	Number of sessions
Advanced mitigation of Anti-DDoS Premium Unlimited Plan	Instance	Based on the validity period of instances	Unlimited
Advanced mitigation of Anti-DDoS Premium Insurance Plan	Instance	One month  <b>Note:</b> Advanced mitigation sessions that are not consumed in the current month are cleared at the beginning of next month.	Two sessions per month
Global advanced mitigation	Alibaba account	One year	Purchase as required

## Pricing

The following table shows the pricing of global advanced mitigation.

Item	Description
Payment type	Subscription
Validity period	One year
Unit price	USD 1,580



### Notice:

The fees paid for global advanced mitigation are non-refundable.

## Instructions

If the two free advanced mitigation sessions for the month are used up, but your services still suffer volumetric DDoS attacks that cause the traffic volume to exceed the basic protection bandwidth, the global advanced mitigation sessions that you purchased are consumed to provide unlimited protection capability.



You can use global advanced mitigation for all instances that meet the usage requirements without the need to connect the global advanced mitigation to a specific instance.

#### Usage requirements

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



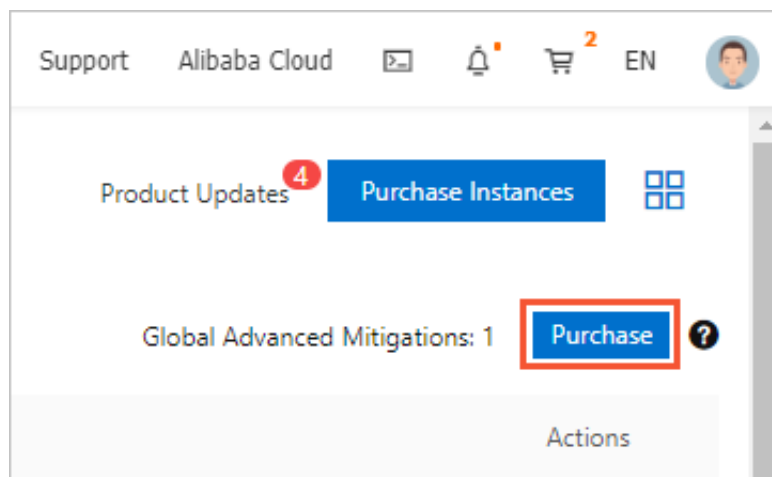
#### Note:

If the number of global advanced mitigation sessions consumed by all instances under your account in the current month exceeds 10, the advanced mitigation feature is automatically frozen. You must wait until the next calendar month to use this feature.

If your services suffer frequent volumetric DDoS attacks, we recommend that you purchase Anti-DDoS Premium Insurance Plan instances to protect your services.

### Purchase global advanced mitigation

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, click **Outside Mainland China**.
3. In the left-side navigation pane, choose **Assets > Instances**.
4. In the upper-right corner of the instance list, click **Purchase**.



5. On the **Anti-DDoS Global Advanced Mitigation** page that appears, set **Quantity** as required and click **Buy Now**.



#### Note:

Make sure that Product is set to **Anti-DDoS Premium**.

**Anti-DDoS Global Advanced Mitigation**

**Basic**

Product: **Anti-DDoS Premium**

Specification: **Region: Global**  
Condition: Anti-DDoS Premium Insurance instance is valid  
Valid Period: 1 years(No Refund)  
**Global Advanced Mitigation will be consumed after Advanced Mitigations in instance are exhausted**

Quantity: **1**

6. Complete the payment.

## 3.3 Instance specification

### 3.3.1 Function plan

Both Anti-DDoS Pro and Anti-DDoS Premium provide standard and enhanced function plans. The enhanced function plan provides the following features in addition to all the features of the standard function plan: static page caching, non-standard ports support, and blocked regions. These features enhance connection capabilities of instances and the ability of Anti-DDoS Pro and Anti-DDoS Premium to prevent DDoS attacks. You can select a mitigation plan as required.

When you purchase Anti-DDoS Pro or Anti-DDoS Premium instances, the standard function plan is selected by default. You can select the enhanced function plan to obtain advanced anti-DDoS protection. The price for each instance that uses the enhanced function plan is USD 1,145 per month.

For a purchased instance that uses the standard function plan, you can scale up the specification to obtain enhanced anti-DDoS protection. For more information, see [Upgrade the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance](#).



**Note:**


After you purchase an instance that uses the enhanced function plan or upgrade an instance to the enhanced function plan, you need to configure the domain names to enable the enhanced capabilities.


### Comparison of the standard and enhanced function plans

The following table describes feature differences between the standard and enhanced function plans.

Category	Feature	Description	Standard function plan	Enhanced function plan
Protection algorithm	Protection against volumetric DDoS attacks	Supports protection against volumetric DDoS attacks such as malformed packet attacks and flood attacks.	✓	✓
	Protection against resource exhaustion DDoS attacks	Supports protection against common HTTP flood attacks at the transport layer, such as HTTP GET floods and HTTP POST floods.  For more information, see <a href="#">Configure frequency control</a> .	✓	✓

Category	Feature	Description	Standard function plan	Enhanced function plan
	Intelligent protection	<ul style="list-style-type: none"> <li>• Supports intelligent protection against application-layer floods and mitigates HTTP flood attacks.</li> <li>• Supports intelligent protection against transport-layer floods and mitigates TCP flood attacks.</li> </ul> <p>For more information, see <a href="#">Configure intelligent protection</a>.</p>	✓	✓
Protection rule	Black lists and white lists	<p>A blacklist and whitelist for each protected domain name can each contain a maximum of 200 IP addresses.</p> <p>For more information, see <a href="#">Configure blacklists and whitelists for domain names</a>.</p>	✓	✓

Category	Feature	Description	Standard function plan	Enhanced function plan
	Accurate access control	Supports fine-grained access control based on HTTP.  For more information, see <a href="#">Configure accurate access control rules</a> .	For each protected domain name , you can configure a maximum of five rules based on the following fields: IP, URL , Referer, and User-Agent.	For each protected domain name , you can configure a maximum of 10 rules.
	Blocked regions	Blocks traffic based on geographic locations.  For more information, see <a href="#">Configure blocked regions for domain names</a> .	✗	✓
Connection methods	Standard HTTP ports (80 and 8080) and HTTPS ports (443 and 8443)	Supports anti-DDoS protections based on standard HTTP ports (80 and 8080) and HTTPS ports (443 and 8443).	✓	✓
	Non-standard HTTP and HTTPS ports	Supports DDoS prevention based on non-standard HTTP and HTTPS ports.   <b>Note:</b> For each instance, you can configure a maximum of 10 port forwarding rules that use non-standard ports.	✗	✓

Category	Feature	Description	Standard function plan	Enhanced function plan
Other	Static page caching	<p>Supports static page caching to reduce page loading time.</p> <div>  <b>Note:</b> Static page caching is in the public preview stage. For each protected domain name, you can configure a maximum of three rules. </div> <p>For more information, see <a href="#">Configure static page caching</a>.</p>	✗	✓

### 3.3.2 Clean bandwidth

This topic describes how to select an appropriate clean bandwidth when you purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

You can select an appropriate clean bandwidth based on the daily inbound and outbound traffic peaks of all existing and future services that you plan to run on the instance. Make sure that the clean bandwidth of the instance is greater than the highest peak bandwidth of the inbound and outbound traffic.



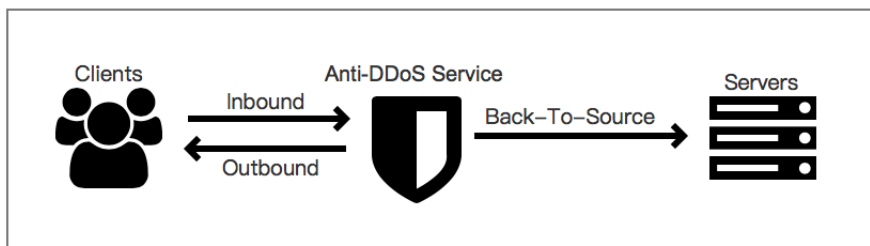
**Note:**

In most cases, the peak of the outbound traffic is greater than that of inbound traffic.

You can estimate the actual bandwidth based on the traffic statistics collected in the Elastic Compute Service (ECS) console or by using other monitoring tools on your origin server. The traffic described here refers to the normal traffic generated by your services.

Assume that you connect a website to an Anti-DDoS Pro or Anti-DDoS Premium instance for protection. If no attacks are launched at your website, Anti-DDoS Pro or Anti-DDoS Premium only needs to forward user traffic to the origin server. However, if your website is under attack, Anti-DDoS Pro or Anti-DDoS Premium blocks malicious traffic and forwards only user

traffic to the origin server. Therefore, the ECS console only displays statistics about inbound and outbound user traffic flows through the origin server. If your services are deployed on multiple origin servers, you must calculate the sum of the traffic volumes required by all origin servers.



Assume that you want to connect three websites to an Anti-DDoS Pro or Anti-DDoS Premium instance. The peak of the outbound user traffic on each website is 50 Mbit/s or lower. The total bandwidth required by the three websites is 150 Mbit/s or lower. In this case, set the clean bandwidth of the instance that you want to purchase to a value greater than 150 Mbit/s.

### 3.3.3 Domains

This topic describes how to determine the number of domain names you require when you purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

Every 10 additional domain names must belong to the same top-level domain name.

- An Anti-DDoS Pro instance can support 50 domain names, which belong to only five top-level domain names.
- An Anti-DDoS Premium instance can support 10 domain names, which belong to only one top-level domain name.

Assume that you want to purchase an Anti-DDoS Pro instance. The instance protects five top-level domain names, such as `abc.com`. Then you can add 50 subdomains and wildcard domains for the top-level domain names, such as `www.abc.com`, `*.abc.com`, `mail.abc.com`, `user.pay.abc.com`, and `x.y.z.abc.com`.

**Note:**

All added domain names, which include the top-level domain names, such as `abc.com`, count in the quota for protected domain names.

If you need to add more top-level domain names or the subdomains of a new top-level domain name, you must increase the maximum number of domain names. If you have

added five top-level domain names or the subdomains of five different top-level domain names, and you want to add a new top-level domain name or a subdomain of a new top-level domain name, a notification appears to remind you of increasing the number of domain names.

In this case, you must upgrade your instance to support additional domain names.




## 4 Quick Start

### 4.1 Set up Anti-DDoS Pro using domains

#### 4.1.1 Overview

This topic describes how to configure and use Anti-DDoS Pro or Anti-DDoS Premium to protect website services.

The following table describes the required steps.

Operation	Description
<a href="#">Step 1: Add forwarding rules</a>	In the Anti-DDoS Pro or Anti-DDoS Premium console, add a website service that you want to protect by using a domain name, associate the service with an Anti-DDoS Pro or Anti-DDoS Premium instance, and configure the traffic forwarding rules.
<a href="#">Step 2: Configure service traffic forwarding</a>	Modify the DNS records of your domain name to reroute the traffic directed to your website to an Anti-DDoS Pro or Anti-DDoS Premium instance. The instance scrubs the traffic and then forwards the traffic to the origin server, which protects your website service against DDoS attacks.
<a href="#">Step 3: Configure protection policies</a>	After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service, Intelligent Protection is enabled automatically. You can manually adjust anti-DDoS protection policies for your website service, which include Intelligent Protection, Black Lists and White Lists (Domain Names), Blocked Regions (Domain Names), Accurate Access Control, and Frequency Control.
<a href="#">Step 4: View the protection data of your website services</a>	<p>After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service, you can use the Security Reports feature and log-related features to view the protection data in the Anti-DDoS Pro or Anti-DDoS Premium console.</p> <div> <b>Note:</b> Only Anti-DDoS Pro supports the Security Reports and Operation Logs features.</div>

## 4.1.2 Step 1: Add forwarding rules

To use Anti-DDoS Pro or Anti-DDoS Premium to protect your website service, you must first add the domain name you want to protect and then add a traffic forwarding rule in the Anti-DDoS Pro or Anti-DDoS Premium console.

### Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is available. For more information, see [Purchase Anti-DDoS Pro or Anti-DDoS Premium instances](#).

### Context



#### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

This topic uses Anti-DDoS Pro as an example to describe this specific operation. If you use Anti-DDoS Premium, see [Add a website](#).

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select **Mainland China**.
3. In the left-side navigation pane, choose **Provisioning > Website Config**.
4. On the **Website Config** page, click **Add Domain**.







#### Note:


You can also import website configurations in batches. For more information, see [Import multiple website configurations at a time](#).



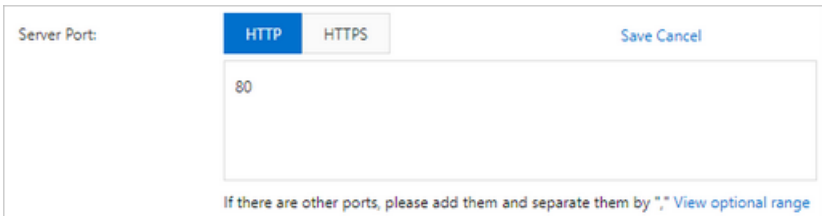

5. On the **Add Domain** wizard, set the parameters in the **Enter Site Information** step and click **Add**.

The screenshot shows the 'Add Domain' wizard with the 'Enter Site Information' step active. The 'Function Plan' is set to 'Standard'. The 'Instance' section shows 0 instances selected. The 'Domain' field is empty. The 'Protocol' section has 'HTTP' and 'HTTPS' checked. 'Enable HTTP/2' is disabled. The 'Server IP' section has 'Origin Server IP' selected. The 'Server Port' section shows 'HTTP 80' and 'HTTPS 443' selected. A green message box at the bottom states: 'If the IP addresses of your origin server have been exposed, click [here](#) to learn how to fix the issue.'

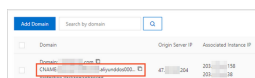
Parameter	Description
<b>Function Plan</b>	<p>The function plan of the instance that you want to use to protect the website. Valid values:</p> <ul style="list-style-type: none"> <li><b>Standard</b></li> <li><b>Enhanced</b></li> </ul> <div>  <b>Note:</b>  For more information, see <a href="#">Function plan</a>. </div>

Parameter	Description
<b>Instance</b>	<p>The instance that you want to use to protect the website. You can select up to eight instances for one domain name. The instances used to protect the same domain name must use the same function plan.</p> <div> <b>Note:</b> The available instances are displayed after you select a function plan. If no instance is available, no instance uses the selected function plan. In this case, you can purchase an instance or upgrade the standard function plan to the enhanced function plan. For more information, see <a href="#">Upgrade the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance</a>.</div>
<b>Domain</b>	<p>Enter the domain of the website that you want to protect.</p> <div> <b>Note:</b></div> <ul style="list-style-type: none"><li>• A domain name can contain letters, digits, and hyphens (-). It must start with a letter or digit. Domain names are not case sensitive.</li><li>• You can enter wildcard domains, such as *.aliyun.com. Anti-DDoS Pro or Anti-DDoS Premium protects the subdomains of wildcard domains.</li><li>• If you specify a domain name and its wildcard domain, such as www.aliyun.com and *.aliyun.com, the forwarding rules and protection policies configured for the domain name supersede those configured for the wildcard domain.</li></ul>
<b>Protocol</b>	<p>The protocols that the website supports. Valid values:</p> <ul style="list-style-type: none"><li>• <b>HTTP</b> (selected by default)</li><li>• <b>HTTPS</b> (selected by default)</li><li>• <b>Websocket</b></li><li>• <b>Websockets</b></li></ul> <div> <b>Note:</b> If your website supports HTTPS, you must select HTTPS. You can select other protocols that your website supports as required.</div>

Parameter	Description
<b>Enable HTTP/2</b>	<p>Specifies whether to enable HTTP 2.0 when the website is protected by an Anti-DDoS Pro instance that uses the enhanced function plan. After the feature is enabled, the protocol version is HTTP 2.0.</p> <div> <b>Note:</b> This feature is available only for Anti-DDoS Pro.</div>
<b>Server IP</b>	<p>The address type of the origin server. You must enter the address after you specify the address type. The address type can be <b>Origin Server IP</b> or <b>Origin Server Domain</b>.</p> <ul style="list-style-type: none"><li>• <b>Origin Server IP:</b> You can specify up to 20 IP addresses. If multiple IP addresses of an origin server are specified, Anti-DDoS Pro or Anti-DDoS Premium uses IP Hash load balancing to forward network traffic to the origin server.</li><li>• <b>Origin Server Domain:</b> If you want to use both Anti-DDoS Pro or Anti-DDoS Premium and web application firewall (WAF), select Origin Server Domain and enter the CNAME record provided by your WAF instance. This provides enhanced protection for your website.</li></ul>

Parameter	Description
<b>Server Port</b>	<p>The server port that is specified based on the selected protocol.</p> <div>  <b>Note:</b>            The forwarding port must be the same as the origin server port.         </div> <ul style="list-style-type: none"> <li>If <b>HTTP</b> or <b>Websocket</b> is selected, this parameter is set to 80 by default.</li> <li>If <b>HTTPS</b> or <b>Websockets</b> is selected, this parameter is set to 443 by default.</li> </ul> <div>  <b>Note:</b>            HTTP 2.0 ports are the same as HTTPS ports.         </div> <p>To add custom ports, you can click <b>Custom</b> and select ports other than the default ones.</p> <ul style="list-style-type: none"> <li>Instances that use the standard function plan support HTTP port 80, WebSocket port 8080, HTTPS port 443, and WebSockets port 8443.</li> <li>Instances that use the enhanced function plan support specific non-standard ports. For more information, see <a href="#">Specify non-standard ports for protection</a>.</li> </ul> <div>  </div>
<b>CNAME Reuse</b>	<p>Specifies whether to enable CNAME reuse. After CNAME reuse is enabled, you can associate the domain names hosted by the same server with the CNAME record assigned by Anti-DDoS Premium. For more information, see <a href="#">CNAME reuse</a>.</p> <div>  <b>Note:</b>            This feature is available only for Anti-DDoS Premium.         </div>

After you add a website, click **Website List**. Then, you can view the added website configuration and its CNAME record on the Website Config page.



## Result

Anti-DDoS Pro assigns a CNAME record to the domain name. You only need to map the DNS record of the domain name to the CNAME record of the Anti-DDoS Pro instance to reroute inbound traffic to the instance for traffic scrubbing.

## What's next

- Configure service traffic forwarding. For more information, see [Step 2: Configure service traffic forwarding](#).
- [Upload an SSL certificate](#). If your website supports the HTTPS protocol, you must upload your SSL certificate to enable the Anti-DDoS Pro instance to filter HTTPS requests.

### 4.1.3 Step 2: Configure service traffic forwarding

After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service by using a domain name, you must modify the DNS records of the domain name to reroute the traffic directed to your website to the instance. The instance scrubs the traffic and then forwards the traffic to the origin server. This topic describes how to modify the CNAME record of a domain name. In this example, the DNS resolution service is provided by Alibaba Cloud DNS.

## Prerequisites

- An Anti-DDoS Pro or Anti-DDoS Premium instance is set up by using a domain name. For more information, see [Step 1: Add forwarding rules](#).
- The back-to-origin IP addresses of instances are added to the whitelist of the origin server. If you deploy third-party security software on your origin server, such as a firewall, add the back-to-origin IP addresses to the whitelist of the security software. For more information, see [Allow back-to-origin IP addresses to access the origin server](#).
- The traffic forwarding settings take effect. Before you switch service traffic to Anti-DDoS Pro or Anti-DDoS Premium, we recommend that you verify that the instances can forward inbound traffic to the origin server on your local machine. For more information, see [Verify the forwarding configuration on your local machine](#).

## Context

In the following example, the domain name is managed by [Alibaba Cloud DNS](#).



### Note:

Alibaba Cloud DNS provides basic DNS services for free and offers other value-added services in the paid edition. If you activated the value-added services of Alibaba Cloud

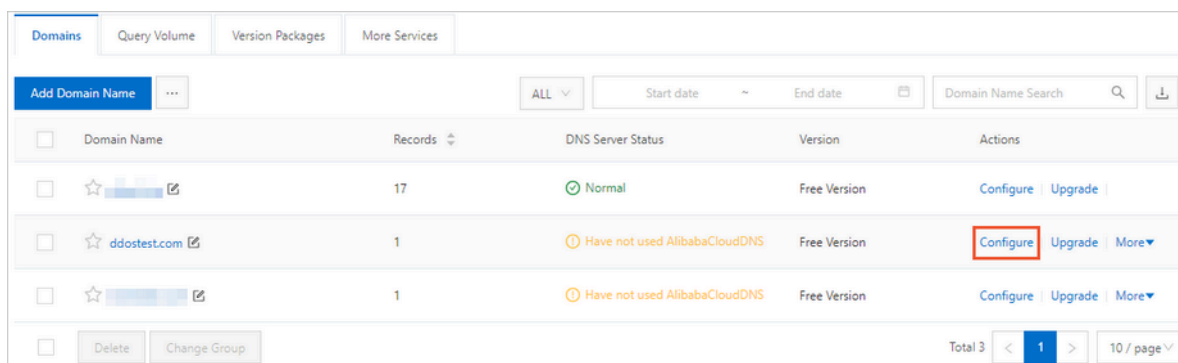
DNS in the paid edition for your website, we recommend that you enable NS Mode Access to reroute traffic to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Enable NS Mode Access to protect a website](#).

If you use third-party DNS services, log on to the system of the DNS provider to modify the DNS records. The following example is for reference only.

Assume that the domain name of your website associated with an instance is `bgp.ddostest.com`. The following procedure describes how to modify and add DNS records in the Alibaba Cloud DNS console.

#### Procedure

1. Log on to the [Alibaba Cloud DNS console](#).
2. On the **Manage DNS** page, find the domain name `ddostest.com` and click **Configure** in the Actions column.



Domains	Query Volume	Version Packages	More Services
<a href="#">Add Domain Name</a>	...	ALL	Start date ~ End date
Domain Name	Records	DNS Server Status	Version
<input type="checkbox"/> [domain]	17	Normal	Free Version
<input type="checkbox"/> ddostest.com	1	Have not used AlibabaCloudDNS	Free Version
<input type="checkbox"/> [domain]	1	Have not used AlibabaCloudDNS	Free Version
Total 3 < 1 > 10 / page			

3. On the **DNS Settings** page, find the A record or CNAME record whose Host is `bgp` and click **Edit** in the Actions column.



#### Note:

If you cannot find the DNS record that you want to manage in the list, you can click **Add Record** to add the record.

Add Record

Import & Export

Query Volume

Getting Started

ALL

Exact Search

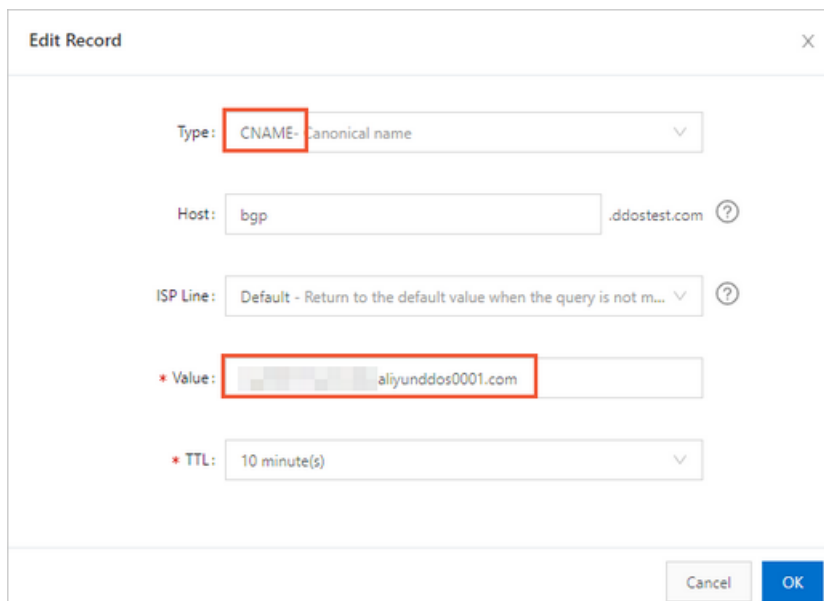
Search by keyword.

Advanced Search

<input type="checkbox"/>	Host	Type	Line(ISP)	Value	TTL	Status	Remark	Actions
<input type="checkbox"/>		CNAME	Default		aliyunddos0001.com	10 minute(s)	Normal	<div><div>Edit</div><div>Disable</div><div>Delete</div><div>Remark</div></div>
<input type="checkbox"/>	<div><div>Disable</div><div>Enable</div><div>Delete</div><div>Change Group</div></div>				Total 1 < 1 > 10 / page			



4. In the **Edit Record** or **Add Record** dialog box, set **Type** to **CNAME** and change **Value** to the CNAME record assigned by Anti-DDoS Pro or Anti-DDoS Premium.



5. Click **OK** and wait for the settings to take effect.

## What's next

[Step 3: Configure protection policies](#)

### 4.1.4 Step 3: Configure protection policies

After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service, Intelligent Protection is enabled automatically. You can manually adjust anti-DDoS protection policies for your website service, which include Intelligent Protection, Black Lists and White Lists (Domain Names), Blocked Regions (Domain Names), Accurate Access Control, and Frequency Control.

#### Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is set up by using a domain name. For more information, see [Step 1: Add forwarding rules](#).

#### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning** > **Website Config**.

4. On the **Website Config** page, find the target domain name and click **Mitigation Settings** in the Actions column.

Add Domain		Search by domain		Q			
<input type="checkbox"/>	Domain	Origin Server IP	Associated Instance IP	Protocol	Certificate Status	Protection Settings	Actions
<input type="checkbox"/>	Domain: .com CNAME: aliyunddos000... Protection Package: Enhanced	2.2	203.38	http port:80,7012,7013 https port:443	No Certificate TLS Security Settings	HTTP Flood Protection: Normal	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Configure DNS Settings</a> <a href="#">Protection Settings</a>

5. On the **Protection for Website Services** tab, configure protection policies for the domain name. Supported protection policies include Intelligent Protection, Black Lists and White Lists (Domain Names), Blocked Regions (Domain Names), Accurate Access Control, and Frequency Control.

Protection for Infrastructure
Protection for Website Services
Protection for Non-website Services

Enter

Intelligent Protection

With adaptive learning about a business traffic baseline, the intelligent analysis engine for big data helps you identify and block next-generation CC attacks. When traffic becomes abnormal, the engine dynamically changes the protection policies of each function module to block abnormal request. These decisions are all based on the distribution of historical traffic. The Protection mode is set to Normal and enabled by default.

Pending Enable Modify

Black Lists and White Lists (Domain Names)

Allow or deny IP requests.

Status You have created 200 blacklists and 200 whitelists. Change Settings

Blocked Regions (Domain Names)

Check the source IP address and block traffic based upon geographical location.

Status You have blocked 34 Chinese provincial regions and 1 international regions. Change Settings

Accurate Access Control

Add a combination of conditions to a policy as the protection policy for common HTTP fields.

Status You have set 10 access control rules. Change Settings

Frequency Control

Control access from source IP address by using the frequency

Status

Preset Mode Normal Emergency Strict Super Strict

Custom Rule Currently, you have created 3 rules. Change Settings

- **Intelligent Protection:** It is enabled by default. Intelligent Protection enables the intelligent and big data-based analysis engine to learn the traffic patterns of workloads, detect and block new types of HTTP flood attacks, and dynamically adjust policies to block malicious requests. You can manually change the protection mode and level. For more information, see [Configure intelligent protection](#).
- **Black Lists and White Lists (Domain Names):** After this policy is enabled, access requests from the IP addresses or CIDR blocks in the blacklist are blocked, while access requests from the IP addresses or CIDR blocks in the whitelist are allowed. For more information, see [Configure blacklists and whitelists for domain names](#).
- **Blocked Regions (Domain Names):** You can specify both the regions inside and outside China that you want to block. Requests from IP addresses in the blocked

regions are blocked. For more information, see [Configure blocked regions for domain names](#).

- **Accurate Access Control:** allows you to customize access control rules. You can filter access requests based on a combination of criteria of commonly used HTTP fields, such as IP, URI, Referer, User-Agent, and Params. For requests that meet these criteria, you can allow, block, or verify them. For more information, see [Configure accurate access control rules](#).
- **Frequency Control:** allows you to restrict the frequency of access from a source IP address to your website. Frequency Control takes effect immediately after it is enabled. By default, the normal mode is used to protect website services against common HTTP flood attacks. You can manually change the protection mode and create custom rules to reinforce protection. For more information, see [Configure frequency control](#).

### 4.1.5 Step 4: View the protection data of your website services

After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service, you can use the Security Reports feature and log-related features to view the protection data in the Anti-DDoS Pro or Anti-DDoS Premium console.

#### Prerequisites

- An Anti-DDoS Pro or Anti-DDoS Premium instance is set up by using a domain name. For more information, see [Step 1: Add forwarding rules](#).
- The traffic forwarding configuration for your website service is complete. For more information, see [Step 2: Configure service traffic forwarding](#).

#### Context

Only Anti-DDoS Pro supports the Security Reports and Operation Logs features. This topic takes Anti-DDoS Pro as an example to describe the features. If you use Anti-DDoS Premium, we recommend that you view service protection on the Security Overview and Log Analysis pages. For more information, see [Check security overview](#) and [Full log](#).

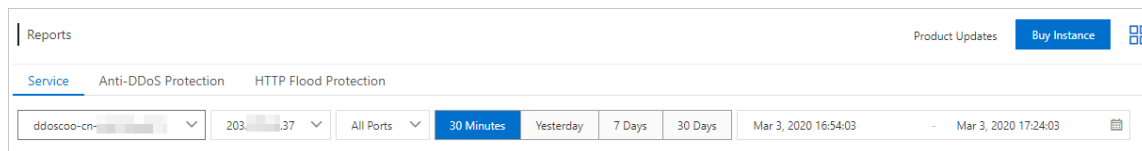
#### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select **Mainland China**.

### 3. Perform the following steps based on your needs:

- View security reports

In the left-side navigation pane, click **Security Reports**. On the **Reports** page, click one of the following tabs to view the relevant reports: **Service**, **Anti-DDoS Protection**, and **HTTP Flood Protection**.



You can add multiple filter conditions to customize the reports. For example, you can filter reports by time range, Anti-DDoS Pro instance, instance IP address, or port. The following table describes the differences between these reports.

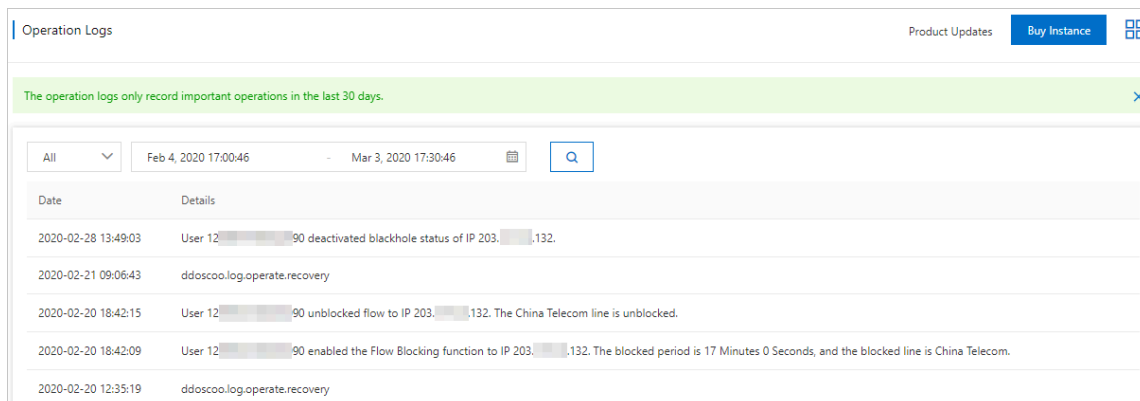
Report	Content	Filter condition
Service	<ul style="list-style-type: none"> <li>Changes of inbound and outbound bandwidth</li> <li>Changes of concurrent connections and new connections</li> </ul>	<ul style="list-style-type: none"> <li>Time range</li> <li>Anti-DDoS Pro instance</li> <li>IP address of the Anti-DDoS Pro instance</li> <li>Forwarding port</li> </ul>
Anti-DDoS Protection	<ul style="list-style-type: none"> <li>Changes of back-to-origin traffic and scrubbed traffic</li> <li>DDoS attack records</li> </ul>	<ul style="list-style-type: none"> <li>Time range</li> <li>Anti-DDoS Pro instance</li> <li>IP address of the Anti-DDoS Pro instance</li> </ul>
HTTP Flood Protection	<ul style="list-style-type: none"> <li>Changes of malicious requests and total requests per second</li> <li>Records of HTTP flood attacks</li> </ul>	<ul style="list-style-type: none"> <li>Time range</li> <li>Domain name</li> </ul>

For more information, see [View security reports](#).

- Query and analyze log data

In the left-side navigation pane, choose **Investigation > Operation Logs**. On the **Operation Logs** page, view operations log. An operations log records important operations in the last 30 days. For example, this log records the operations performed

on IP addresses of protected assets and ECS instances. You can filter the logs by time range.



Date	Details
2020-02-28 13:49:03	User 1234567890 deactivated blackhole status of IP 203.113.2.
2020-02-21 09:06:43	ddoscoo.log.operate.recovery
2020-02-20 18:42:15	User 1234567890 unblocked flow to IP 203.113.2. The China Telecom line is unblocked.
2020-02-20 18:42:09	User 1234567890 enabled the Flow Blocking function to IP 203.113.2. The blocked period is 17 Minutes 0 Seconds, and the blocked line is China Telecom.
2020-02-20 12:35:19	ddoscoo.log.operate.recovery

If you need to analyze log data in real time and display results by using graphs, we recommend that you activate the Log Analysis feature. After the Log Analysis feature is activated, the logs of access to your website and HTTP flood attack logs are collected and maintained by Alibaba Cloud Log Service. You can search and analyze log data in real time, and view search results on dashboards. For more information, see [#unique\\_48](#).

The Log Analysis feature is a value-added service. To use this service, you must both activate and enable it. Specifically, you must perform the following steps:

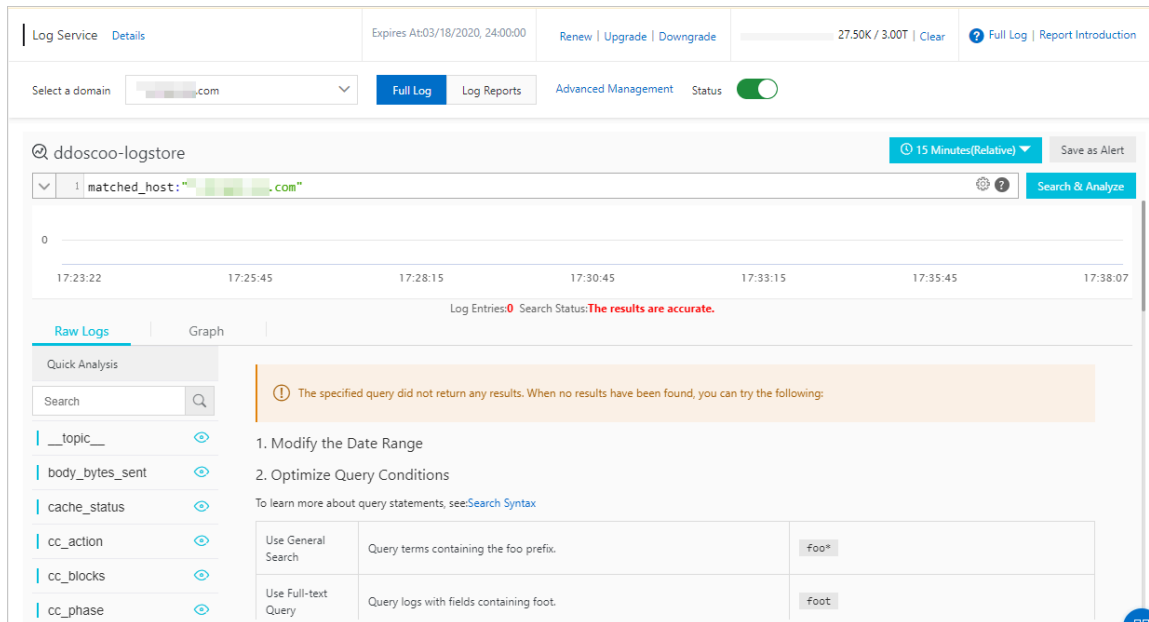
- a. Activate the feature. For more information, see [Activate the Log Analysis feature](#).
- b. Enable the feature. For more information, see [Enable the Log Analysis feature for a website](#).

After the Log Analysis feature is activated and enabled, you can navigate to the **Investigation > Log Analysis** page to search and analyze log data in real time. You can also view and edit dashboards, and configure monitoring and alerts on this page.



**Note:**

For more information about the fields supported by the Log Analysis feature, see [Fields supported by the Log Analysis feature](#).



## 4.2 Set up Anti-DDoS Pro using IPs and ports

### 4.2.1 Overview

This topic describes how to configure and use Anti-DDoS Pro or Anti-DDoS Premium to protect non-website services, such as client-based games, mobile games, or apps.

The following table describes the required steps.

Step	Description
<a href="#">Step 1: Create a port forwarding rule</a>	Add a non-website service that you want to protect by using a port in the Anti-DDoS Pro or Anti-DDoS Premium console. Use the IP address of your Anti-DDoS Pro or Anti-DDoS Premium instance as your service IP address to reroute inbound traffic to your instance. After you change the IP address, the instance scrubs the inbound traffic and then forwards the traffic to the origin server.
<a href="#">Step 2: Configure port forwarding and anti-DDoS protection policies</a>	Configure port forwarding policies as required, such as session persistence and health checks for multiple origin IP addresses. You can also configure anti-DDoS protection policies for non-website services, such as False Source, Speed Limit for Destination, Packet Length Limit, and Speed Limit for Source.

Step	Description
<a href="#">Step 3: View the protection data of a port</a>	View the traffic that goes through a port on the Security Overview page of the Anti-DDoS Pro or Anti-DDoS Premium console after you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your non-website service.

### 4.2.2 Step 1: Create a port forwarding rule

To use Anti-DDoS Pro or Anti-DDoS Premium to protect non-website services, such as client-based games, mobile games, or apps, you must create port forwarding rules and use the IP address of your Anti-DDoS Pro or Anti-DDoS Premium instance as the service IP address. This topic describes how to create a port forwarding rule in the Anti-DDoS Pro or Anti-DDoS Premium console.

#### Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is available. For more information, see [Purchase Anti-DDoS Pro or Anti-DDoS Premium instances](#).

#### Context



#### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

If you set up either Anti-DDoS Pro or Anti-DDoS Premium instances to protect non-website services, these instances only support Layer 4 forwarding. Both Anti-DDoS Pro and Anti-DDoS Premium only provide protection against Layer 4 attacks, such as SYN and UDP flood attacks. They do not parse Layer 7 packets or mitigate Layer 7 attacks, such as HTTP flood attacks and web attacks. To create an instance to protect non-website services, you only need to create port forwarding rules and use the IP address of your instance as the service IP address.

#### Procedure

1. Log on to the [Anti-DDoS Pro console](#).

2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.
4. On the **Port Config** page, select the target instance and click **Create Rule**.

Port Settings

Product Updates

Buy Instance

203.132

Forwarding Port

You can create a maximum of 50 rules. You have already created 6 rules.

Create Rule

	Forwarding Protocol	Forwarding Port	Origin Server Port	Forwarding Mode	Origin Server IP	Session Persistence	Health Check	Anti-DDoS Protection Policy	Actions
<input type="checkbox"/>	TCP	80	80	--	--	--	--	--	--
<input type="checkbox"/>	TCP	443	443	--	--	--	--	--	--

**Note:**

You can also create multiple rules at a time. For more information, see [Create multiple forwarding rules at a time](#).



5. In the **Create Rule** dialog box, specify the required parameters.

Create Rule

Note: if the port provides HTTP or HTTPS service, we recommend you to use the website configurations. This greatly improve the protection of the 7-layer HTTP flood attack for the HTTP or HTTPS service. The website configuration now supports adding non-standard ports. [Click to view supported non-standard ports](#)

\* Forwarding

☒ TCP ☐ UDP

Protocol:

\* Forwarding Port:

\* Origin Server

Port:

Forwarding Mode:

Round-robin


\* Origin Server IP:

Separate multiple IP addresses with commas (.). You can add a maximum of 20 IP addresses.

Complete

Cancel

Parameter	Description
<b>Forwarding Protocol</b>	The protocol that you want to use to forward traffic. Valid values: <b>TCP</b> and <b>UDP</b> .
<b>Forwarding Port</b>	<div>The port used by the instance to forward inbound traffic.</div> <ul style="list-style-type: none"><li>We recommend that you set the forwarding port to the port of the origin server.</li><li>To prevent domain owners from creating their own DNS servers with protection features, Anti-DDoS Pro and Anti-DDoS Premium do not protect the transport-layer services that use port 53.</li><li>You cannot specify a port that is already used as the forwarding port for another rule. In an instance, forwarding rules that use the same protocol must use different forwarding ports. If you attempt to create a rule with a protocol and forwarding port already used by another rule, an error message appears, indicating that rules overlap. Do not create a rule that overlaps with the forwarding rules that are automatically generated when a website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see <a href="#">Automatically generate forwarding rules for website services</a>.</li></ul>

Parameter	Description
Origin Server Port	The port of the origin server that you want to use to create the rule.
Origin Server IP	<div>The IP address of the origin server that you want to use to create the rule.</div> <div> <b>Note:</b> You can specify a maximum of 20 origin server IP addresses to implement load balancing. Separate multiple IP addresses with commas (,).</div>

6. Click **OK**.

After a port forwarding rule is created, you can configure session persistence, health checks, and anti-DDoS protection policies for non-website services as required. For more information, see [Step 2: Configure port forwarding and anti-DDoS protection policies](#).

You can also **edit** or **delete** a rule as required.

7. Change the IP address of the service that you want to protect to the IP address of your instance to reroute inbound traffic to the instance. After you change the IP address, the instance scrubs the inbound traffic and then forwards the traffic to the origin server.

Before you change the IP address to reroute inbound traffic to your instance, we recommend that you verify that the forwarding rule has taken effect. For more information, see [Verify the forwarding configuration on your local machine](#).



**Notice:**

If you change the service IP address before the forwarding rule takes effect, your service may be interrupted.

### 4.2.3 Step 2: Configure port forwarding and anti-DDoS protection policies

This topic describes how to configure port forwarding policies, such as session persistence and health checks for multiple origin IP addresses and how to configure anti-DDoS protection policies for non-website services, such as False Source, Speed Limit for Destination, Packet Length Limit, and Speed Limit for Source.

#### Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is set up by using a port. For more information, see [Step 1: Create a port forwarding rule](#).

## Context

You can configure port forwarding rules and anti-DDoS protection policies for non-website services as required to optimize the forwarding feature of Anti-DDoS Pro or Anti-DDoS Premium.

- You can configure a session persistence policy to forward requests from a specific IP address to the same backend server.
- You can configure a health check policy to check the availability of the backend servers, which ensures that requests from clients are forwarded to normal servers.
- You can configure anti-DDoS protection policies to limit the connection speeds and packet lengths of non-website services that are protected by Anti-DDoS Pro or Anti-DDoS Premium. This protects your non-website services against connection-oriented DDoS attacks that consume low bandwidth.

## Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.

4. On the **Port Config** page, select an instance, find the target forwarding rule, and configure the session persistence, health check, anti-DDoS protection policies for non-website services as required.

Anti-DDoS / Provisioning / Port Config

Port Config

Product Updates <sup>4</sup> Purchase Instances

You can create a maximum of 50 rules. You have already created 2 rules. Create Rule

<input type="checkbox"/>	Forwarding Protocol	Forwarding Port	Origin Server Port	Forwarding Mode	Origin Server IP	Session Persistence	Health Check	Anti-DDoS Protection Policy	Actions
<input type="checkbox"/>	TCP	80	80	--	--	--	--	--	--
<input type="checkbox"/>	TCP	443	443	--	--	--	--	--	--
<input type="checkbox"/>	TCP	5000	5000	Round-robin	30.137	Disabled Change	Disabled Change	Enabled Change	Edit Delete

- **Session Persistence**

- a. Click **Change** in the **Session Persistence** column.
- b. In the **Session Persistence** dialog box, enable or disable session persistence as required.

Session Persistence

\* Timeout Period: 900

The valid range is 30 to 3600.

[Disable Session Persistence](#)

Complete Cancel

- To enable session persistence, set the **Timeout Period** parameter and click **Complete**.
- To disable session persistence, click **Disable Session Persistence**.

- **Health Check**

- a. Click **Change** in the **Health Check** column.
- b. In the **Health Check** dialog box, configure health check settings. For more information about configuration items, see [Configure health check](#).

Health Check

Port: 456

Response Timeout: 1

Check Interval: 10

Unhealthy: 1

Healthy Timeout: 1

Complete Cancel

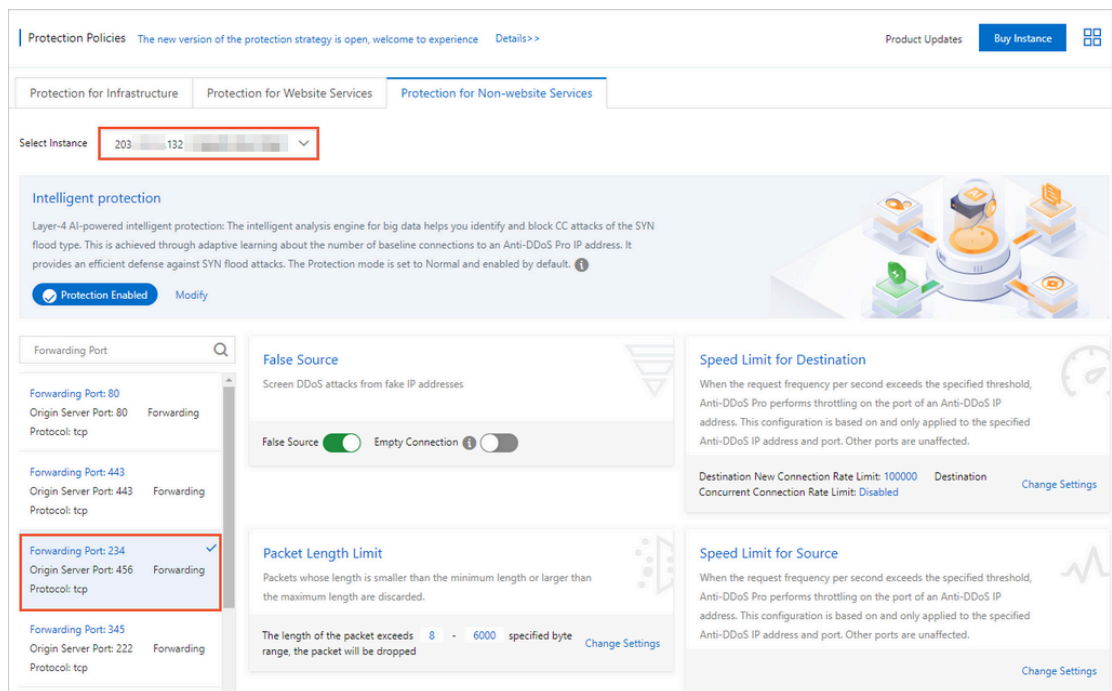
c. Click **Complete**.

To disable a health check, click **Change** in the Health Check column. In the **Health Check** dialog box, click **Disable Health Check**.

- Protection for non-website services

a. Click **Change** in the **Anti-DDoS Protection Policy** column.

- b. On the **Protection for Non-website Services** tab, configure anti-DDoS protection policies as required, which include False Source, Speed Limit for Destination, Packet Length Limit, and Speed Limit for Source.



- False Source: verifies and filters DDoS attacks initiated from forged IP addresses
- Speed Limit for Destination: The data transfer rate of the port used by the instance that exceeds the maximum visit frequency is limited based on the IP address and port of an Anti-DDoS Pro or Anti-DDoS Premium instance. The data transfer rates of other ports are not limited.
- Packet Length Limit: specifies the minimum and maximum lengths of packets that are allowed to pass through. Packets with invalid lengths are dropped.
- Speed Limit for Source: The data transfer rate of a source IP address from which access requests exceed the maximum visit frequency is limited based on the IP address and port of an Anti-DDoS Pro or Anti-DDoS Premium instance. The data transfer rates of source IP addresses from which access requests do not

exceed the maximum visit frequency are not limited. This policy also supports the IP address blacklist policy. An IP address from which access requests exceed the maximum visit frequency five times within 60 seconds can be added to a blacklist. You can also specify the blocking period.

For more information, see [Create an anti-DDoS protection policy](#).

### 4.2.4 Step 3: View the protection data of a port

After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your non-website services, you can view the traffic that goes through the port on the Security Overview page of the Anti-DDoS Pro or Anti-DDoS Premium console.

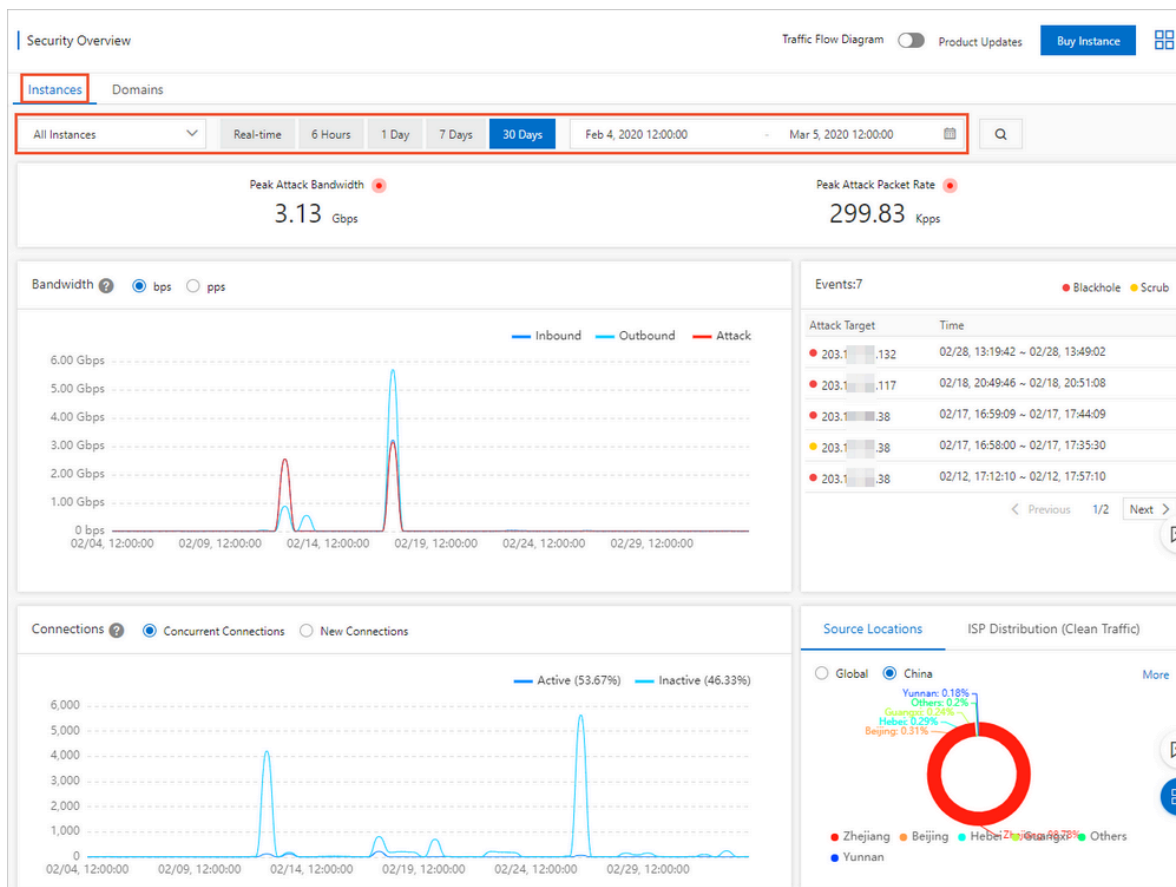
#### Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is set up by using a port. For more information, see [Step 1: Create a port forwarding rule](#).

#### Procedure

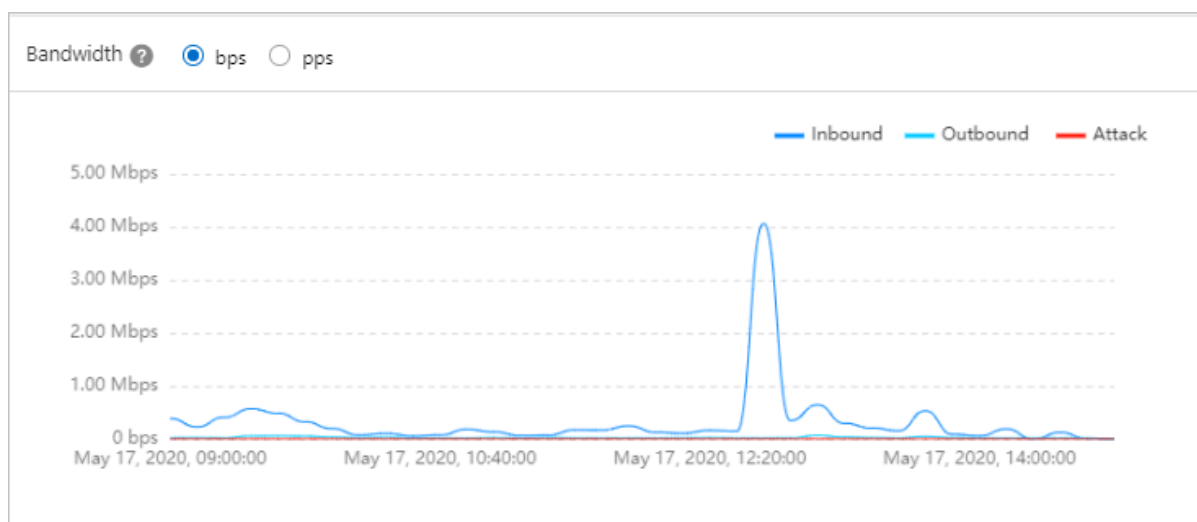
1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, click **Security Overview**.

4. Click the **Instances** tab, select one or more instances, and specify a time range to view the relevant metrics.

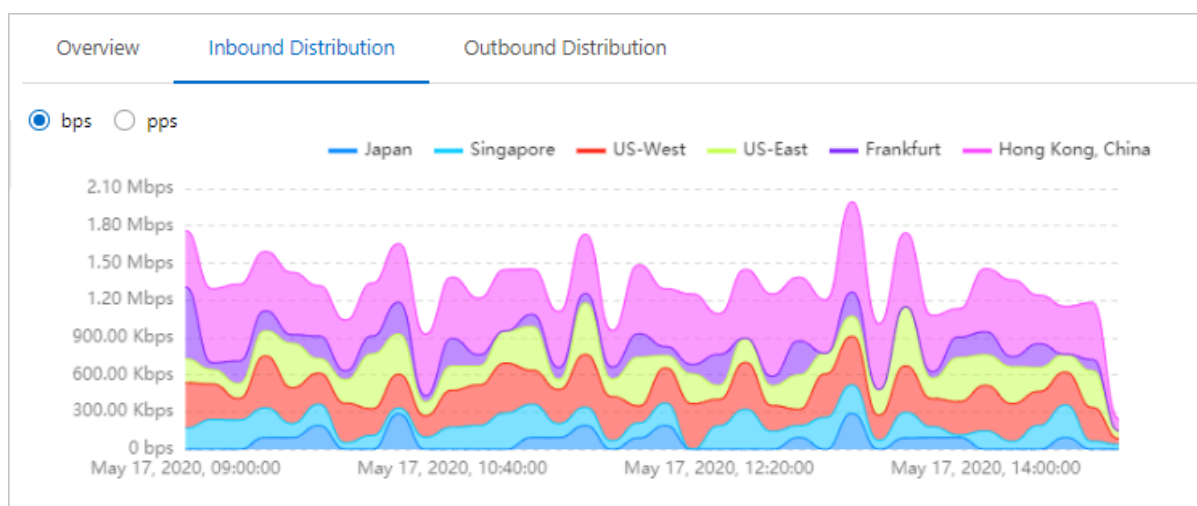


You can view the following instance information:

- **Peak Attack Bandwidth** and **Peak Attack Packet Rate**
- Traffic trends
  - The **Bandwidth** trend chart provided by Anti-DDoS Pro displays the traffic information by **bps** or **pps**. You can view the trends of inbound, outbound, and attack traffic of an instance for a specific period of time.



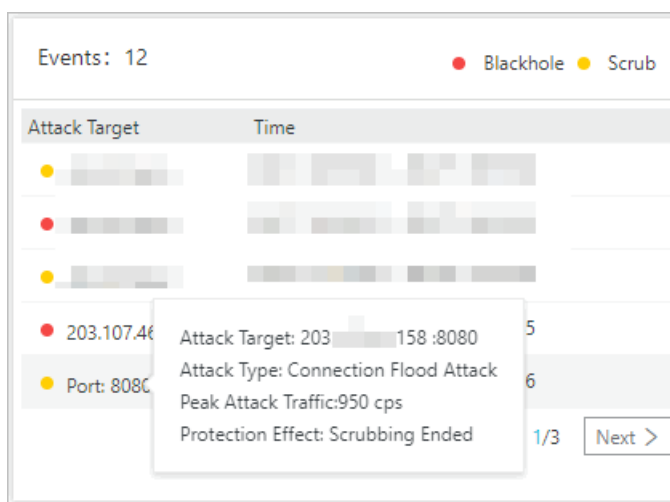
- Anti-DDoS Premium provides the following tabs to provide bandwidth trends, distribution of inbound traffic, and distribution of outbound traffic, respectively: **Overview, Inbound Distribution, and Outbound Distribution.**



- **Attack Events** of blackhole and mitigation

You can move the pointer over an IP address or a port to view the details of an attack, such as Attack Target, Attack Type, Peak Attack Traffic, and Protection Effect.



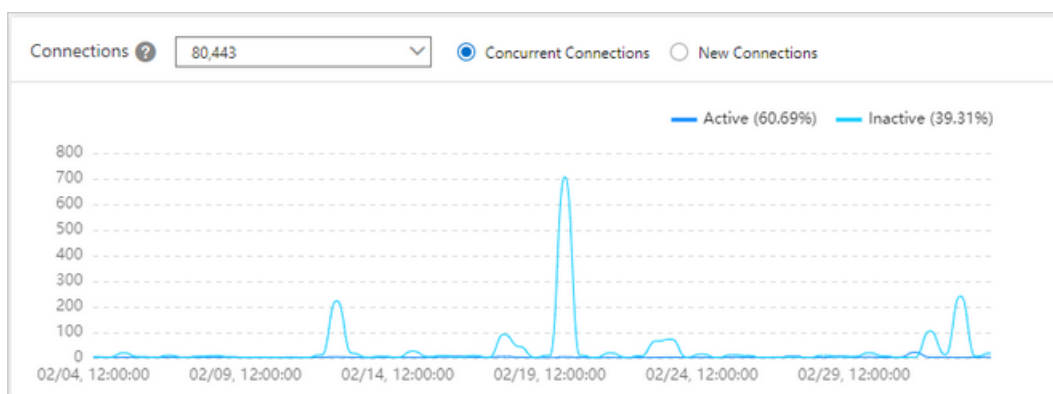


- **Connections** on a port
  - **Concurrent Connections:** the total number of concurrent TCP connections established between clients and the instance
  - **New Connections:** the number of new TCP connections established between clients and the instance per second



#### Note:

If you select an instance, the Connections chart displays the numbers of connections on different ports. If you select multiple instances, the total number of connections of ports are displayed.



- The distribution of traffic by **Source Locations** and **Source Service Providers**

## 5 Resource management

---

### 5.1 Purchase Anti-DDoS Pro or Anti-DDoS Premium instances

This topic describes how to purchase Anti-DDoS Pro and Anti-DDoS Premium instances.

#### Context

If your servers are deployed in mainland China, we recommend that you purchase an Anti-DDoS Pro instance. In this case, your domain names must obtain ICP licenses to enable access to your domain names. If your servers are deployed outside mainland China, we recommend that you purchase an Anti-DDoS Premium instance.

- For information about the price of Anti-DDoS Pro, see [Anti-DDoS Pro billing method](#).
- For information about the price of Anti-DDoS Premium, see [Anti-DDoS Premium billing method](#).

#### Purchase an Anti-DDoS Pro instance

1. Go to the buy page of [Alibaba Cloud Anti-DDoS Pro](#) and use your Alibaba Cloud account to log on.

## 2. Configure an Anti-DDoS pro instance as required.

### Anti-DDoS Pro (Mainland China)

Anti-DDoS Pro (Mainland China)

Anti-DDoS Premium

GameShield(Pay-As-You-Go)

**No refund.**

If your server is hosted in Mainland China, we recommend that you use Anti-DDoS Pro. Your domain must obtain an ICP license before you can activate Anti-DDoS Pro. If your server is not hosted in Mainland China, we recommend that you use the Anti-DDoS Premium.

Mitigation Plan

Professional

Specification

Diversion Mode: DNS Diversion

Reserved Resource: 1 Dedicated IP

Bandwidth Type: BGP Network

Mitigation Capacity: Basic protection (Prepaid) + Burstable protection (Postpaid)

Basic Protection

30Gb	60Gb	100Gb	300Gb	400Gb	500Gb
600Gb					

Basic mitigation capacity. (Prepaid)

Burstable Protection

30Gb	40Gb	50Gb	60Gb	70Gb	80Gb
100Gb	150Gb	200Gb	300Gb		

The burstable protection is the maximum mitigation capacity provided by the instance during protection. If you set the burstable protection and basic protection to the same value, no additional fees will be incurred and the maximum mitigation capacity provided by the instance equals the basic protection. If you set the burstable protection to a value greater than the basic protection, the instance can provide protection against attacks with bandwidth greater than the basic protection but no greater than the burstable protection. Additional fees will be incurred based on the peak attack bandwidth.

Clean Bandwidth

11

1250M

2500M

5000M

100

M

When the traffic on your website exceeds the service bandwidth, packet loss may occur or the server performance may degrade. We recommend that you increase your service bandwidth to resolve these issues.

Function Plan

Standard Function

Enhanced Function

Function Spec

Supports Non-Standard ports for HTTP(S) and WebSocket(s)

Supports GeoIP blocking rules (i.e. Allow access from Europe only)

Supports custom application layer Access-Control-Rules

Supports static website caching

Supports for custom TLS protocol versions and cipher suites

Supports for CDN Interaction

Domains

50

Web domains(FQDN) that could be protected in instance

Every 10 domains(FQDN) supports 1 top-level domain(site).

Clean QPS

3000

Clean QPS is the normal HTTP/S traffic's QPS in non-DDoS attack status.

Ports

50

Quantity

1

Duration

1 Month

2 Months

3 Months

4 Months

5 Months


6 Months


1 Year

2 Years

☐ Auto Renew

Parameter	Description
Mitigation Plan	Default value: <b>Professional</b> . You cannot modify this parameter.

Parameter	Description
<b>Basic Protection</b>	The basic bandwidth that you want to purchase for the Anti-DDoS Pro instance. Your subscription fee is determined based on the basic bandwidth and the valid period you purchase.
<b>Burstable Protection</b>	<p>The maximum protection bandwidth of the Anti-DDoS Pro instance that you want to purchase. If the attack bandwidth exceeds the basic protection bandwidth, the burstable protection bandwidth is consumed to protect the instance. Additional fees are incurred based on the difference between the peak attack bandwidth and basic bandwidth.</p> <div> <b>Note:</b> If you do not want to enable this feature, you can set the burstable protection and basic protection bandwidths to the same value. In this case, no additional fees are incurred and the maximum protection bandwidth provided by Anti-DDoS Pro equals the basic protection bandwidth.</div>
<b>Resource Group</b>	The resource group to which the Anti-DDoS Pro instance belongs.
<b>Clean Bandwidth</b>	<p>The maximum bandwidth of your services if no attacks are detected. The bandwidth must be greater than the highest peak bandwidth of the inbound and outbound traffic.</p> <p>For more information about how to select an appropriate clean bandwidth, see <a href="#">Clean bandwidth</a>.</p>
<b>Function Plan</b>	Valid value: <b>Standard Function</b> and <b>Enhanced Function</b>

Parameter	Description
<b>Domains</b>	<p>The number of HTTP and HTTPS domain names that the instance can protect.</p> <div>  <b>Note:</b>            Every 10 domain names must belong to the same top-level domain name and contain the subdomains and wildcard domains of the top-level domain name.         </div> <p>For more information, see <a href="#">Domains</a>.</p>
<b>QPS</b>	The maximum number of HTTP and HTTPS requests that the instance can concurrently process per second if no attacks are detected.
<b>Ports</b>	The number of TCP and UDP ports that the instance can protect.
<b>Quantity</b>	The number of instances with the current specifications that you want to purchase.
<b>Plan</b>	<p>The validity period of the instance that you want to purchase. <b>Auto Renew</b></p> <ul style="list-style-type: none"> <li>Monthly subscription: The instance is automatically renewed for a one-month valid period after it expires.</li> <li>Annual subscription: The instance is automatically renewed for a one-year valid period after it expires.</li> </ul>

3. Confirm the configurations and click **Buy Now**.

4. Confirm your order and complete the payment.

### Purchase an Anti-DDoS Premium instance

1. Go to the buy page of [Anti-DDoS Premium](#) and use your Alibaba Cloud account to log on.

## 2. Configure an Anti-DDoS Premium instance as required.

### Anti-DDoS Premium

Anti-DDoS Pro (Mainland China)

**Anti-DDoS Premium**

Anti-DDoS Origin

GameShield(Pay-As-You-Go)

No refund

Basic

Mitigation Plan

Insurance

Unlimited

MCA

Insurance Plan is fit for protecting the services those have low DDoS Attack risk

Specification

Diversion Mode: DNS Diversion

Reserved Resource: 1 Dedicated Anycast IP

Mitigation Capacity: Two Advanced Mitigations/Month

Important: Please purchase Anti-DDoS Pro if most users of your service are in Mainland China.

Business Size

Clean Bandwidth

100Mbps

150Mbps

200Mbps

250Mbps

300Mbps

Clean Bandwidth is the maximum normal business traffic size in non-DDoS attack status

Function Plan

Standard Function

Enhanced Function

Domains

10

Web domains(FQDN) that could be protected in instance  
Every 10 domains(FQDN) supports 1 site  
For example: If you have 3 domains(FQDN)[www.example1.com, \*.example1.com, www.example2.com] need to be protected, those domains belong to 2 sites[example1.com, example2.com], then you should select 20 domains

Clean QPS

500

Clean QPS is the normal HTTP/S traffic's QPS in non-DDoS attack status

Ports

5

TCP/UDP ports that could be protected in instance

Purchase Plan

Quantity

1

Subscription

3 Months

6 Months

1 Year

2 Years

☐ Auto Renew

Parameter	MCA supported	Description
<b>Mitigation Plan</b>	Yes	<p>Valid values: <b>Insurance</b>, <b>Unlimited</b>, and <b>MCA</b>.</p> <ul style="list-style-type: none"> <li>For information about insurance and unlimited mitigation plans, see <a href="#">Anti-DDoS Premium billing method</a>.</li> <li>For information about MCA, see <a href="#">Mainland China Acceleration</a>.</li> </ul>
<b>Clean Bandwidth</b>	Yes	<p>The maximum bandwidth of your services if no attacks are detected. The bandwidth must be greater than the highest peak bandwidth of the inbound and outbound traffic.</p> <p>For more information about how to select an appropriate clean bandwidth, see <a href="#">Clean bandwidth</a>.</p>
<b>Function Plan</b>	No	Valid value: <b>Standard Function</b> and <b>Enhanced Function</b>
<b>Domains</b>	No	<p>The number of HTTP and HTTPS domain names that the instance can protect.</p> <div>  <b>Note:</b> <p>Every 10 domain names must belong to the same top-level domain name and contain the subdomains and wildcard domains of the top-level domain name.</p> <p>For more information, see <a href="#">Domains</a>.</p> </div>
<b>Clean QPS</b>	No	The maximum number of HTTP and HTTPS requests that the instance can concurrently process per second if no attacks are detected.
<b>Ports</b>	No	The number of TCP and UDP ports that the instance can protect.
<b>Quantity</b>	Yes	The number of instances with the current specifications that you want to purchase.

Parameter	MCA supported	Description
Subscription	Yes	<p>The validity period of the instance that you want to purchase. <b>Auto Renew</b></p> <ul style="list-style-type: none"><li>• Monthly subscription: The instance is automatically renewed for a one-month valid period after it expires.</li><li>• Annual subscription: The instance is automatically renewed for a one-year valid period after it expires.</li></ul>

3. Confirm the configurations and click **Buy Now**.
4. Confirm your order and complete the payment.

## 5.2 Upgrade the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance

If the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance, which include the function plan, basic protection, clean bandwidth, and the number of domain names and ports, cannot meet your needs, you can upgrade your instances in the Anti-DDoS Pro or Anti-DDoS Premium console.

### Context

You can upgrade the standard function plan to the enhanced function plan or increase the basic bandwidth, clean bandwidth, and the number of domain names and ports. You are responsible for any price difference that are incurred by the upgrade. The new specifications immediately take effect after you complete the payment.



#### Note:

You cannot downgrade the specifications of Anti-DDoS Pro and Anti-DDoS Premium instances.

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Assets > Instances**.



4. Find the Anti-DDoS Pro or Anti-DDoS Premium instance whose specifications you want to upgrade, and click **Upgrade** in the Actions column.
5. On the **Upgrade/Downgrade** page that appears, select the specification that you want to upgrade to, and click **Buy Now**.
6. Complete the payment. The new specifications take effect immediately.

## 5.3 Manage instance tags

Anti-DDoS Pro allows you to manage the tags of an instance. You can use tags to mark instances and manage instances with the same tag simultaneously.

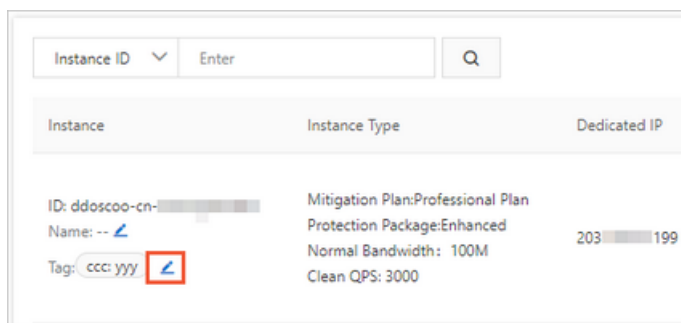
### Context

Each tag is a key-value pair. Tags have the following limits:

- You can attach up to 20 tags to an instance.
- The key of each tag attached to an instance must be unique. The tag value of a new tag key overwrites the tag value of an existing tag key.
- Each tag must be attached to at least one instance.

### Add a tag

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose **Assets > Instances**.
3. On the **Instances** page, find the target instance, and click the Edit icon in the **Instance** column.



4. In the **Edit Tag** dialog box that appears, click **Create Tag**.



### Note:

If you have existing tags, you can click **Select Tag** to select a tag for the instance.

5. Enter the **Tag Key** and **Tag Value**, and then click **OK**.

**Note:**

If you want to use an existing tag, select a tag from the drop-down list.

Edit Tag

site: china X

Select Tag | Create Tag

Tag Key business Tag Value web OK | Cancel

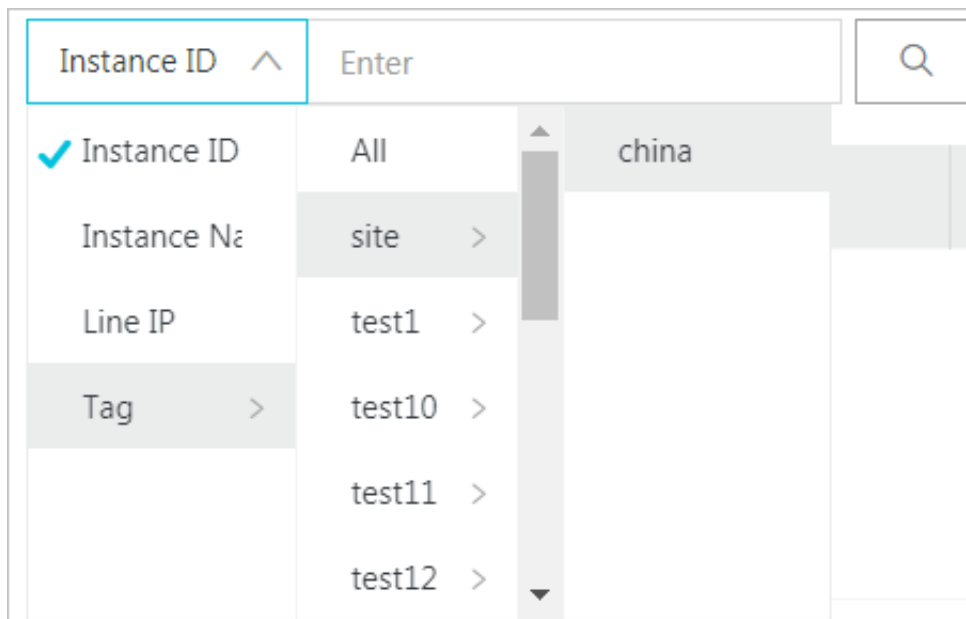
OK Cancel

6. Click **OK** to attach the tag to the instance. You can also select multiple tags in the **Edit Tag** dialog box.

**Search for instances by tag**

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose **Assets > Instances**.

3. On the **Instances** page, select **Tag** from the drop-down list next to the search box, and then select the tag key and value.

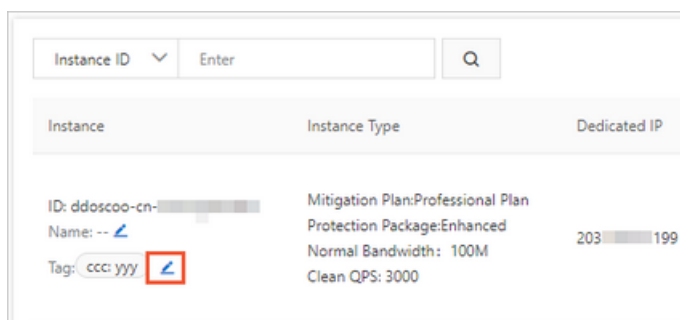


Instances that have the specified tag are displayed in the instance list.

### Remove a tag

You can only remove tags from one instance at a time.

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose **Assets > Instances**.
3. On the **Instances** page, find the target instance, and click the Edit icon in the **Instance** column.



4. In the **Edit Tag** dialog box, click the Delete icon next to a tag, and then click **OK**.



#### Note:

After a tag is removed from an instance, the tag is deleted if it is not attached to any instance.

## 6 Check security overview

---

After you switch your service traffic to an Anti-DDoS Pro or Anti-DDoS Premium instance, you can view the metrics and DDoS attack events in real time on the Security Overview page in the relevant console.

### Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased and your service is protected by the instance.

### Context



#### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

The Security Overview page provides an overview of the following metrics and DDoS attack events:

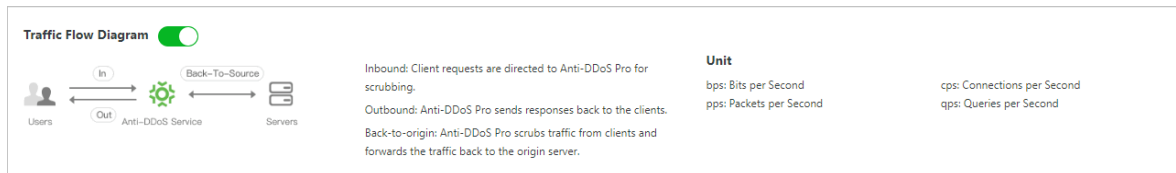
- Service metrics: clean bandwidth, QPS, connections per second (CPS), protected domain names, and protected ports.
- Attack events: volumetric DDoS attacks, connection-oriented attacks, and resource exhaustion attacks.

### Procedure

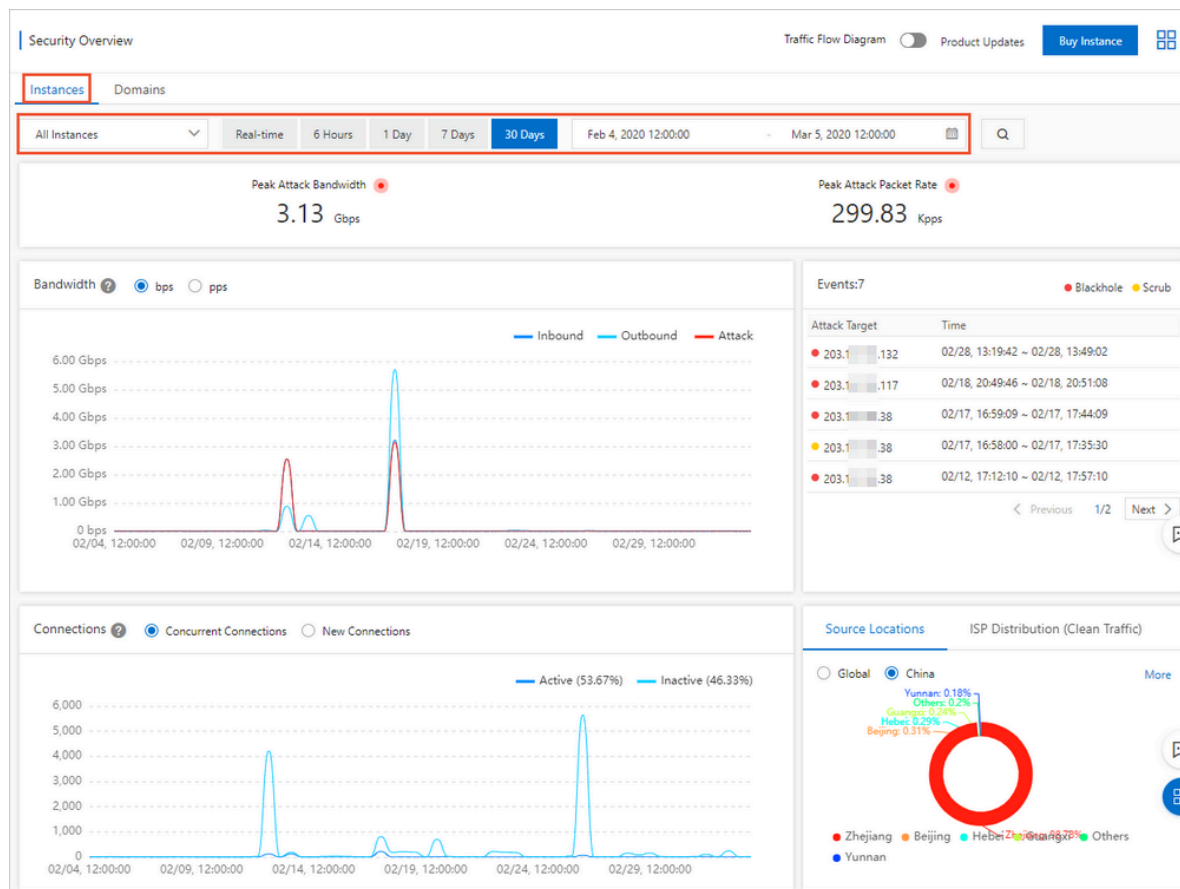
1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China**: Anti-DDoS Pro
  - **Outside Mainland China**: Anti-DDoS Premium
3. In the left-side navigation pane, click **Security Overview**.

4. Optional: Turn on **Traffic Flow Diagram** to view the background information and concepts.

**Traffic Flow Diagram** displays the relationship between origin servers and Anti-DDoS Pro or Anti-DDoS Premium instances, the terminology, and commonly used units.

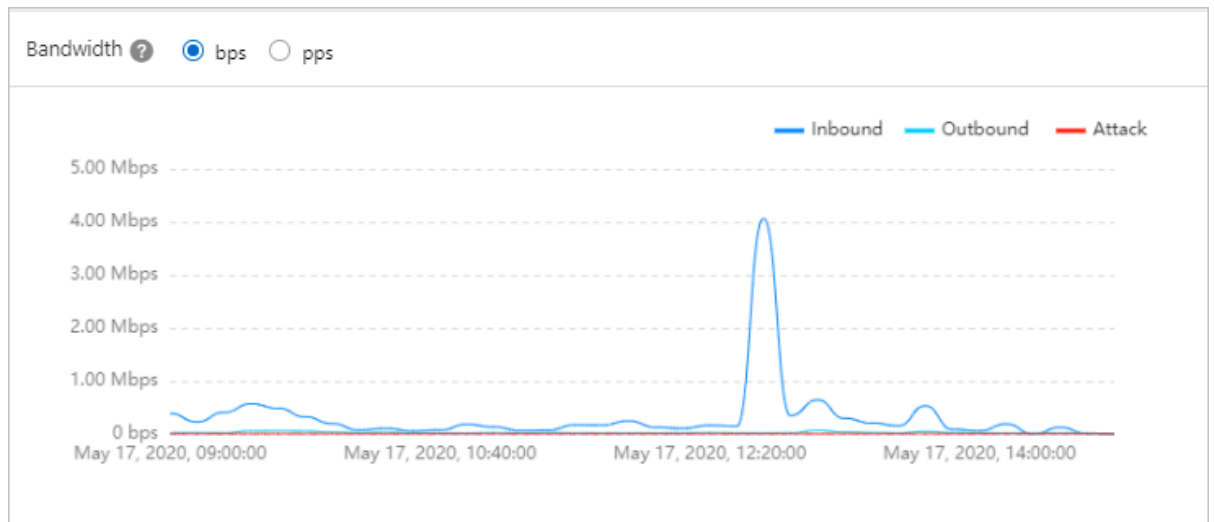


- Click the **Instances** tab, select one or more instances, and specify a time range to view the relevant metrics.



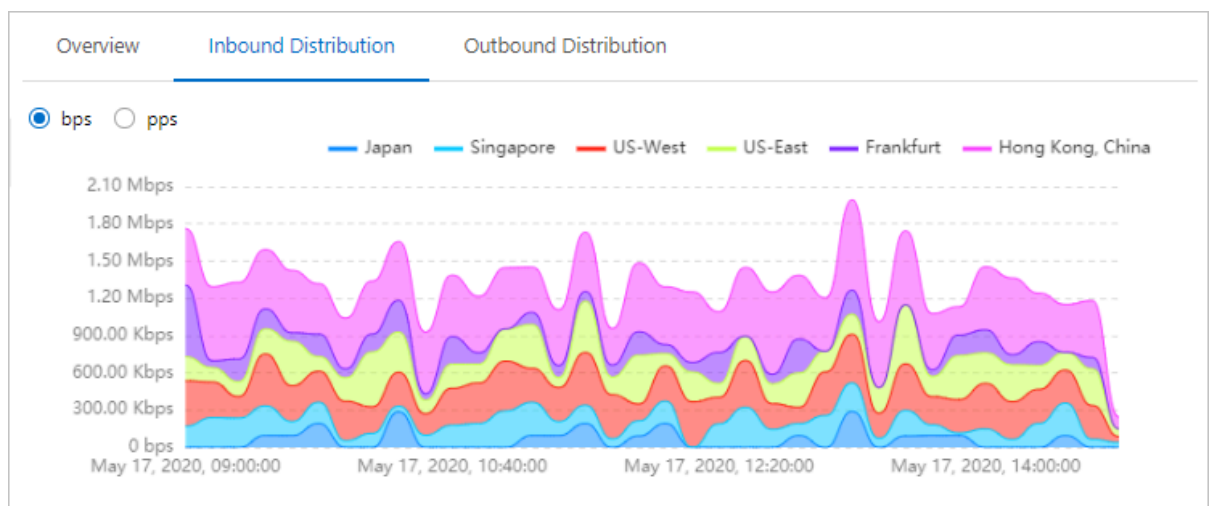
You can view the following instance information:

- Peak Attack Bandwidth and Peak Attack Packet Rate**
- Traffic trends**
  - The **Bandwidth** trend chart provided by Anti-DDoS Pro displays the traffic information by **bps** or **pps**. You can view the trends of inbound, outbound, and attack traffic of an instance for a specific period of time.



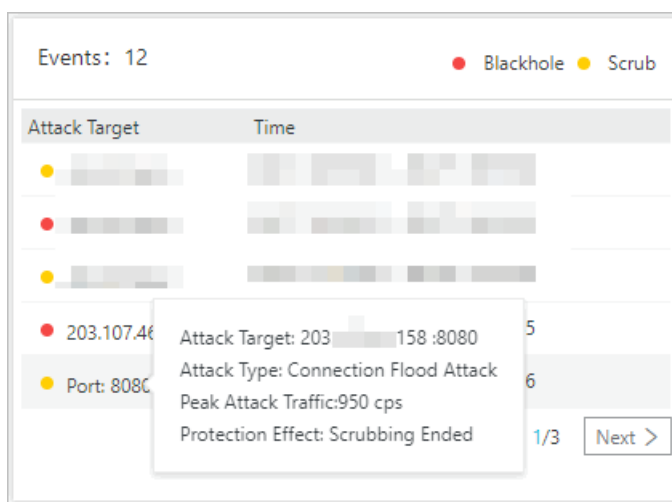
- Anti-DDoS Premium provides the following tabs to provide bandwidth trends, distribution of inbound traffic, and distribution of outbound traffic, respectively:

**Overview, Inbound Distribution, and Outbound Distribution.**



- **Attack Events** of blackhole and mitigation

You can move the pointer over an IP address or a port to view the details of an attack, such as Attack Target, Attack Type, Peak Attack Traffic, and Protection Effect.

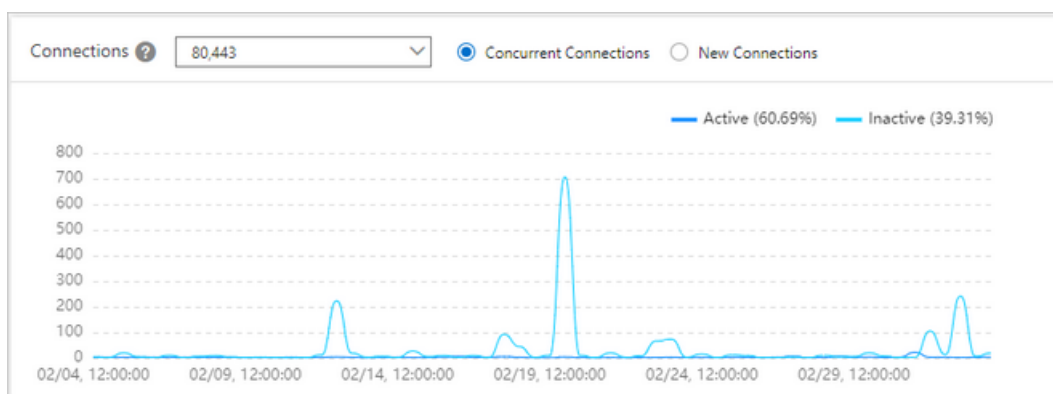


- **Connections** on a port
  - **Concurrent Connections:** the total number of concurrent TCP connections established between clients and the instance
  - **New Connections:** the number of new TCP connections established between clients and the instance per second



#### Note:

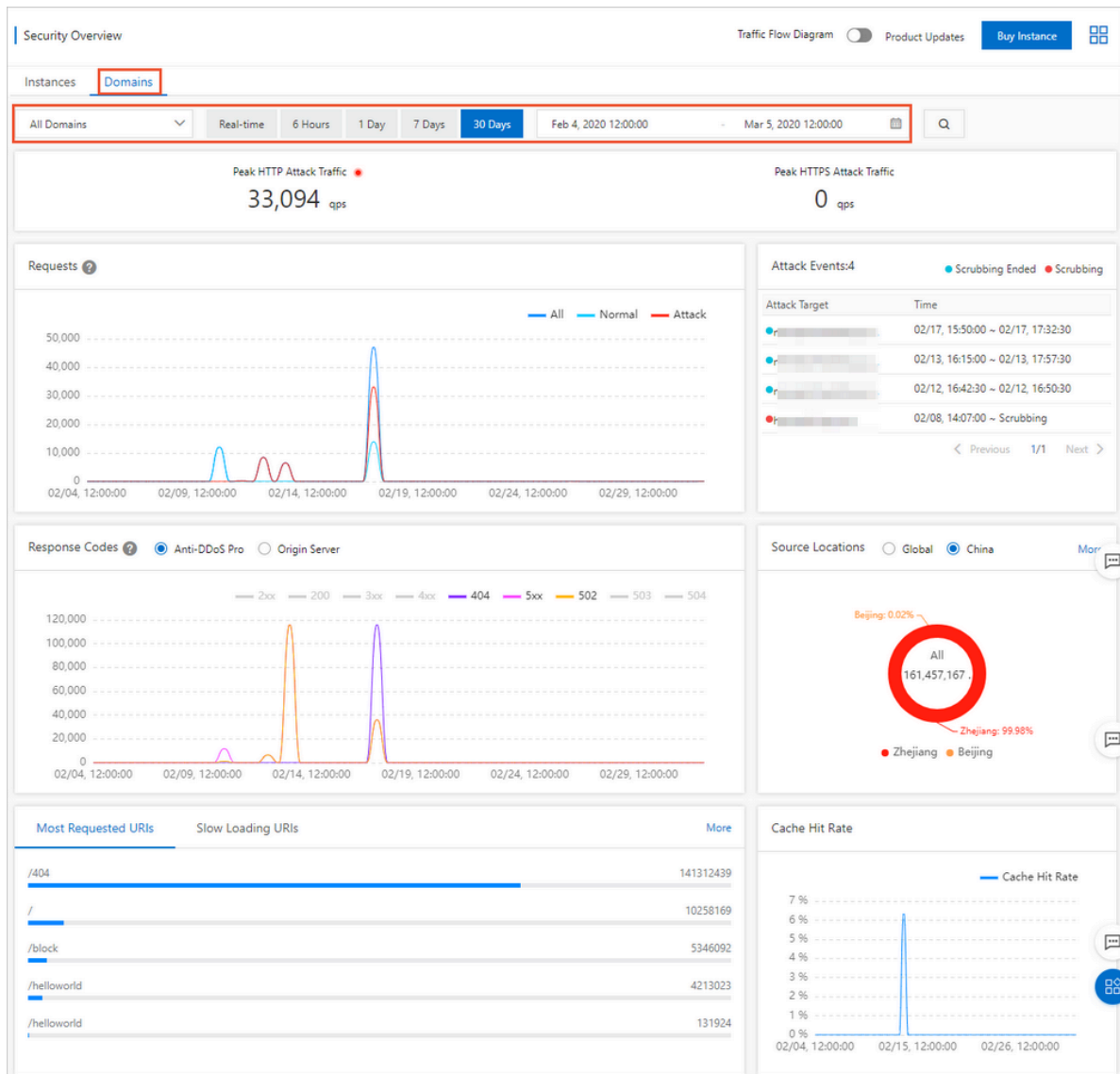
If you select an instance, the Connections chart displays the numbers of connections on different ports. If you select multiple instances, the total number of connections of ports are displayed.



- The distribution of traffic by **Source Locations** and **Source Service Providers**



6. Click the **Domains** tab, select one or more domains, and specify a time range to view the relevant metrics.



You can view the following domain information:

- **Peak HTTP Attack Traffic** and **Peak HTTPS Attack Traffic**
- **Requests**

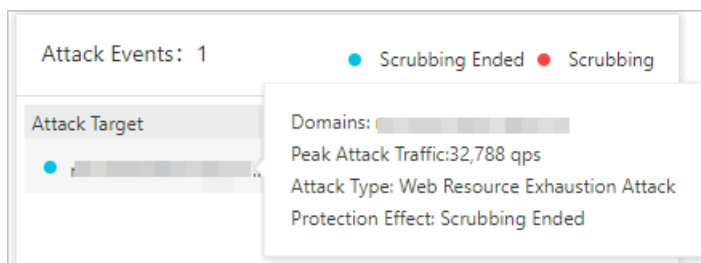
The trend of requests is displayed based on the peak values in a specific time range. The displayed time granularity is based on the specific time range:

- If the time range is less than an hour, the granularity is 1 minute.
- If the time range is between 1 and 6 hours, the granularity is 10 minutes.
- If the time range is between 6 and 24 hours, the granularity is 30 minutes.
- If the time range is between 1 and 7 days, the granularity is 1 hour.
- If the time range is between 7 and 15 days, the granularity is 4 hours.

- For larger time ranges, the granularity is 12 hours.

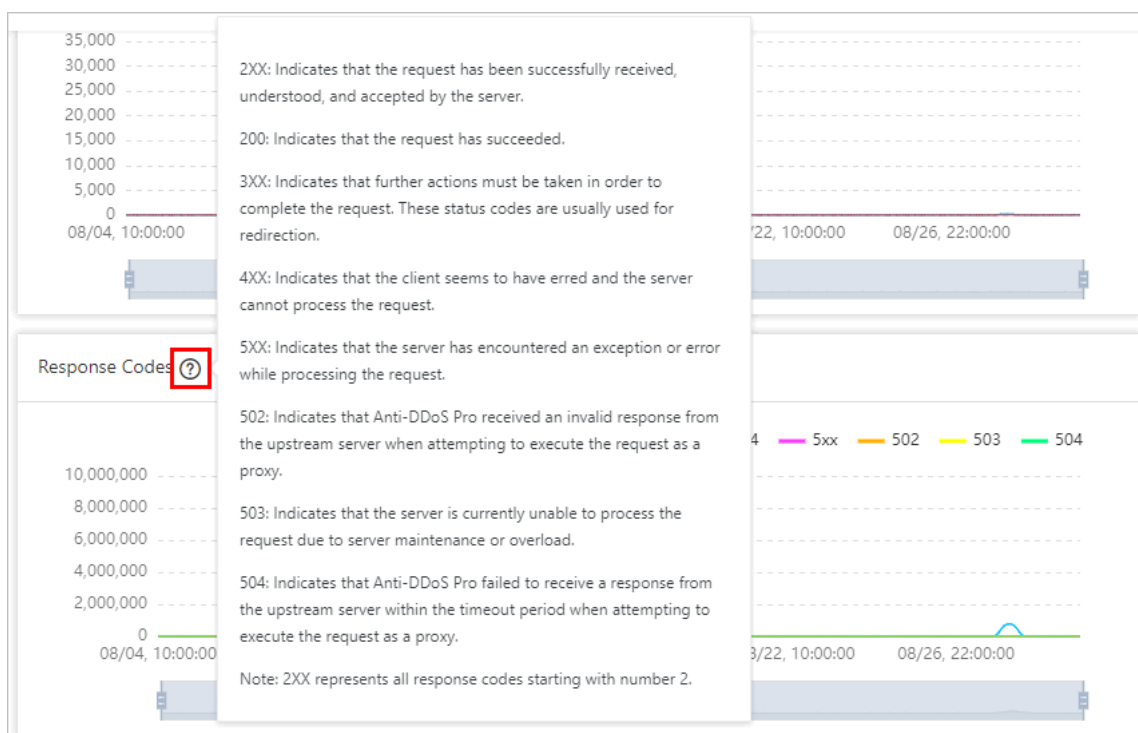
- **Attack Events**

You can move the pointer over a domain to view the details of an attack, such as Domains, Peak Attack Traffic, and Attack Type.



- **Response Codes**

The trend chart of response codes displays the accumulated numbers of response codes within a specific time range. This time range is the same as that specified in the **Requests** chart. You can move the pointer over the question mark icon to view the explanation of response codes.



- **Source Locations**
- **Most Requested URIs and Slow Loading URIs**
- **Cache Hit Rate**



**Note:**

You must enable the static page caching feature before you can view the trend chart of the cache hit rate. For more information, see [Configure static page caching](#).

## 7 View security reports

---

After you set up an Anti-DDoS Pro instance to protect your services and the service traffic is rerouted to the instance, you can view traffic statistics and information about DDoS attack prevention on the Security Reports page.

### Prerequisites

An Anti-DDoS Pro instance is purchased and your service is protected by the instance.



#### Note:

Only Anti-DDoS Pro supports the Security Reports feature. If you use Anti-DDoS Premium, we recommend that you view the service protection information on the Security Overview page.

### Procedure

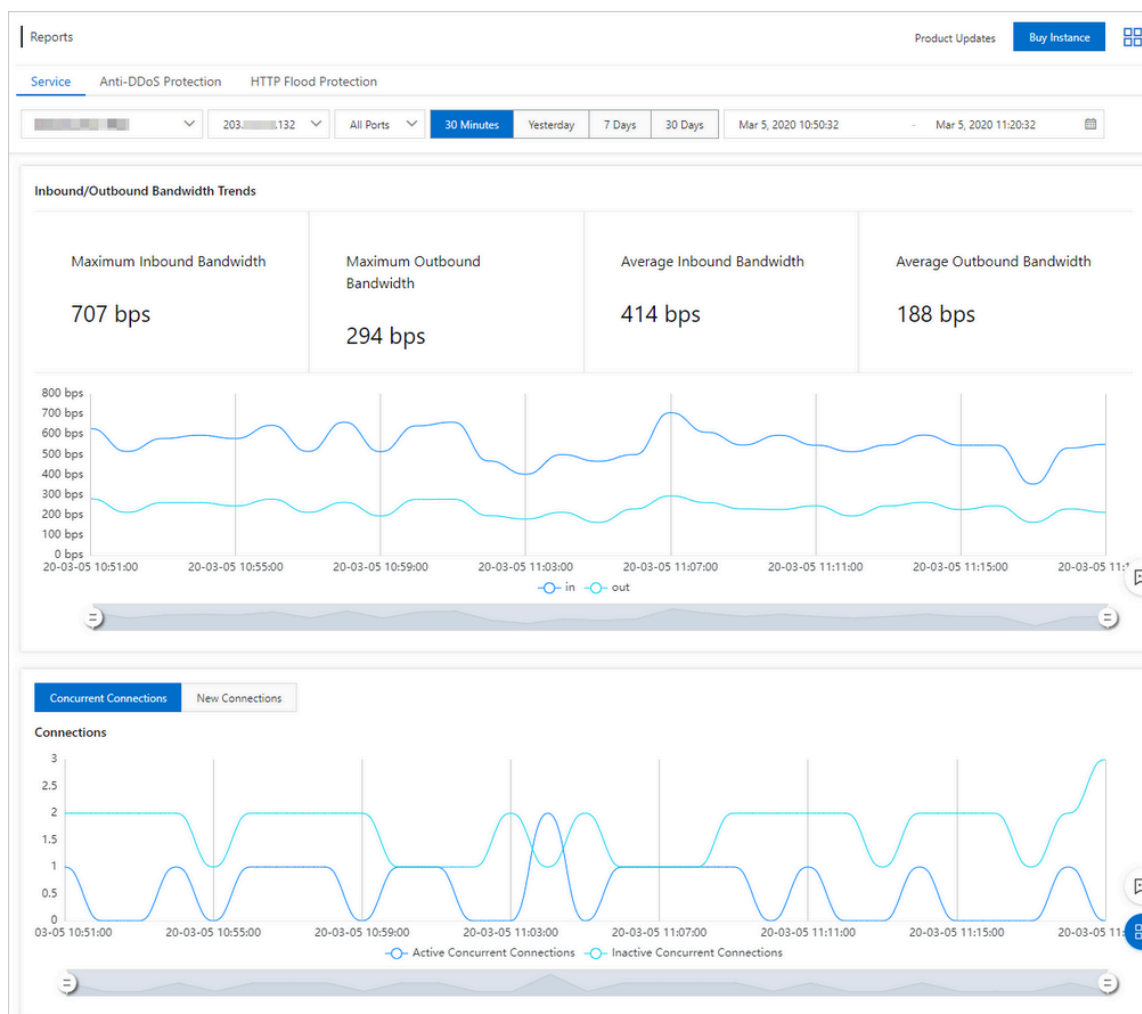
1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select **Mainland China**.
3. In the left-side navigation pane, click **Security Reports**.
4. On the **Reports** page, click the following tabs to view relevant reports: Service, Anti-DDoS Protection, and HTTP Flood Protection.
  - View the service report of protected service.

Click the **Service** tab, select the Anti-DDoS Pro instance and ports that you want to view and specify a time range to view the trend of inbound traffic, trend of outbound traffic, and connections of the protected services during that time.



#### Note:

You can query traffic information and connections from the last 30 days.



You can also move the slider to adjust the time range. This function facilitates time-specific queries.

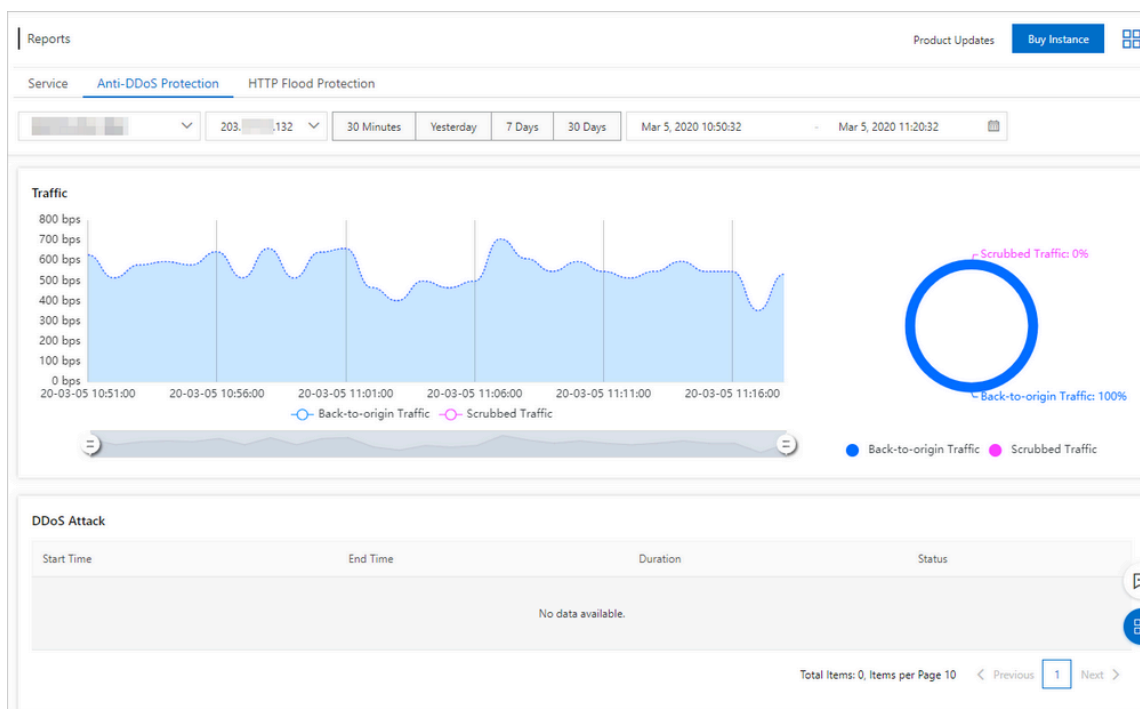
- View the anti-DDoS protection report of protected service.

Click the **Anti-DDoS Protection** tab, select the Anti-DDoS Pro instance that you want to view and specify a time range to view DDoS attacks at and traffic information of the protected services during that time.



**Note:**

You can query traffic information and DDoS attacks from the last 30 days.



#### Note:

Anti-DDoS Pro and Anti-DDoS Premium automatically filter out malformed packets, such as small SYN packets and packets that do not meet TCP requirements, such as invalid SYN flags. This way, your servers do not allocate resources to manage malformed packets. Anti-DDoS Pro and Anti-DDoS Premium take the filtered malformed packets into account in the scrubbed traffic statistics. This means that the traffic chart may show a traffic scrubbing event even if the size of the network traffic received by the server does not exceed the traffic scrubbing threshold.

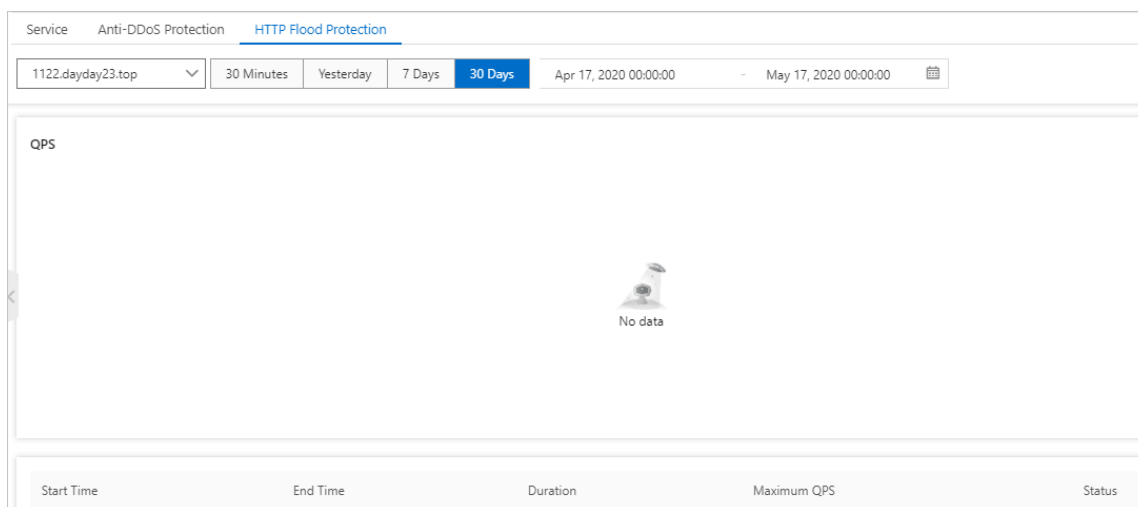
- View HTTP flood protection record of protected services.

Click the **HTTP Flood Protection** tab, select the domain name and specify the time range to view the information about queries per second (QPS) and HTTP flood attacks during that time.



#### Note:

You can query information about QPS and HTTP flood attacks from the last 30 days.



## 8 Deploy Anti-DDoS Pro

### 8.1 Use domains

#### 8.1.1 Add a website

Website configurations define how Anti-DDoS Pro or Anti-DDoS Premium forwards the inbound traffic of a protected website. To use Anti-DDoS Pro or Anti-DDoS Premium for website protection, you must add the website to Anti-DDoS Pro or Anti-DDoS Premium. You can add multiple websites at a time. This topic describes how to add a website and how to import multiple website configurations to Anti-DDoS Pro or Anti-DDoS Premium at a time.

##### Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see [Purchase Anti-DDoS Pro or Anti-DDoS Premium instances](#).

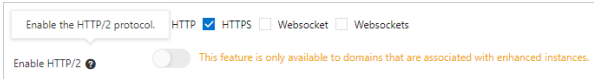
##### Differences of website configurations between Anti-DDoS Pro and Anti-DDoS Premium



##### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

The following table describes the feature differences between Anti-DDoS Pro and Anti-DDoS Premium.

Feature	Description	Anti-DDoS Pro	Anti-DDoS Premium
<b>Enable HTTP/2</b>	You can enable this feature for websites associated with Anti-DDoS Pro or Anti-DDoS Premium instances that use the enhanced function plan. After the feature is enabled, the protocol version is HTTP 2.0. 	Supported	Not supported



Feature	Description	Anti-DDoS Pro	Anti-DDoS Premium
<b>CNAME Reuse</b>	<p>After the feature is enabled, domain names hosted by the same server are associated with the CNAME record assigned by Anti-DDoS Pro or Anti-DDoS Premium. For more information, see <a href="#">CNAME reuse</a>.</p> <div><div>CNAME Reuse</div><div><input type="checkbox"/></div><div><a href="#">Documentation</a></div></div>	Not supported	Supported

### Add a website

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning** > **Website Config**.
4. On the **Website Config** page, click **Add Domain**.







#### Note:


You can import multiple website configurations at a time. For more information, see [Import multiple website configurations at a time](#).



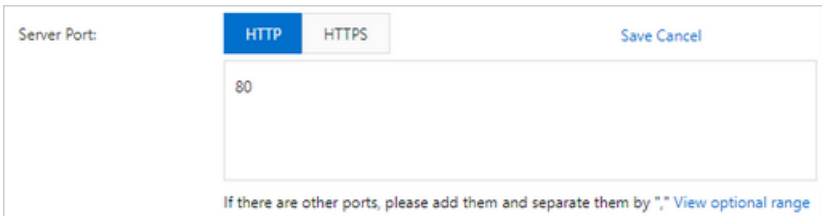

5. On the **Add Domain** wizard, set the parameters in the **Enter Site Information** step and click **Add**.

The screenshot shows the 'Add Domain' wizard with the 'Enter Site Information' step active. The 'Function Plan' is set to 'Standard'. The 'Instance' section shows 0 instances selected. The 'Domain' field is empty. The 'Protocol' section has 'HTTP' and 'HTTPS' checked. 'Enable HTTP/2' is disabled. The 'Server IP' section has 'Origin Server IP' selected. The 'Server Port' section shows 'HTTP 80' and 'HTTPS 443'. A green message box at the bottom states: 'If the IP addresses of your origin server have been exposed, click [here](#) to learn how to fix the issue.'

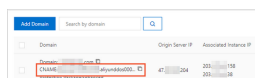
Parameter	Description
<b>Function Plan</b>	<p>The function plan of the instance that you want to use to protect the website. Valid values:</p> <ul style="list-style-type: none"> <li><b>Standard</b></li> <li><b>Enhanced</b></li> </ul> <div>  <b>Note:</b>  For more information, see <a href="#">Function plan</a>. </div>

Parameter	Description
<b>Instance</b>	<p>The instance that you want to use to protect the website. You can select up to eight instances for one domain name. The instances used to protect the same domain name must use the same function plan.</p> <div> <b>Note:</b> The available instances are displayed after you select a function plan. If no instance is available, no instance uses the selected function plan. In this case, you can purchase an instance or upgrade the standard function plan to the enhanced function plan. For more information, see <a href="#">Upgrade the specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance</a>.</div>
<b>Domain</b>	<p>Enter the domain of the website that you want to protect.</p> <div> <b>Note:</b></div> <ul style="list-style-type: none"><li>• A domain name can contain letters, digits, and hyphens (-). It must start with a letter or digit. Domain names are not case sensitive.</li><li>• You can enter wildcard domains, such as *.aliyun.com. Anti-DDoS Pro or Anti-DDoS Premium protects the subdomains of wildcard domains.</li><li>• If you specify a domain name and its wildcard domain, such as www.aliyun.com and *.aliyun.com, the forwarding rules and protection policies configured for the domain name supersede those configured for the wildcard domain.</li></ul>
<b>Protocol</b>	<p>The protocols that the website supports. Valid values:</p> <ul style="list-style-type: none"><li>• <b>HTTP</b> (selected by default)</li><li>• <b>HTTPS</b> (selected by default)</li><li>• <b>Websocket</b></li><li>• <b>Websockets</b></li></ul> <div> <b>Note:</b> If your website supports HTTPS, you must select HTTPS. You can select other protocols that your website supports as required.</div>

Parameter	Description
<b>Enable HTTP/2</b>	<p>Specifies whether to enable HTTP 2.0 when the website is protected by an Anti-DDoS Pro instance that uses the enhanced function plan. After the feature is enabled, the protocol version is HTTP 2.0.</p> <div> <b>Note:</b> This feature is available only for Anti-DDoS Pro.</div>
<b>Server IP</b>	<p>The address type of the origin server. You must enter the address after you specify the address type. The address type can be <b>Origin Server IP</b> or <b>Origin Server Domain</b>.</p> <ul style="list-style-type: none"><li>• <b>Origin Server IP:</b> You can specify up to 20 IP addresses. If multiple IP addresses of an origin server are specified, Anti-DDoS Pro or Anti-DDoS Premium uses IP Hash load balancing to forward network traffic to the origin server.</li><li>• <b>Origin Server Domain:</b> If you want to use both Anti-DDoS Pro or Anti-DDoS Premium and web application firewall (WAF), select Origin Server Domain and enter the CNAME record provided by your WAF instance. This provides enhanced protection for your website.</li></ul>

Parameter	Description
<b>Server Port</b>	<p>The server port that is specified based on the selected protocol.</p> <div>  <b>Note:</b>            The forwarding port must be the same as the origin server port.         </div> <ul style="list-style-type: none"> <li>If <b>HTTP</b> or <b>Websocket</b> is selected, this parameter is set to 80 by default.</li> <li>If <b>HTTPS</b> or <b>Websockets</b> is selected, this parameter is set to 443 by default.</li> </ul> <div>  <b>Note:</b>            HTTP 2.0 ports are the same as HTTPS ports.         </div> <p>To add custom ports, you can click <b>Custom</b> and select ports other than the default ones.</p> <ul style="list-style-type: none"> <li>Instances that use the standard function plan support HTTP port 80, WebSocket port 8080, HTTPS port 443, and WebSockets port 8443.</li> <li>Instances that use the enhanced function plan support specific non-standard ports. For more information, see <a href="#">Specify non-standard ports for protection</a>.</li> </ul> <div>  </div>
<b>CNAME Reuse</b>	<p>Specifies whether to enable CNAME reuse. After CNAME reuse is enabled, you can associate the domain names hosted by the same server with the CNAME record assigned by Anti-DDoS Premium. For more information, see <a href="#">CNAME reuse</a>.</p> <div>  <b>Note:</b>            This feature is available only for Anti-DDoS Premium.         </div>

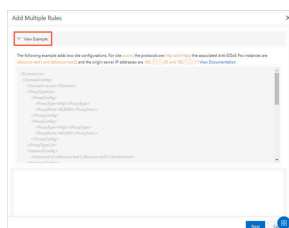
After you add a website, click **Website List**. Then, you can view the added website configuration and its CNAME record on the Website Config page.



## Import multiple website configurations at a time

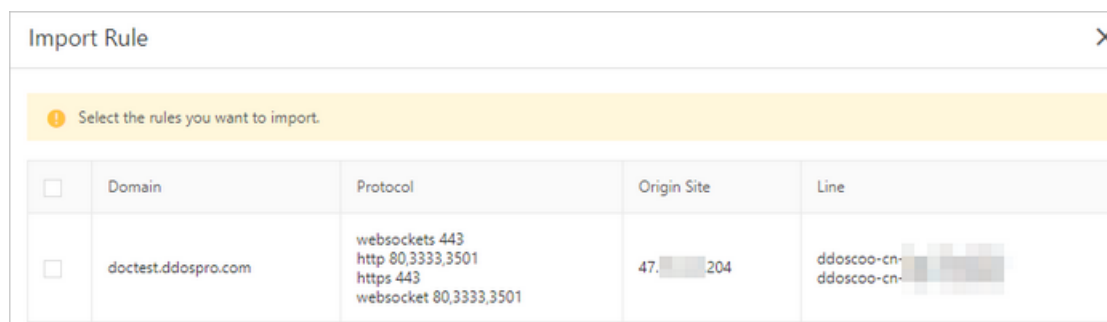
1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning** > **Website Config**.
4. On the **Website Config** page, click **Batch Domains Import**.
5. In the **Add Multiple Rules** pane, enter the information of the websites that you want to add and click **Next**.

You can edit the information of the websites that you want to add in an XML file and then copy the content into the field. For more information about the format of the file, see [Website configurations in an XML file](#).



If the content of the XML file is valid, the file is parsed into the configurations of the websites that you want to add.

6. In the **Import Rule** pane, select the websites that you want to add and click **OK**.



7. After the configurations are imported, close the **The rules have been created** pane.

## What to do next

Anti-DDoS Pro or Anti-DDoS Premium assigns a CNAME record to each added website. You can modify the DNS records to associate the CNAME record of the instance with the website. We recommend that you use a local machine to verify that the traffic forwarding

settings have taken effect before you switch your service traffic to an instance. For more information, see [Verify the forwarding configuration on your local machine](#).

**Notice:**

If you switch your service traffic to an instance before the forwarding settings take effect, your service may be interrupted.

After you add the website to Anti-DDoS Pro or Anti-DDoS Premium, you can perform the following operations on the **Website Config** page:

- If security software such as firewalls is deployed on the origin server, you must add the back-to-origin IP addresses of Anti-DDoS Pro or Anti-DDoS Premium to the whitelist of the origin server. For more information, see [Allow back-to-origin IP addresses to access the origin server](#).
- If the website provides services over HTTPS, you must upload an SSL certificate. For more information, see [Upload an SSL certificate](#).
- If the website provides services over HTTPS and is protected by an instance that uses the enhanced function plan, you can customize a TLS security policy. For more information, see [Create a custom TLS policy](#).
- Configure Layer 7 anti-DDoS protection for the website, such as anti-DDoS protection policies, HTTP flood protection policies, and network acceleration policies. For more information, see [Configure protection policies](#).
- Edit or delete a website configuration. For more information, see [Edit a website configuration](#) and [Delete a website configuration](#).
- Export multiple website configurations at a time. For more information, see [Export multiple website configurations at a time](#).
- If the origin server is deployed on an ECS instance, and the IP address of the origin server is exposed, we recommend that you change the public IP address of the ECS instance. This prevents attackers from bypassing Anti-DDoS Pro or Anti-DDoS Premium and launching attacks against the origin server. For more information, see [Change the public IP address of an ECS origin server](#).

## 8.1.2 Edit a website configuration

If you want to associate another Anti-DDoS Pro or Anti-DDoS Premium instances with a website or change the IP address of the origin server of a protected website, you can edit

the website configuration. You can edit multiple website configurations at a time. This topic describes how to edit one or more website configurations.

### Prerequisites

A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Add a website](#).

### Edit website configurations

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Website Config**.
4. Find the website configuration that you want to edit and click **Edit** in the Actions column.



#### Note:

If you use Anti-DDoS Pro, you can modify multiple website configurations at a time. For more information, see [Modify multiple website configurations at a time](#).

5. On the **Edit Site Configuration** page, edit the website configuration and click **OK**.

You can modify all parameters except for the domain name. For more information about the website configurations, see [Website configurations](#).

For example, to change the instance associated with a website, you can change the value of **Function Plan** and **Instance**. You can also change the value of **Server IP**.

### Modify multiple website configurations at a time



#### Note:

You can modify multiple website configurations at a time only in the Anti-DDoS Pro console.

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select **Mainland China**.
3. In the left-side navigation pane, choose **Provisioning > Website Config**.
4. On the **Website Config** page, click **Batch Domains Edit**.



5. In the **Batch Domains Edit** pane, enter the configurations and click **Next**.

You can import an XML file to modify multiple website configurations at a time. For more information about the format in the file, see [Website configurations in an XML file](#).

Batch Domains Edit

View Example

The following example adds two site configurations. For site **a.com**, the protocols are **http** and **https**; the associated Anti-DDoS Pro instances are **ddoscoo-test1** and **ddoscoo-test2**; and the origin server IP addresses are **192.168.1.45** and **192.168.1.11**. [View Documentation](#)

```
<DomainList>
  <DomainConfig>
    <Domain>a.com</Domain>
    <ProxyTypeList>
      <ProxyConfig>
        <ProxyType>http</ProxyType>
        <ProxyPorts>80,8080</ProxyPorts>
      </ProxyConfig>
      <ProxyConfig>
        <ProxyType>https</ProxyType>
        <ProxyPorts>443,445</ProxyPorts>
      </ProxyConfig>
    </ProxyTypeList>
    <InstanceConfig>
      <InstanceList>ddoscoo-test1,ddoscoo-test2</InstanceList>
    </InstanceConfig>
  </DomainConfig>
</DomainList>
```

Next Cancel

If the content of the XML file is valid, the file is parsed into the configurations of the websites that you want to import.

6. In the **Import Rule** pane, select the websites that you want to add and click **OK**.

Import Rule

Select the rules you want to import.

	Domain	Protocol	Origin Site	Line
<input type="checkbox"/>	doctest.ddospro.com	websockets 443 http 80,3333,3501 https 443 websocket 80,3333,3501	47.204	ddoscoo-cn- ddoscoo-cn-

7. After the configurations are imported, close the **The rules have been created** pane.

### 8.1.3 Delete a website configuration

If a website no longer requires anti-DDoS protection, you can delete the website configuration. Before you perform this operation, you must update the DNS record. Make sure that the DNS record does not use the IP address of an Anti-DDoS Pro or Anti-DDoS Premium instance or the CNAME record. The CNAME record refers to that assigned by Anti-

DDoS Pro or Anti-DDoS Premium, or that assigned by Sec-Traffic Manager. If you delete a website configuration without updating its DNS record, your service may be interrupted.

### Prerequisites

The DNS record of the website is updated.

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Website Config**.
4. Find the website configuration that you want to delete and click **Delete** in the Actions column.



#### Note:

Anti-DDoS Pro allows you to delete multiple website configurations at a time. You can select multiple website configurations that you want to delete and click **Batch Delete** below the list.

5. In the message that appears, click **OK**.

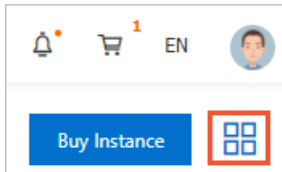
## 8.1.4 Export multiple website configurations at a time

Anti-DDoS Pro and Anti-DDoS Premium allow you to export multiple website configurations at a time. You can export all website configurations as an XML file and download the file to your local machine. The exported files use the same format as the file that you use to import or modify website configurations at a time.

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Website Config**.
4. Click **Batch Domains Export** below the list to deliver the export task.

5. After the export task is delivered, click the Tasks icon in the upper-right corner of the page.



6. In the **Tasks** pane, wait until the export task is completed and click **Download** in the Actions column.

**Note:**

If the task status is in the **Pending Export** state, wait until the task is complete.

Tasks			
Name	Status	Start Time	Actions
Layer 7 Export	● Exported	03/04/2020, 15:23:00	<div>Delete Download</div>

You can use a text editor, such as Notepad or Notepad++, to view the website configuration in the downloaded XML file. For more information, see [Website configurations in an XML file](#).

**Note:**

If you use Anti-DDoS Pro, the name of the exported file starts with DDoSCoo\_. If you use Anti-DDoS Premium, the name of the exported file starts with DDoSDip\_. The formats

of the files exported from the Anti-DDoS Pro and Anti-DDoS Premium consoles are the same.

```
<?xml version="1.0" encoding="UTF-8"?><DomainList>
<DomainConfig>
<Domain> [REDACTED] .com</Domain>
<ProxyTypeList>
<ProxyConfig>
<ProxyType>websockets</ProxyType>
<ProxyPorts>443</ProxyPorts>
</ProxyConfig>
<ProxyConfig>
<ProxyType>http</ProxyType>
<ProxyPorts>80,3333,3501</ProxyPorts>
</ProxyConfig>
<ProxyConfig>
<ProxyType>https</ProxyType>
<ProxyPorts>443</ProxyPorts>
</ProxyConfig>
<ProxyConfig>
<ProxyType>websocket</ProxyType>
<ProxyPorts>80,3333,3501</ProxyPorts>
</ProxyConfig>
</ProxyTypeList>
<InstanceConfig>
<InstanceList>ddoscoo-cn-[REDACTED]-ddoscoo-cn-[REDACTED]</InstanceList>
</InstanceConfig>
<RealServerConfig>
<ServerType>0</ServerType>
<ServerList>47.[REDACTED].204</ServerList>
</RealServerConfig>
</DomainConfig>
</DomainList>
```

- Optional: In the **Tasks** pane, find the task that you want to delete and click **Delete** in the Actions column.

### 8.1.5 Specify non-standard ports for protection

Anti-DDoS Pro and Anti-DDoS Premium instances that use the standard function plan support standard HTTP ports 80 and 8080 and standard HTTPS ports 443 and 8443 to protect websites against DDoS attacks. Instances that use the enhanced function plan support non-standard HTTP and HTTPS ports. However, only a limited number of ports are supported.



#### Note:

To support non-standard HTTP or HTTPS ports, make sure that your website is associated with an instance that uses the enhanced function plan.

#### Limit on the total number of ports

An instance that uses the enhanced function plan supports a maximum of 10 different ports

#### Supported ports



#### Note:

Instances protect only the specific HTTP and HTTPS ports. Inbound traffic of unsupported ports is not scrubbed and forwarded. For example, Anti-DDoS Pro or Anti-DDoS Premium discards the inbound traffic of port 4444.

- Instances that use the enhanced function plan support the following HTTP and WebSocket ports:

80, 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, 7060, 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, 8787, 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, and 33702

- Instances that use the enhanced function plan support the following HTTPS and WebSockets ports:

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

## 8.1.6 Upload an SSL certificate

To use Anti-DDoS Pro or Anti-DDoS Premium to scrub traffic transmitted over HTTPS, you must select HTTPS when you add the website and upload the required SSL certificate. If the uploaded SSL certificate changes, you must update the certificate in the Anti-DDoS Pro or Anti-DDoS Premium console.

### Prerequisites

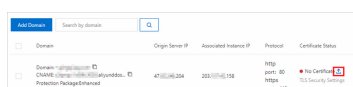
- A website is added to Anti-DDoS Pro or Anti-DDoS Premium, and the website supports the HTTPS protocol. For more information, see [Add a website](#).
- The certificate file of the website is prepared.

If you have uploaded the certificate file to [Alibaba Cloud SSL Certificates](#), you can select the certificate. Otherwise, you must upload your own certificate and private key file. In most cases, the following files are required:

- The public key file in CRT format or the certificate file in PEM format.
- The private key file in the KEY format.

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning** > **Website Config**.
4. On the **Website Config** page, find the domain name for which you want to upload a certificate and click the upload icon in the **Certificate Status** column.

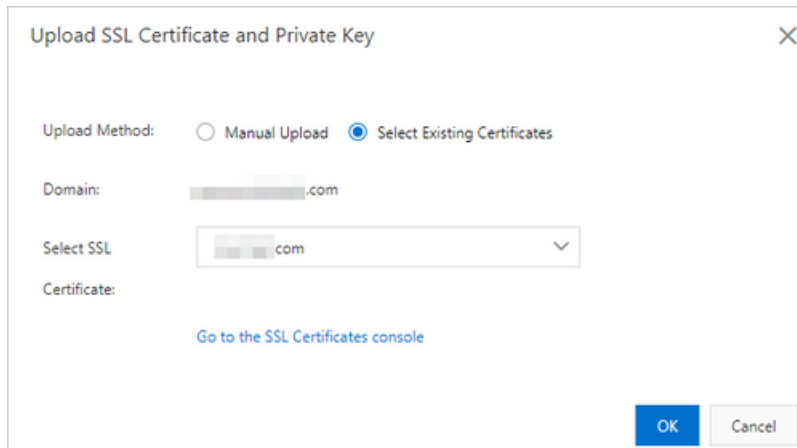


Domain	Origin Server IP	Associated Instance IP	Protocol	Certificate Status
Domain: <a href="#">http://api.bilibili.com</a> Click to upload certificate Protection Package: Enhanced	47.100.162.204	203.107.142.128	http port: 80 https port: 443	No Certificate SSL Security Settings

5. In the **Upload SSL Certificate and Private Key** dialog box, select an **Upload Method** and set other parameters. You can use one of the following methods to upload your certificate:

- **Select Existing Certificates** (recommended)

If you have uploaded the certificate to Alibaba Cloud SSL Certificates, select the certificate and upload it to Anti-DDoS Pro or Anti-DDoS Premium.



If you have not uploaded the certificate to Alibaba Cloud SSL Certificates, click **Go to the SSL Certificate console** to upload your certificate. For more information about how to upload certificates to Alibaba Cloud SSL Certificates, see [#unique\\_69](#).

- **Manual Upload**

Specify **Certificate Name**, and copy the content in the certificate file to the **Certificate File** field and the private key file to the **Private Key** field.

**Note:**

- You can use a text editor to open the files in PEM, CER, or CRT format and copy the file content. You must convert the files in uncommon formats, such as PFX and P7B, into the PEM format and use a text editor to open the files and copy the file content. For information about how to convert the format of a certificate file, see [#unique\\_70](#).
- If the SSL certificate includes multiple certificate files, such as a certificate chain, you must concatenate the content of these certificate files in the certificate chain and copy the concatenated content to the **Certificate File** field.

## Certificate file example

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxvs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+
j2kcubVpsE2cgHdj4v8H6jUz9ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+
g92cL8IGOkjgvlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nx
Jf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiN
Y7yZlo2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

## Private key file example

```
-----BEGIN RSA PRIVATE KEY-----
xxxxxxxxxxxxtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThL
yvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQ
ra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/
3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw==
```



```
-----END RSA PRIVATE KEY-----
```

6. Click **OK**.

## Result

After the certificate is uploaded, the certificate status becomes Updated.

## 8.1.7 Create a custom TLS policy

Anti-DDoS Pro and Anti-DDoS Premium support custom transport layer security (TLS) policies for you to choose TLS protocols as required.

### Prerequisites

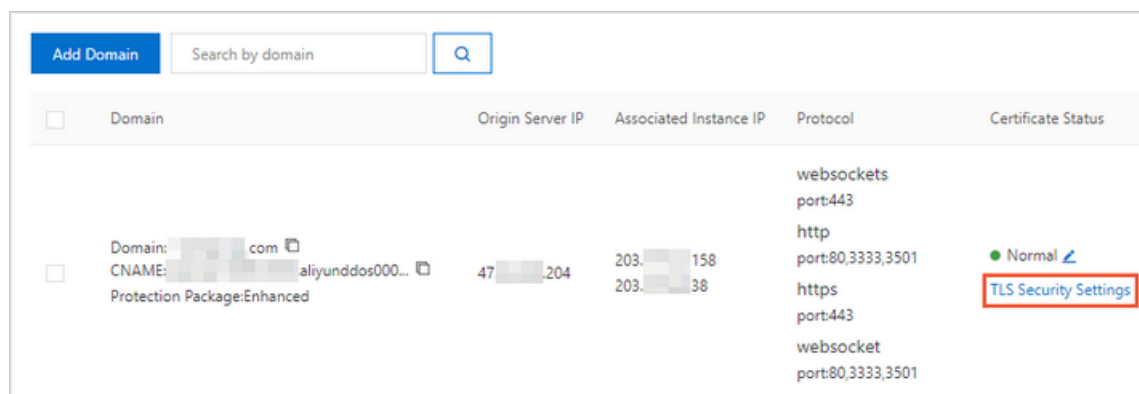
- A website is added to Anti-DDoS Pro or Anti-DDoS Premium and associated with an instance that uses the enhanced function plan. For more information, see [Add a website](#).
- The website supports the HTTPS protocol, and the required HTTPS certificate is uploaded. For more information, see [Upload an SSL certificate](#).

### Context

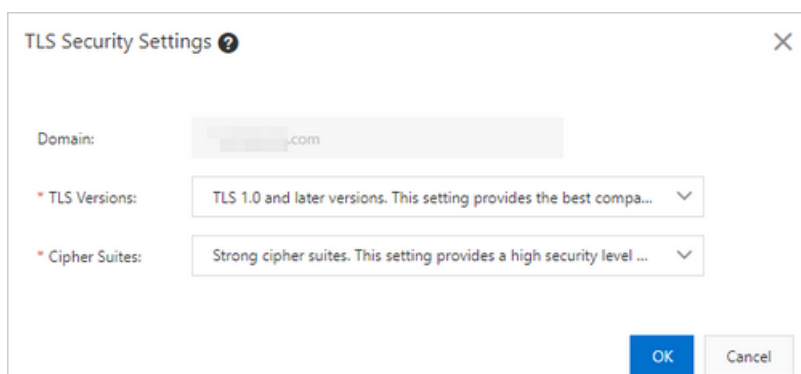
If one of your services needs to comply with PCI DSS 3.2, you must disable TLS 1.0 for the service. However, the terminals of the another services only support TLS 1.0. To address this issue, you can customize TLS policies for different services.

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Website Config**.
4. Find the domain name for which you want to configure a TLS policy and click **TLS Security Settings** in the Certificate Status column.



5. In the **TLS Security Settings** dialog box, set **TLS Versions** and **Cipher Suites**, and click **OK**.



- **TLS Versions**

- **TLS1.0 and later versions. This setting provides the best compatibility but a low security level.** This is the default setting
- **TLS1.1 and later versions. This setting provides a good compatibility and a medium security level.**
- **TLS1.2 and later versions. This setting provides a good compatibility and a high security level.**

- **Cipher Suites**

- **Strong cipher suites. This setting provides a high security level but a low compatibility.**

The following strong cipher suites are supported:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-WITH-CHACHA20-POLY1305
- ECDHE-RSA-WITH-CHACHA20-POLY1305
- ECDHE-RSA-AES256-CBC-SHA
- ECDHE-RSA-AES128-CBC-SHA
- ECDHE-ECDSA-AES256-CBC-SHA
- ECDHE-ECDSA-AES128-CBC-SHA

- **All cipher suites. This setting provides a low security level but a high compatibility.**

The following weak cipher suites are supported:

- RSA-AES256-CBC-SHA
- RSA-AES128-CBC-SHA
- ECDHE-RSA-3DES-EDE-CBC-SHA
- RSA-3DES-EDE-CBC-SHA

## 8.1.8 Website configurations in an XML file

You can export, modify, or import multiple website configurations at a time by using an XML file. This topic describes how to configure a website in an XML file.


### Parameters


The website configurations in an XML file start with the `<DomainList>` tag, end with the `</DomainList>` tag, and include the parameters for multiple websites between the `<DomainList>` tag pair. The configurations for each website start with the `<DomainConfig>` tag, ends with the `</DomainConfig>` tag, and include parameters for each website between the `<DomainConfig>` tag pair.



#### Note:

An extra tag pair `<DomainConfig>..... </DomainConfig>` is required for each additional website configuration.

Parameter	Description
<code>&lt;Domain&gt;a.com&lt;/Domain&gt;</code>	The domain name that you want to associate with an Anti-DDoS Pro or Anti-DDoS Premium instance. You can enter only one domain name in a tag pair.
<code>&lt;ProtocolConfig&gt;&lt;ProtocolList&gt;http,https&lt;/ProtocolList&gt;&lt;/ProtocolConfig&gt;</code>	The protocol type of the domain name. You can separate multiple protocol types with commas (,). In this example, the protocol types of the domain name are HTTP and HTTPS.
<code>&lt;InstanceConfig&gt;&lt;InstanceList&gt;ddoscoo-cn-xxxxxxxxx001&lt;/InstanceList&gt;&lt;/InstanceConfig&gt;</code>	<p>The instances that you want to associate with the domain name.</p> <div>  <b>Note:</b> Each instance has a unique ID. Enter the instance IDs between the <code>&lt;InstanceList&gt;</code> tag pair. Separate multiple instance IDs with commas (,).         </div>

Parameter	Description
<pre>&lt;RealServerConfig&gt;&lt;ServerType&gt;0 &lt;/ServerType&gt;&lt;ServerList&gt;1.x.x.4&lt;/ ServerList&gt;&lt;/RealServerConfig&gt;</pre>	<p>The information of the origin server. The configurations include the following parameters:</p> <ul style="list-style-type: none"> <li><code>&lt;ServerType&gt;0&lt;/ServerType&gt;</code>: identifies origin servers by using IP addresses.</li> <li><code>&lt;ServerType&gt;1&lt;/ServerType&gt;</code>: identifies origin servers by using domain names.</li> </ul> <p><code>&lt;ServerList&gt;1.x.x.4&lt;/ServerList&gt;</code>: the addresses of the origin server. Separate multiple addresses with commas (,)</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <b>Note:</b>          To associate the domain name of an origin server with an instance, you can use either the IP address or the domain name of an origin server.       </div>

### Example

```
<DomainList>
<DomainConfig>
<Domain>a.com</Domain>
<ProtocolConfig>
<ProtocolList>http,https</ProtocolList>
</ProtocolConfig>
<InstanceConfig>
<InstanceList>ddoscoo-cn-xxxxxxxxx001</InstanceList>
</InstanceConfig>
<RealServerConfig>
<ServerType>0</ServerType>
<ServerList>1.x.x.4</ServerList>
</RealServerConfig>
</DomainConfig>
<DomainConfig>
<Domain>b.com</Domain>
<ProtocolConfig>
<ProtocolList>http,websocket,websockets</ProtocolList>
</ProtocolConfig>
<InstanceConfig>
<InstanceList>ddoscoo-cn-xxxxxxxxx002,ddoscoo-cn-xxxxxxxxx00d</InstanceList>
</InstanceConfig>
<RealServerConfig>
<ServerType>1</ServerType>
<ServerList>q840a82zf2j23afs.xxxxxxxxx.com</ServerList>
</RealServerConfig>
</DomainConfig>
</DomainList>
```

In this example, the following website configurations are added:

- The domain name is a.com. The protocols are HTTP and HTTPS. The associated instance is ddoscoo-cn-xxxxxxxxx001. The IP address of the origin server is 1.x.x.4.
- The domain name is b.com. The protocols are HTTP, WebSocket, and WebSockets. The associated instances are ddoscoo-cn-xxxxxxxxx002 and ddoscoo-cn-xxxxxxxxx00ddoscoo-cn-xxxxxxxxx001. The domain name of the origin server is q840a82zf2j23afs.xxxxxxxxx.com.

## 8.2 Use ports

### 8.2.1 Create forwarding rules

To use Anti-DDoS Pro or Anti-DDoS Premium to protect your non-website services, you must create forwarding rules on the Port Config page. You can also configure Layer 4 anti-DDoS protection, such as session persistence, health checks, and anti-DDoS protection policies. You can manage multiple forwarding rules at a time.

#### Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see [Purchase Anti-DDoS Pro or Anti-DDoS Premium instances](#).



#### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

#### Create a forwarding rule

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China**: Anti-DDoS Pro
  - **Outside Mainland China**: Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning** > **Port Config**.

4. On the **Port Config** page, select the instance that you want to manage and click **Create Rule**.

Port Settings

Product Updates Buy Instance

203.132 Forwarding Port You can create a maximum of 50 rules. You have already created 6 rules. Create Rule

	Forwarding Protocol	Forwarding Port	Origin Server Port	Forwarding Mode	Origin Server IP	Session Persistence	Health Check	Anti-DDoS Protection Policy	Actions
<input type="checkbox"/>	TCP	80	80	--	--	--	--	--	--
<input type="checkbox"/>	TCP	443	443	--	--	--	--	--	--

**Note:**

You can also create multiple rules at a time. For more information, see [Create multiple forwarding rules at a time](#).

5. In the **Create Rule** dialog box, set the parameters and click **Complete**.

Create Rule

Note: if the port provides HTTP or HTTPS service, we recommend you to use the website configurations. This greatly improve the protection of the 7-layer HTTP flood attack for the HTTP or HTTPS service. The website configuration now supports adding non-standard ports. [Click to view supported non-standard ports](#)

\* Forwarding ☒ TCP ☐ UDP

Protocol:

\* Forwarding Port:

\* Origin Server Port:



Forwarding Mode: Round-robin

\* Origin Server IP:

Separate multiple IP addresses with commas (.). You can add a maximum of 20 IP addresses.

Complete Cancel

Parameter	Description
<b>Forwarding Protocol</b>	The protocol that you want to use to forward traffic. Valid values: <b>TCP</b> and <b>UDP</b> .

Parameter	Description
<b>Forwarding Port</b>	<p>The port that you want to use to forward traffic.</p> <div>  <b>Note:</b> <ul style="list-style-type: none"> <li>We recommend that you set the forwarding port to the port of the origin server.</li> <li>To prevent domain owners from creating their own DNS servers with protection features, Anti-DDoS Pro and Anti-DDoS Premium do not protect the transport-layer services that use port 53.</li> <li>You cannot specify a port that is already used as the forwarding port by another rule. In an instance, forwarding rules that use the same protocol must use different forwarding ports. If you attempt to create a rule with a protocol and forwarding port that is already used by another rule, an error message appears, which indicates that these rules overlap. Do not create a rule that overlaps with the forwarding rules that are automatically generated when a website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see <a href="#">Automatically generate forwarding rules for website services</a>.</li> </ul> </div>
<b>Origin Server Port</b>	The port of the origin server that you want to use to create the rule.
<b>Origin Server IP</b>	<p>The IP address of the origin server that you want to use to create the rule.</p> <div>  <b>Note:</b> <p>You can specify a maximum of 20 origin server IP addresses to implement load balancing. Separate multiple IP addresses with commas (,).</p> </div>

You can view the created rule on the Port Config page.

### Create multiple forwarding rules at a time

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.

4. On the **Port Config** page, select the instance that you want to manage, click **Batch Operation** below the rule list, and select **Create Rule**.
5. In the **Create Rule** dialog box, enter the required information as shown in the sample file and click **OK**.

Create Rule

tcp 90 91 192.136.12.41  
udp 22 13 12.14.1.23,10.23.4.12

Sample File:

tcp 90 91 192.136.12.41  
udp 22 13 12.14.1.23,10.23.4.12

ddoscoo.layer4.add\_rulesHtml

Create Cancel

The format is described as follows:

- Each row represents a rule.
  - From left to right, the fields in each rule indicate the following parameters:  
forwarding protocol, forwarding port, origin server port, origin server IP address.  
Fields are separated with spaces. For more information about the parameters, see [rule parameters](#).
6. Confirm the entered information, select the rules that you want to create, and click **OK**.

Create Rule

Confirm the fields you have entered. Click here to change the field values.

<input type="checkbox"/>	Forwarding Protocol/Port	Origin Server Port	Forwarding Mode	Origin Server IP	Status
<input type="checkbox"/>	tcp:90	91	Round-robin	192.136.12.41	

OK Cancel

7. After the rules are uploaded, close the **Create Rule** dialog box. You can view the created rules on the Port Config page.



## What to do next

After you create forwarding rules, you can change the IP addresses of your services to the IP addresses of instances to reroute their traffic. We recommend that you use a local machine to verify that the forwarding rules take effect before you switch your service traffic to instances. For more information, see [Verify the forwarding configuration on your local machine](#).



### Notice:

If you switch your service traffic to instances before the forwarding rules take effect, your services may be interrupted.

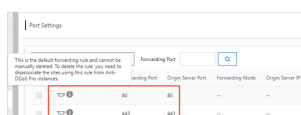
After you create forwarding rules, you can perform the following operations on the **Port Config** page.

- Configure Layer 4 anti-DDoS protection, such as session persistence, health checks, and anti-DDoS protection policies. For more information, see [Configure a forwarding rule](#).
- Edit or delete rules. For more information, see [Edit forwarding rules](#) and [Delete forwarding rules](#).
- Export multiple forwarding rules and Layer 4 anti-DDoS protection settings at a time. For more information, see [Export multiple port configurations](#).

## Automatically generate forwarding rules for website services

After you add a domain name to an instance, Anti-DDoS Pro or Anti-DDoS Premium generates a forwarding rule for the instance. For more information about how to add a domain name, see [Add a website](#).

- If you specify port 80 of the origin server when you add a domain name to an instance, Anti-DDoS Pro or Anti-DDoS Premium generates a rule that forwards traffic to the origin server over port 80 by using TCP.
- If you specify port 443 of the origin server when you add a domain name to an instance, Anti-DDoS Pro or Anti-DDoS Premium generates a rule that forwards traffic to the origin server over port 443 by using TCP.
- Anti-DDoS Pro and Anti-DDoS Premium do not generate rules that have already been generated for another website.



You cannot modify or delete a rule that is automatically generated when you add a website to Anti-DDoS Pro or Anti-DDoS Premium. Automatically generated rules are automatically deleted only after all the websites where the rules are applied are disassociated from instances.

## 8.2.2 Edit forwarding rules

You can modify the IP addresses of origin servers only for manually created forwarding rules. You cannot perform this operation on automatically generated rules. To modify the IP address of an origin server, you can edit the forwarding rule. If the forwarding protocol and port of a rule are changed, we recommend that you create a forwarding rule. This topic describes how to edit one or more forwarding rules.

### Prerequisites

Forwarding rules are created for the Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see [Create forwarding rules](#).

### Edit a forwarding rule

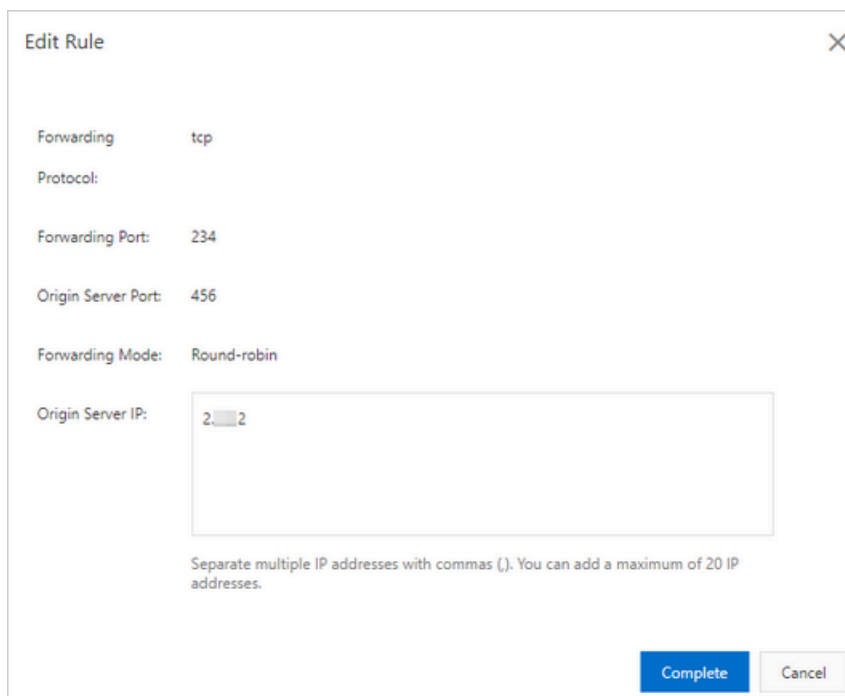
1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.
4. On the **Port Config** page, select the instance that you want to manage.
5. Find the rule that you want to edit and click **Edit** in the Actions column.



#### Note:

If you use Anti-DDoS Pro, you can edit multiple rules at a time. For more information, see [Edit multiple forwarding rules at a time](#).

6. In the **Edit Rule** dialog box, change the value of **Origin Server IP** and click **Complete**.



2.2.2

Separate multiple IP addresses with commas (.). You can add a maximum of 20 IP addresses.

After you change the IP address of the origin server in a rule, Anti-DDoS Pro or Anti-DDoS Premium forwards service traffic based on the new rule.

### Edit multiple forwarding rules at a time



#### Note:

Only Anti-DDoS Pro allows you to edit multiple forwarding rules at a time.

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select **Mainland China**.
3. In the left-side navigation pane, choose **Provisioning > Port Config**.
4. On the **Port Config** page, select the Anti-DDoS Pro instance that you want to manage, click **Batch Operation** below the rule list, and select **Edit Rule**.

5. In the **Edit Rule** dialog box, enter new information for the rules and click **OK**.

tcp 90 91 192.168.1.41  
udp 22 13 12.34.56.12

Sample File:(Batch Rules Edit only supports editing the origin IPs.)

tcp 90 91 192.168.1.41  
udp 22 13 12.34.56.12

Edit Cancel

The format is described as follows:

- Each row represents a rule.
- From left to right, the fields in each rule indicate the following parameters:  
forwarding protocol, forwarding port, origin server port, and origin server IP address.  
Fields are separated with spaces. For more information about the parameters, see [rule parameters](#).



**Note:**

You can only modify the IP addresses of origin servers.

6. Confirm the entered information, select the rules that you want to edit, and click **OK**.

Confirm the fields you have entered. Click here to change the field values.

<input type="checkbox"/>	Forwarding Protocol/Port	Origin Server Port	Forwarding Mode	Origin Server IP	Status
<input type="checkbox"/>	tcp:90	91	Round-robin	192.168.1.41	

OK Cancel

7. Close the **Edit Rule** dialog box.

### 8.2.3 Delete forwarding rules

You can delete manually created forwarding rules that are no longer required. Before this operation, ensure that inbound traffic is no longer rerouted to Anti-DDoS Pro or Anti-DDoS Premium instances. If you delete a forwarding rule before you restore the IP address of your

service from that of your Anti-DDoS Pro or Anti-DDoS Premium instance to the actual IP address, your service may be interrupted.

### Prerequisites

The IP address of your service is restored from that of your Anti-DDoS Pro or Anti-DDoS Premium instance to the actual IP address.

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.
4. On the **Port Config** page, select the instance that you want to manage.
5. Find the rule that you want to delete and click **Delete** in the Actions column.



#### Note:

To delete multiple rules at a time, select the rules and click **Batch Delete** below the rule list.

6. In the message that appears, click **OK**.

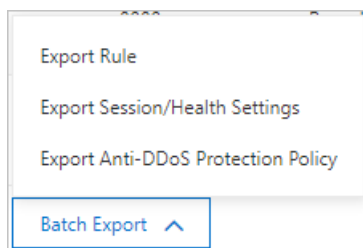
## 8.2.4 Export multiple port configurations

Anti-DDoS Pro and Anti-DDoS Premium allow you to export multiple port configurations at a time. You can export manually created forwarding rules, session and health check settings, and anti-DDoS protection policies under an Anti-DDoS Pro or Anti-DDoS Premium instance as a TXT file. You can also download the file to your local machine. The exported file has the same format as the file used to manage multiple rules, session and health check settings, and anti-DDoS protection policies.

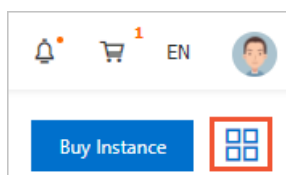
### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.

4. On the **Port Config** page, select the target instance.
5. Below the rule list, click **Batch Export** and select **Export Rule**, **Export Session/Health Settings**, or **Export Anti-DDoS Protection Policy** as required.



6. After the export task is delivered, click the Tasks icon in the upper-right corner of the page.



7. In the **Tasks** pane, click **Download** in the Actions column that corresponds to the export record after the export task is completed.

**Note:**

If the task is in the **Pending Export** state, wait until the task is completed.

Tasks			
Name	Status	Start Time	Actions
Layer 4 Export_ddoscoo-cn-o401...	● Exported	03/06/2020, 10:15:40	<a href="#">Delete</a> <a href="#">Download</a>

After the exported file is downloaded to your local machine, you can open the TXT file to view the rules or settings. For more information about the format in the TXT file, see [The format of content in the files](#).

8. Optional: In the **Tasks** pane, find the task that you want to delete and click **Delete** in the Actions column.

### The format of content in the files

All exported files are in TXT format. The format in the files varies with the exported content.

**Note:**

If you use Anti-DDoS Pro, the name of the exported file starts with DDoSCoo\_. If you use Anti-DDoS Premium, the name of the exported file starts with DDoSDip\_. The formats of the files exported from the Anti-DDoS Pro and Anti-DDoS Premium consoles are the same.

- Rule files

Each row represents a rule that contains four values. From left to right, the fields in each rule indicate the following parameters: forwarding protocol, forwarding port, origin server port, and origin server IP address.

```
tcp 90 91 192.168.1.41
tcp 123 123 1.1.1.2
tcp 888 2222 1.1.1.1
udp 3999 3999 1.1.1.4
```

For more information, see [Create multiple forwarding rules at a time](#).

- Files of session and health check settings

Each row represents a rule. From left to right, the fields in each rule indicate the following parameters: forwarding port, forwarding protocol, session persistence timeout, health check type, port, response timeout period, check interval, unhealthy threshold, healthy threshold, path, and domain. If the value of session persistence timeout is 0, session persistence is disabled. If no value is specified for the health check type, the health check is disabled, and the values that follow the parameter are left blank. The values of path and domain are only provided for HTTP-based health checks.

```
90 tcp 0
123 tcp 0
888 tcp 0
8080 tcp 400 http 22 5 3 3 /search.php example.com
```

For more information, see [Configure session persistence or health checks for multiple rules at a time](#).

- Files of anti-DDoS protection policies

Each row represents a rule. From left to right, the fields in each rule indicate the following parameters: forwarding port, forwarding protocol, source new connection rate limit, source concurrent connection rate limit, destination new connection rate limit, destination concurrent connection rate limit, minimum packet length, maximum packet length, and false source and empty connection. The value of the last field applies only when TCP is used. You must turn on False Source before you turn on Empty Connection.

```
90 tcp 20000 50000 0 0 1 6000 on off
123 tcp 0 0 100000 0 0 6000 on on
888 tcp 20000 0 0 0 0 6000 on off
8080 tcp 1 1 100 1000 0 6000 on off
```

For more information, see [Create anti-DDoS protection policies for multiple port forwarding rules at a time](#).

## 8.2.5 Configure a health check

Anti-DDoS Pro and Anti-DDoS Premium provide Layer 4 and Layer 7 health checks for protected non-website services. The health check feature is suitable for any service that has multiple origin server IP addresses and needs to check the availability of the origin servers. After you add forwarding rules to an Anti-DDoS Pro or Anti-DDoS Premium instance and use the instance to protect a non-website service, you can configure session persistence or health checks for a specific rule or multiple rules at a time. This topic describes how to configure a health check.

### Prerequisites

A port forwarding rule for a non-website service is configured on the Port Config page. For more information, see [Create forwarding rules](#).

### Context

The health check feature is suitable for any service that has multiple origin server IP addresses. When Anti-DDoS Pro or Anti-DDoS Premium forwards traffic to origin servers, health checks are used to verify the availability of origin servers. Traffic is forwarded to the healthy origin servers to make sure that the service runs properly. If you configure only one origin server IP address in a port forwarding rule, we recommend that you do not enable the health check feature. For more information, see [Health check overview](#).

The port configuration feature of Anti-DDoS Pro and Anti-DDoS Premium provides protection against DDoS attacks based on IP addresses and ports. The health check feature is available to all IP addresses and ports that are protected by Anti-DDoS Pro or Anti-DDoS Premium instances. You can configure health checks for forwarding ports of Anti-DDoS Pro or Anti-DDoS Premium instances.




Anti-DDoS Pro and Anti-DDoS Premium allow you to configure Layer 4 and Layer 7 health checks. The following table describes the parameters.



#### Note:

For advanced settings, click **Advanced Settings**. We recommend that you use the default settings. You can configure advanced settings for Layer 4 and Layer 7 health checks. Both health checks have the same parameters.



Type	Parameter	Description
Layer 4 Health Check	Port	<p>The port that is used to access the origin servers during health checks. The valid value ranges from 1 to 65535. By default, the backend port configured for the listener is used.</p> <div>  <b>Note:</b>            The Layer 4 health check is suitable for TCP and UDP forwarding rules.         </div>
	Domain and Path.	<p>During a Layer 7 health check, the Anti-DDoS Pro or Anti-DDoS Premium forwarding system sends an HTTP HEAD request to the default homepage of the origin server.</p> <div>  <b>Note:</b>            The Layer 7 health check is suitable only for TCP forwarding rules and HTTP health checks.         </div> <ul style="list-style-type: none"> <li>If you do not want to use the default homepage of the origin server for health checks, you must specify a domain name and path of the page that you want to check.</li> <li>If you have limited the host field for the HTTP HEAD request, you only need to specify the URI for health checks. The Domain parameter is optional and set to the domain name of the origin server by default.</li> </ul>
Advanced Settings	Port	The port that is used to access the origin servers during health checks. The valid value ranges from 1 to 65535. By default, the backend port configured for the listener is used.
	Response Timeout Period	The timeout period of a health check. The valid value ranges from 1 to 30 seconds. If the origin server does not respond within the specific timeout period, the origin server is unhealthy.
	Check Interval	<p>The time interval between two health checks. The valid value ranges from 1 to 30 seconds.</p> <div>  <b>Note:</b>            Each scrubbing node in a cluster performs health checks on origin servers at specific intervals independently and concurrently. Scrubbing nodes may perform health checks on the same origin server at different times. Therefore, the health check records on the origin server do not indicate the time interval specified for the health check.         </div>

Type	Parameter	Description
	<b>Unhealthy Threshold</b>	The number of consecutive failed health checks performed by the same scrubbing node that must occur before an origin server is declared unhealthy. The valid value ranges from 1 to 10.
	<b>Healthy Threshold</b>	The number of consecutive successful health checks performed by the same scrubbing node that must occur before an origin server is declared healthy. The valid value ranges from 1 to 10.

### Configure a health check for a port

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.
4. On the **Port Config** page, select the target instance, find the target forwarding rule, and click **Change** in the **Health Check** column.



#### Note:

You can also configure session persistence or health checks for multiple rules at a time. For more information, see [Configure session persistence or health checks for multiple rules](#).

203.132.132.132	Forwarding Port	Q	You can create a maximum of 50 rules. You				
<input type="checkbox"/>	Forwarding Protocol	Forwarding Port	Origin Server Port	Forwarding Mode	Origin Server IP	Session Persistence	Health Check
<input type="checkbox"/>	TCP ⓘ	80	80	--	--	--	--
<input type="checkbox"/>	TCP ⓘ	443	443	--	--	--	--
<input type="checkbox"/>	TCP	234	456	Round-robin	2.2.2.2	● Disabled <a href="#">Change</a>	● Disabled <a href="#">Change</a>

5. In the **Health Check** dialog box, set the parameters and click **Complete**. For more information about the parameters, see [Health check parameters](#).

## Configure session persistence or health checks for multiple rules

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.
4. On the **Port Config** page, select the target instance, click **Batch Operations** below the rule list, and select **Session Persistence/Health Check Settings**.
5. In the **Create Session/Health Settings** dialog box, enter the required information and click **Create**.



**Note:**

You can export health check settings to a TXT file, modify the settings in the TXT file, and then copy and paste the settings to the Create Session/Health Settings dialog box. In the TXT file, keep the settings of all rules in the same format. For more information, see [Export multiple port configurations](#).

The formats of session persistence and health check settings are described as follows:

- Enter the session persistence and health check settings of each forwarding rule in each row.
- Health check settings include the following fields left to right: forwarding port, forwarding protocol (TCP or UDP), session persistence period, health check type, port, response timeout period, check interval, unhealthy threshold, healthy threshold, path, and domain. The session persistence period is measured in seconds, and the valid value ranges from 30 to 3600. Fields are separated with spaces. For more information about the fields, see [Health check parameters](#).
- The forwarding port must be specified in forwarding rules.
- Health check types include TCP, HTTP, and UDP. If a forwarding rule uses UDP, we recommend that you configure a UDP health check. If a forwarding rule uses TCP, we recommend that you configure a TCP health check (Layer 4 health check) or HTTP health check (Layer 7 health check).
- If you configure an HTTP health check, the Path parameter is required, but the Domain parameter is optional.

## 8.2.6 Configure session persistence

Anti-DDoS Pro and Anti-DDoS Premium both allow you to configure the session persistence feature for protected non-website service. Session persistence forwards requests from the same client to the same server within a specific period. After you add forwarding rules to an Anti-DDoS Pro or Anti-DDoS Premium instance and associate the instance with a non-website service, you can configure session persistence or health checks for a port forwarding rule or multiple rules at a time.

### Prerequisites

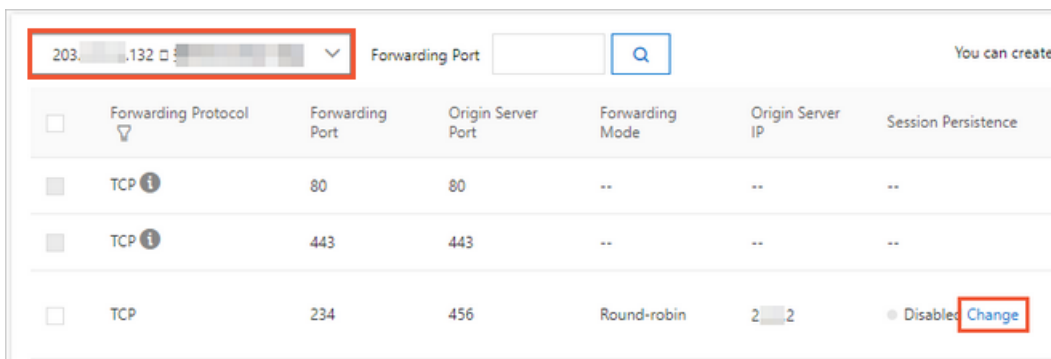
A port forwarding rule for a non-website service is configured on the Port Config page. For more information, see [Create forwarding rules](#).

### Context

Anti-DDoS Pro and Anti-DDoS Premium provide protection against DDoS attacks based on IP addresses and ports. The session persistence feature is available to all non-website service. You can configure session persistence for the forwarding port of a specific instance.

### Configure session persistence for ports

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.
4. On the **Port Config** page, select the instance for which you want to configure session persistence, find the target forwarding rule, and click **Change** in the **Session Persistence** column.



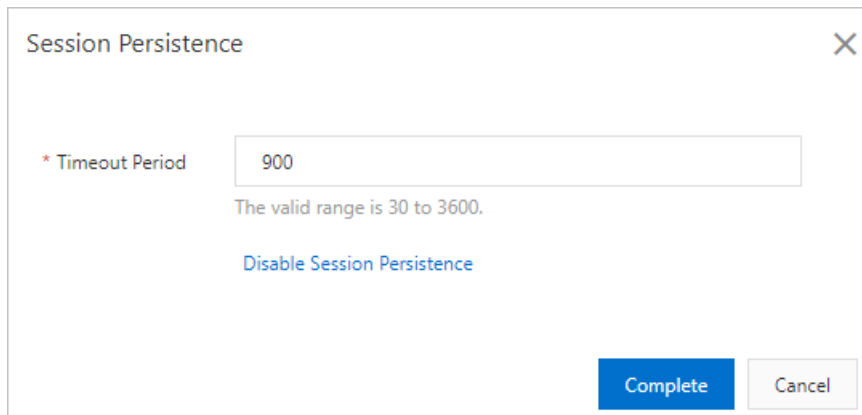
<input type="checkbox"/>	Forwarding Protocol	Forwarding Port	Origin Server Port	Forwarding Mode	Origin Server IP	Session Persistence
<input type="checkbox"/>	TCP ⓘ	80	80	--	--	--
<input type="checkbox"/>	TCP ⓘ	443	443	--	--	--
<input type="checkbox"/>	TCP	234	456	Round-robin	2.2	Disabled <a href="#">Change</a>



#### Note:

You can also configure session persistence for multiple forwarding rules of an instance at a time. For more information, see [Configure session persistence or health checks for multiple rules at a time](#).

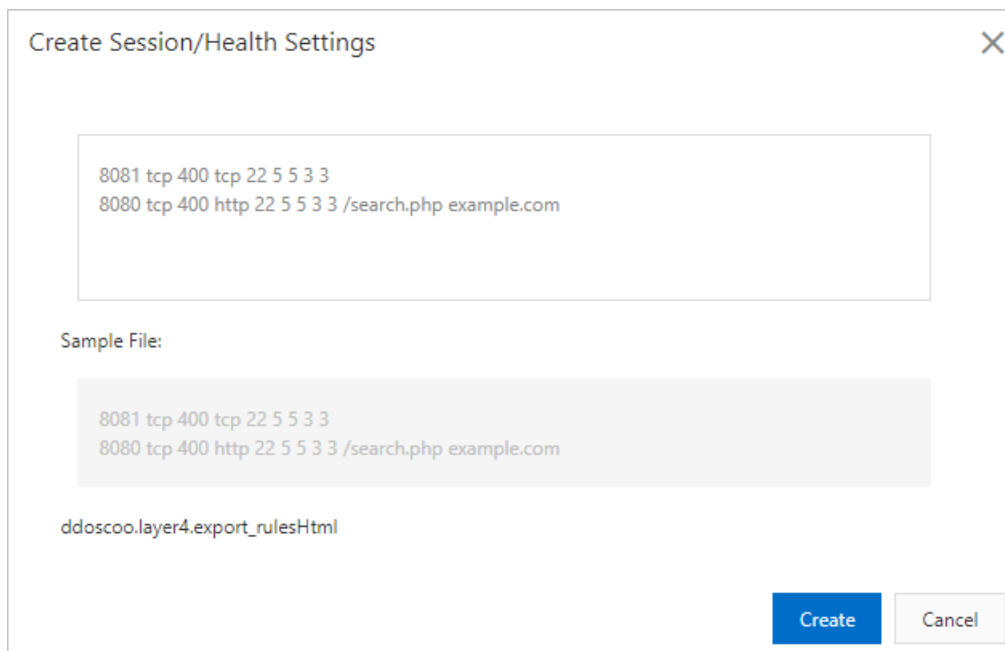
5. In the **Session Persistence** dialog box, set **Timeout Period** and click **Complete**. The timeout period is measured in seconds, and the valid value ranges from 30 to 3600.

A screenshot of the 'Session Persistence' dialog box. The dialog has a title bar with a close button (X). Inside, there is a label '\* Timeout Period' followed by a text input field containing the value '900'. Below the input field, a message states 'The valid range is 30 to 3600.' and there is a blue link 'Disable Session Persistence'. At the bottom right, there are two buttons: 'Complete' (blue) and 'Cancel' (gray).

### Configure session persistence or health checks for multiple rules at a time

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.
4. On the **Port Config** page, select the target instance, click **Batch Operations** below the rule list, and select **Session Persistence/Health Check Settings**.

5. In the **Create Session/Health Settings** dialog box, enter the required information and click **Create**.



Create Session/Health Settings

8081 tcp 400 tcp 22 5 5 3 3  
8080 tcp 400 http 22 5 5 3 3 /search.php example.com

Sample File:

8081 tcp 400 tcp 22 5 5 3 3  
8080 tcp 400 http 22 5 5 3 3 /search.php example.com

ddoscoo.layer4.export\_rulesHtml

Create Cancel

**Note:**

You can export health check settings to a TXT file, modify the settings in the TXT file, and then copy and paste the settings to the Create Session/Health Settings dialog box. In the TXT file, keep the settings of all rules in the same format. For more information, see [Export multiple port configurations](#).

The format of configurations for session persistence or health check is described as follows:

- Enter the session persistence and health check settings of each forwarding rule in each row.
- From left to right, each configuration of session persistence and health check contains the following fields: forwarding port, forwarding protocol, session persistence period, health check type, port, health check timeout period, check interval, unhealthy threshold, healthy threshold, path, and domain. The forwarding protocol can be TCP or UDP. The session persistence period is measured in seconds, and the valid value ranges from 30 to 3600. Fields are separated with spaces. For more information about the fields, see [Health check parameters](#).
- The forwarding port must be specified in forwarding rules.
- Health check types include TCP, HTTP, and UDP. If a forwarding rule uses UDP, we recommend that you configure a UDP health check. If a forwarding rule uses TCP, we

recommend that you configure a TCP health check (Layer 4 health check) or HTTP health check (Layer 7 health check).

- If you configure an HTTP health check, the Path parameter is required, but the Domain parameter is optional.

## 8.3 Provisioning settings

### 8.3.1 Modify DNS records to protect websites

After you add a website to Anti-DDoS Pro or Anti-DDoS Premium, you must modify the DNS records of the website to reroute the inbound traffic of the website to an Anti-DDoS Pro or Anti-DDoS Premium instance. This topic describes how to modify the DNS records of a website. DNS records can be CNAME records or the A records. In this example, the DNS resolution service is provided by Alibaba Cloud DNS.

#### Prerequisites

- A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Add a website](#).
- The back-to-origin IP addresses of instances are added to the whitelist of the origin server. If you deploy third-party security software on your origin server, such as a firewall, add the back-to-origin IP addresses to the whitelist of the security software. For more information, see [Allow back-to-origin IP addresses to access the origin server](#).
- The traffic forwarding settings take effect. Before you switch service traffic to Anti-DDoS Pro or Anti-DDoS Premium, we recommend that you verify that the instances can forward inbound traffic to the origin server on your local machine. For more information, see [Verify the forwarding configuration on your local machine](#).

#### Select a DNS record type

When you modify the DNS records of your website, you can choose to modify the CNAME or A record to reroute network traffic to the CNAME record or IP address of an associated instance.



#### Note:

You can query the CNAME record and IP address of an associated instance on the **Website Config** page.



<div> <div>Add Domain</div> <div>Search by domain</div> <div>Q</div> </div>		
<input type="checkbox"/>	Domain	Origin Server IP
<input type="checkbox"/>	Domain: <span>...</span> .com	
<input type="checkbox"/>	CNAME: <span>...</span> .aliyunddos000...	47. <span>...</span> .204
	Protection Package: Enhanced	
		Associated Instance IP
		203. <span>...</span> 158
		203. <span>...</span> 38

- If you choose to use the CNAME record, you can modify DNS records just for once. If the IP address of the instance changes, Anti-DDoS Pro or Anti-DDoS Premium automatically reroutes traffic based on the CNAME record. If your website is associated with multiple instances, Anti-DDoS Pro or Anti-DDoS Premium automatically schedules traffic and reroutes it to the IP addresses of the instances.
- If you choose to use the A record, you must modify DNS records each time the IP address of the instance changes. If your website is associated with multiple instances, you must manually schedule traffic and reroute traffic to the IP addresses of the instances.

We recommend that you use the CNAME record in most cases and use the A record only if the CNAME record is unavailable or conflicts with other DNS records.

## Procedure

In the following example, the domain name is managed by [Alibaba Cloud DNS](#).



### Note:

Alibaba Cloud DNS provides basic DNS services for free and offers other value-added services in the paid edition. If you activated the value-added services of Alibaba Cloud DNS in the paid edition for your website, we recommend that you enable NS Mode Access to reroute traffic to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Enable NS Mode Access to protect a website](#).

If you use third-party DNS services, log on to the system of the DNS provider to modify the DNS records. The following example is for reference only.

Assume that the domain name of your website associated with an instance is `bgp.ddostest.com`. The following procedure describes how to modify and add DNS records in the Alibaba Cloud DNS console.

1. Log on to the [Alibaba Cloud DNS console](#).

2. On the **Manage DNS** page, find the domain name **ddostest.com** and click **Configure** in the Actions column.

Domains					
<div>Add Domain Name</div>					
<div>ALL Start date ~ End date Domain Name Search</div>					
<input type="checkbox"/>	Domain Name	Records	DNS Server Status	Version	Actions
<input type="checkbox"/>		17	<span>Normal</span>	Free Version	<a href="#">Configure</a> <a href="#">Upgrade</a>
<input type="checkbox"/>	ddostest.com	1	<span>Have not used AlibabaCloudDNS</span>	Free Version	<a href="#">Configure</a> <a href="#">Upgrade</a> <a href="#">More</a>
<input type="checkbox"/>		1	<span>Have not used AlibabaCloudDNS</span>	Free Version	<a href="#">Configure</a> <a href="#">Upgrade</a> <a href="#">More</a>
<div><input type="checkbox"/> Delete <input type="button" value="Change Group"/></div>					Total 3 < 1 > 10 / page

3. On the **DNS Settings** page, find the A record or CNAME record whose Host is **bgp** and click **Edit** in the Actions column.

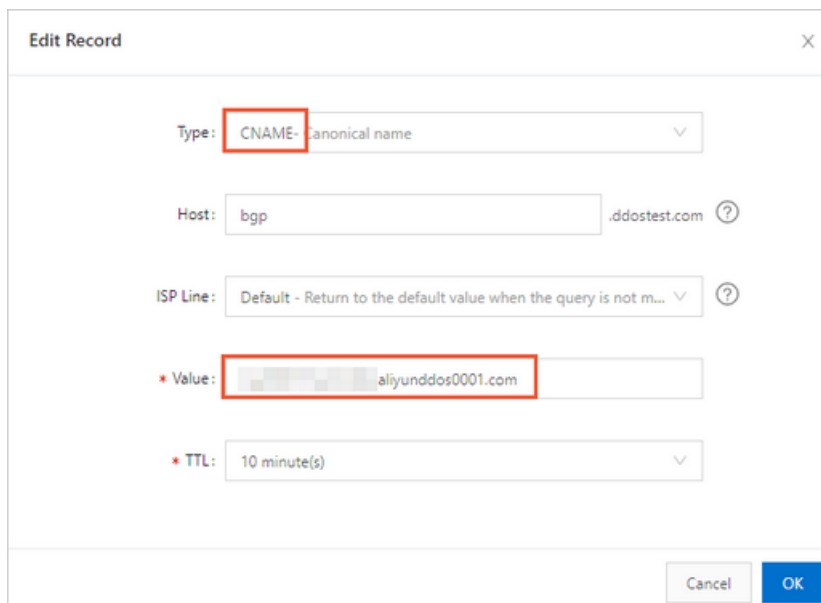
**Note:**

If you cannot find the DNS record that you want to manage in the list, you can click **Add Record** to add the record.

DNS Settings							
<div>Add Record Import &amp; Export Query Volume Getting Started</div>							
<div>ALL Exact Search Search by keyword. Advanced Search</div>							
<input type="checkbox"/>	Host	Type	Line(ISP)	Value	TTL	Status	Remark
<input type="checkbox"/>		CNAME	Default	aliyunddos0001.com	10 minute(s)	Normal	
<div><input type="checkbox"/> Disable <input type="button" value="Enable"/> <input type="button" value="Delete"/> <input type="button" value="Change Group"/></div>							Total 1 < 1 > 10 / page

4. In the **Add Record** or **Edit Record** dialog box, select a record type and modify the record.

- (Recommended) CNAME record: Set **Type** to **CNAME** and set **Value** to the CNAME record of the instance that you want to set to protect the domain name.



- A record: Set **Type** to **A** and set **Value** to the IP address of the instance that you want to set to protect the domain name.



5. Click **OK** and wait for the settings to take effect.

6. Check whether the website can be accessed.

## What to do next

After you add your website to Anti-DDoS Pro or Anti-DDoS Premium, you can perform the following operations:

- Enable Sec-Traffic Manager and configure scheduling rules between Anti-DDoS Pro or Anti-DDoS Premium and protected cloud resources. These rules trigger Anti-DDoS Pro or Anti-DDoS Premium in specific scenarios only. For more information, see [Sec-Traffic Manager](#).
- Change the public IP address of the Elastic Compute Service (ECS) origin server. If the IP address of your origin server is exposed, attackers may bypass Anti-DDoS Pro or Anti-DDoS Premium to attack the origin server. To prevent this, you can change the IP address

of an ECS origin server in the Anti-DDoS Pro or Anti-DDoS Premium console. For more information, see [Change the public IP address of an ECS origin server](#).

### 8.3.2 Enable NS Mode Access to protect a website

After you add a website to Anti-DDoS Pro, you must modify the DNS records of your website to reroute inbound traffic to the Anti-DDoS Pro instance. If you have purchased the paid edition of Alibaba Cloud DNS service for domain name resolution, you can enable NS Mode Access to automatically modify DNS records. This topic describes how to enable NS Mode Access in the Anti-DDoS Pro console.

#### Prerequisites

- An Anti-DDoS Pro instance is purchased.



#### Note:

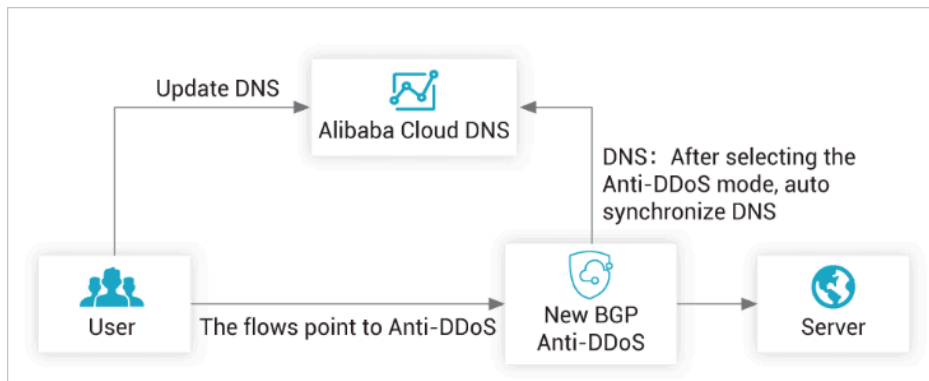
Only Anti-DDoS Pro supports NS Mode Access. If you use Anti-DDoS Premium, we recommend that you modify the DNS records of websites. For more information, see [Modify DNS records to protect websites](#).

- The domain name of your website is managed by the paid edition of Alibaba Cloud DNS. For more information, see [Alibaba Cloud DNS product overview](#).
- A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Add a website](#).
- The back-to-origin IP addresses of instances are added to the whitelist of the origin server. If you deploy third-party security software on your origin server, such as a firewall, add the back-to-origin IP addresses to the whitelist of the security software. For more information, see [Allow back-to-origin IP addresses to access the origin server](#).
- The traffic forwarding settings take effect. Before you switch service traffic to Anti-DDoS Pro or Anti-DDoS Premium, we recommend that you verify that the instances can forward inbound traffic to the origin server on your local machine. For more information, see [Verify the forwarding configuration on your local machine](#).

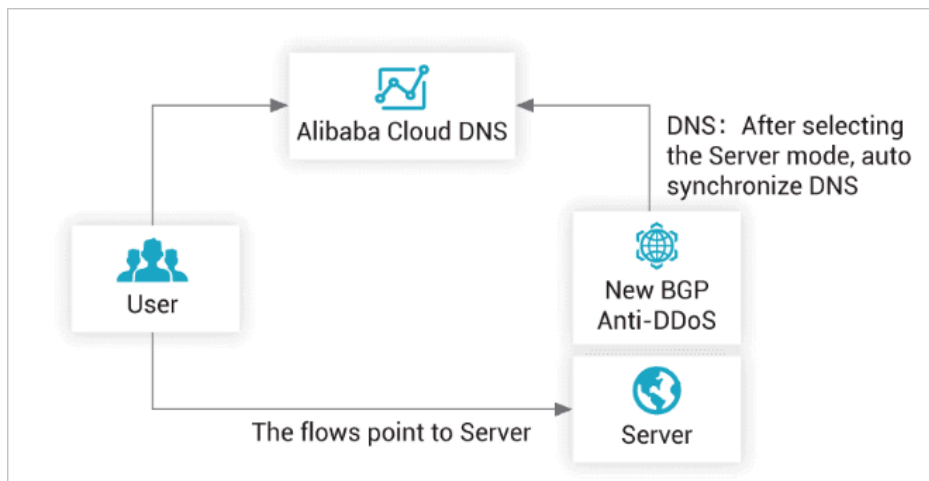
#### Context

After you enable NS Mode Access, Anti-DDoS Pro automatically modifies the DNS records based on the forwarding rules in the website configuration. NS Mode Access supports the following two modes:

- Anti-DDoS: enables Anti-DDoS Pro and automatically modifies DNS records to reroute inbound traffic to the Anti-DDoS Pro instance.



- Back-To-Source: disables Anti-DDoS Pro and forwards the traffic to the origin server.



We recommend that you use the following steps to configure NS Mode Access. If the domain name of your website is managed by a third-party DNS service and cannot be migrated to Alibaba Cloud DNS, NS Mode Access is unavailable. In this case, you must manually modify the DNS records of your website. For more information, see [Modify DNS records to protect websites](#).

#### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select **Mainland China**.
3. In the left-side navigation pane, choose **Provisioning > Website Config**.

4. On the **Website Config** page, find the domain name whose DNS records you want to modify and click **Configure DNS Settings** in the Actions column.

<input type="checkbox"/>	Domain	Origin Server IP	Associated Instance IP	Protocol	Certificate Status	Mitigation Settings	Actions
<input type="checkbox"/>	Domain: [redacted] CNAME: [redacted] Protection Package: Enhanced	47.[redacted].167	203.[redacted].158	http port:80 https port:443	No Certificate TLS Security Settings	HTTP Flood Protection: Normal	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Configure DNS Settings</a> <a href="#">Mitigation Settings</a>

5. On the **Configure DNS Settings** page, find the **NS Mode Access** section, turn on **Status**, and select **Anti-DDoS** or **Back-To-Source** as the access mode.

- If you select the Anti-DDoS mode, Anti-DDoS Pro automatically modifies the DNS records and reroutes inbound traffic to the Anti-DDoS Pro instance.
- If you select the Back-to-Origin mode, Anti-DDoS Pro automatically modifies the DNS records and forwards inbound traffic to the origin server.

NS Mode Access (Recommended, no DNS record change required)

Prerequisite: Service to be accessed must use Alibaba Cloud DNS. For more information, click to view Alibaba Cloud DNS. If your service cannot be accessed through NS mode. Please access the service by manually changing the DNS record. For more information, click to view the configuration guide.

Domain: [redacted]

Status: ☒

Mode: ☒ Anti-DDoS ☐ Back-To-Source

If you have purchased the paid edition of Alibaba Cloud DNS, you can enable this feature. If you did not purchase the paid edition of Alibaba Cloud DNS, an error message appears.

6. Wait for the settings to take effect. You can use a third-party DNS testing platform to check whether a domain name is resolved as expected.

### 8.3.3 Modify the CNAME record to protect a non-website service

To add a non-website service to Anti-DDoS Pro or Anti-DDoS Premium, you must create port forwarding rules and change the IP address of the service to the IP address of an Anti-DDoS Pro or Anti-DDoS Premium instance. In specific scenarios, you may need to use domain names to set up multiple Anti-DDoS Pro instances for Layer 4 services and set up an automatic mechanism to switch service traffic among these instances. In this is the case, we recommend that you add the domain names to Anti-DDoS Pro or Anti-DDoS Premium instances and then modify the CNAME records of the domain names.

#### Context

This example shows how to set up Anti-DDoS Pro for a gaming service whose domain is game.aliyundemo.com, TCP ports are 1234 and 5678, and the origin server IP address is 1.1.1.1.

## Procedure

1. Add the website that you want to protect and obtain the CNAME record assigned to the website.
  - a) Log on to the [Anti-DDoS Pro console](#).
  - b) In the top navigation bar, select the region where your server is deployed.
    - **Mainland China:** Anti-DDoS Pro
    - **Outside Mainland China:** Anti-DDoS Premium
  - c) In the left-side navigation pane, choose **Provisioning > Website Config**.
  - d) On the **Website Config** page, click **Add Domain**.
  - e) On the **Add Domain** wizard, set the parameters in the **Enter Site Information** step and click **Add**.

The parameters are described as follows:

- **Function Plan** and **Instance:** Select the instances with which you want to associate the domain name. In this example, the domain name is associated with two instances that use the enhanced function plan.
- **Domain:** Enter the domain name that you want to protect. In this example, the domain name is game.aliyundemo.com.
- **Protocol** and **Server Port:** Use the default values.
- **Server IP:** Select **Origin Server IP** and enter the IP address of the origin server.
  - If the domain name provides website services, you must specify the actual protocol and IP address of the origin server.
  - If the domain name does not provide website services, you can enter any IP address. The user traffic is rerouted by using the port forwarding rules created in step 2.

For more information, see [Add a website](#).

After you add a domain name, Anti-DDoS Pro or Anti-DDoS Premium assigns a CNAME record to the domain name.



Add Domain

game.aliyundemo.com

Q

<input type="checkbox"/>	Domain	Origin Server IP	Associated Instance IP
<input type="checkbox"/>	Domain: game.aliyundemo.com		
<input type="checkbox"/>	CNAME: .aliyunddos000...	1..1	203. 132
	Protection Package:Enhanced		203. 38

Batch Delete

Batch Domains Import

Batch Domains Edit

Batch Domains Export

## 2. Create a port forwarding rule.

- In the left-side navigation pane, choose **Provisioning** > **Port Config**.
- On the **Port Config** page, select the instance for which you want to create a port forwarding rule and click **Create Rule**.



**Note:**

Select one of the associated instances from step 1.

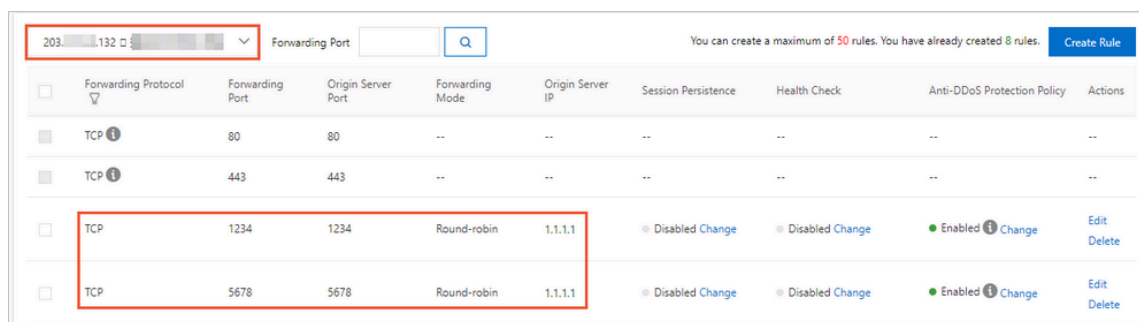
- c) In the **Create Rule** dialog box, specify the required parameters and click **Complete**.

The parameter configurations in this example are described as follows:

- **Forwarding Protocol:** Select TCP.
- **Forwarding Port:** Enter 1234.
- **Origin Server Port:** Enter 1234.
- **Origin Server IP:** Enter 1.1.1.1. This parameter specifies the IP address of the origin server.

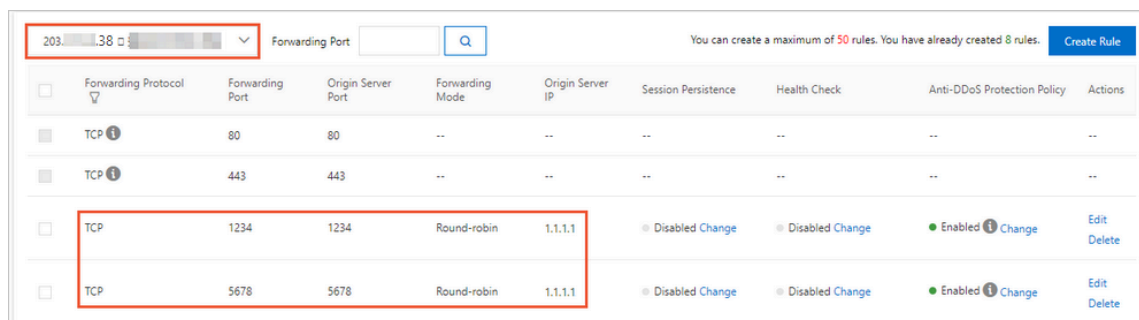
For more information, see [Create forwarding rules](#).

- d) Repeat the preceding two steps to create another port forwarding rule for the instance. In this rule, set both the forwarding port and origin server port to 5678.



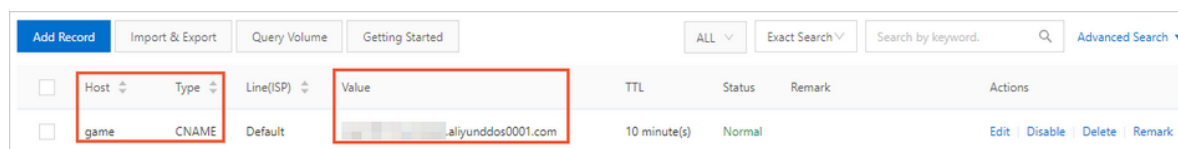
	Forwarding Protocol	Forwarding Port	Origin Server Port	Forwarding Mode	Origin Server IP	Session Persistence	Health Check	Anti-DDoS Protection Policy	Actions
<input type="checkbox"/>	TCP	80	80	--	--	--	--	--	--
<input type="checkbox"/>	TCP	443	443	--	--	--	--	--	--
<input type="checkbox"/>	TCP	1234	1234	Round-robin	1.1.1.1	Disabled Change	Disabled Change	Enabled Change	Edit Delete
<input type="checkbox"/>	TCP	5678	5678	Round-robin	1.1.1.1	Disabled Change	Disabled Change	Enabled Change	Edit Delete

- e) Repeat the preceding three steps to create port forwarding rules for other instances.



	Forwarding Protocol	Forwarding Port	Origin Server Port	Forwarding Mode	Origin Server IP	Session Persistence	Health Check	Anti-DDoS Protection Policy	Actions
<input type="checkbox"/>	TCP	80	80	--	--	--	--	--	--
<input type="checkbox"/>	TCP	443	443	--	--	--	--	--	--
<input type="checkbox"/>	TCP	1234	1234	Round-robin	1.1.1.1	Disabled Change	Disabled Change	Enabled Change	Edit Delete
<input type="checkbox"/>	TCP	5678	5678	Round-robin	1.1.1.1	Disabled Change	Disabled Change	Enabled Change	Edit Delete

3. Go to the DNS provider that has the domain name game.aliyundemo.com to modify the DNS record. Use the CNAME record to map the domain name to the CNAME record obtained in step 1.



	Host	Type	Line(ISP)	Value	TTL	Status	Remark	Actions
<input type="checkbox"/>	game	CNAME	Default	aliyunddos0001.com	10 minute(s)	Normal		Edit Disable Delete Remark

For more information, see [Modify DNS records to protect websites](#).

## 8.3.4 Modify the CNAME record to reroute traffic by using Sec-Traffic Manager

After you use Sec-Traffic Manager to create a scheduling rule for a domain name, you must update the CNAME record of the domain name to reroute website traffic to Sec-Traffic Manager. The rule takes effect only after you update the CNAME record. This topic describes how to use Sec-Traffic Manager to modify the CNAME record of a domain name to reroute traffic. In this example, the DNS resolution service is provided by Alibaba Cloud DNS.

### Prerequisites

A scheduling rule is created and the CDN interaction is set up by using Sec-Traffic Manager. For more information, see [Sec-Traffic Manager](#).

### Context

After you create a scheduling rule or set up CDN interaction for a domain name, Sec-Traffic Manager assigns a CNAME record to the domain name. To reroute the inbound traffic by using Sec-Traffic Manager, you must map the protected domain name to the assigned CNAME record.



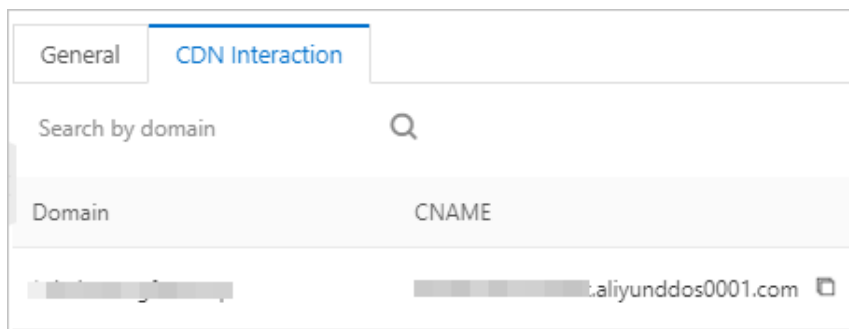
#### Note:

You can query the CNAME record assigned by Sec-Traffic Manager on the **Sec-Traffic Manager** page.

- General rules are used to map the domain names of protected cloud resources to the CNAME record of a specific forwarding rule.

General		CDN Interaction	
Create Rule		Search by rule name	Q
Name	CNAME		
111	[redacted].aliyunddos0001.com		

- CDN interaction rules are used to map domain names that have CDN interaction enabled to specific CNAME records assigned by Sec-Traffic Manager.



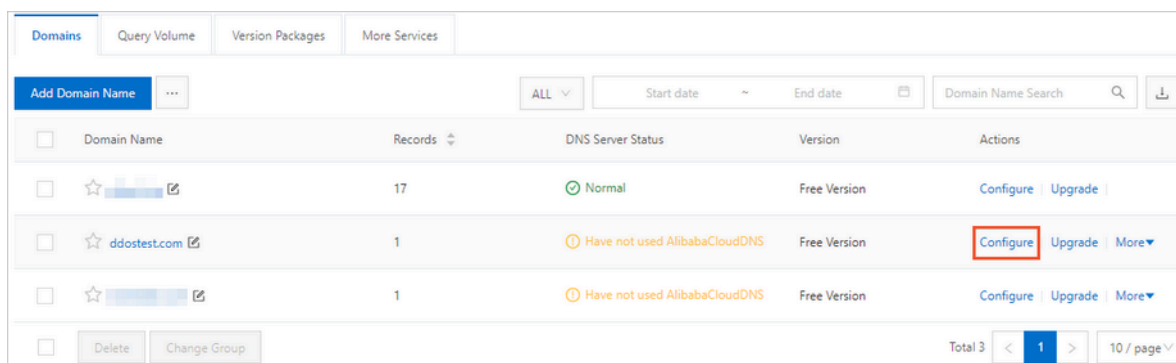
In the following example, the domain name is managed by [Alibaba Cloud DNS](#).

If you use third-party DNS services, log on to the system of the DNS provider to modify the DNS records. The following example is for reference only.

Assume that the domain name in a scheduling rule is `bgp.ddostest.com`. You can perform the following steps to modify or add DNS records in the Alibaba Cloud DNS console.

#### Procedure

1. Log on to the [Alibaba Cloud DNS console](#).
2. On the **Manage DNS** page, find the domain name `ddostest.com` and click **Configure** in the Actions column.

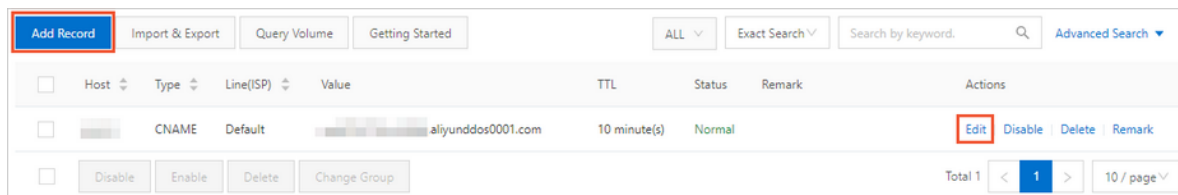


3. On the **DNS Settings** page, find the A record or CNAME record whose Host is **bgp** and click **Edit** in the Actions column.

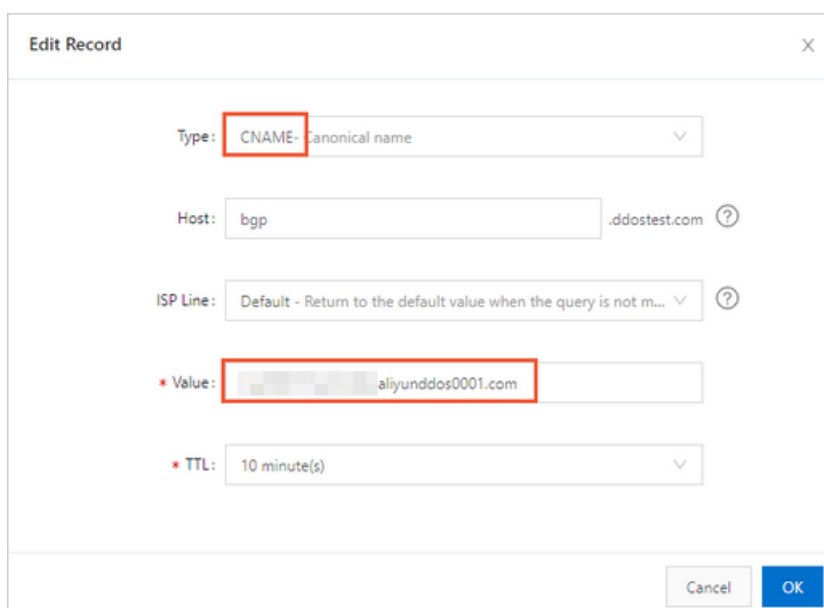


#### Note:

If you cannot find the DNS record that you want to manage in the list, you can click **Add Record** to add the record.



4. In the **Edit Record** or **Add Record** dialog box, set **Type** to **CNAME** and change **Value** to the CNAME record of the scheduling rule or CDN interaction domain name.



5. Click **OK** and wait for the settings to take effect.
6. Check whether the website can be accessed.

## 8.4 Sec-Traffic Manager

Anti-DDoS Pro and Anti-DDoS Premium both provide Sec-Traffic Manager for you to set rules on the interaction between them and the protected cloud resources. You can configure rules for Anti-DDoS Pro or Anti-DDoS Premium to take effect in specific scenarios. This helps you keep your service running with no interruptions as long as no DDoS attacks are launched against your service and provides effective protection when DDoS attacks are launched. Sec-Traffic Manager provides features such as cloud service interaction, tiered protection, CDN interaction, and network acceleration. The network acceleration feature is available only for Anti-DDoS Premium instances. This topic describes the scenarios most suitable for these features and how to configure them.

## Differences between Sec-Traffic Manager provided by Anti-DDoS Pro and that provided by Anti-DDoS Premium



### Notice:


In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

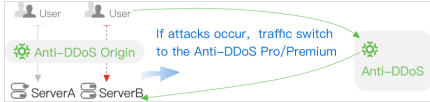



The following table describes the feature differences of Sec-Traffic Manager provided by Anti-DDoS Pro and Anti-DDoS Premium.

Feature	Description	Anti-DDoS Pro	Anti-DDoS Premium
<b>Network acceleration</b>	If you use Anti-DDoS Premium to protect your service, network acceleration provides an IP address that is used to accelerate access to your service for users in mainland China as long as no DDoS attacks are launched against your service. If DDoS attacks are launched against your service, Anti-DDoS Premium takes effect.	Not supported	Supported

## Scenarios

The following table describes the scenarios of these features.


Feature	Scenarios	Description
Cloud service interaction	Anti-DDoS Pro or Anti-DDoS Premium takes effect only when your service is attacked.	<p>If no DDoS attacks are launched against your service, Anti-DDoS Pro or Anti-DDoS Premium is dormant to avoid a high latency. If DDoS attacks are launched, Anti-DDoS Pro or Anti-DDoS Premium automatically takes effect.</p>  <pre> graph LR     User1[User] --&gt; ServerA[ServerA]     User2[User] --&gt; ServerB[ServerB]     ServerA --&gt; AntiDDoS[Anti-DDoS]     ServerB --&gt; AntiDDoS     AntiDDoS --&gt; ServerA     AntiDDoS --&gt; ServerB     </pre> <p>The diagram illustrates the traffic flow during a DDoS attack. Two users send traffic to two servers, ServerA and ServerB. When an attack occurs, the traffic is automatically switched to the Anti-DDoS service, which then routes the traffic back to the servers. A green arrow points from the servers to the Anti-DDoS service, indicating the switch in traffic flow.</p>

Feature	Scenarios	Description
Tiered protection	Anti-DDoS Pro or Anti-DDoS Premium takes effect only when your service suffers volumetric DDoS attacks.	<p>Anti-DDoS Origin is used to protect your service against common attacks and avoid a high latency. If volumetric DDoS attacks are launched, Anti-DDoS Pro or Anti-DDoS Premium automatically takes effect.</p> 
CDN interaction	Content Delivery Network (CDN) is used for network acceleration. If DDoS attacks are launched, user traffic is rerouted from CDN to Anti-DDoS Pro or Anti-DDoS Premium.	<p>If no DDoS attacks are launched against your service, the CDN nodes nearest to users are used to accelerate access. If DDoS attacks are launched, the service traffic is rerouted from CDN to Anti-DDoS Pro or Anti-DDoS Premium.</p> 
Network acceleration <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <b>Note:</b> This feature is available only for Anti-DDoS Premium.           </div>	For an Anti-DDoS Premium instance, network acceleration provides an IP address that is used to accelerate access to your service for users in mainland China as long as no DDoS attacks are launched against your service. If DDoS attacks are launched, Anti-DDoS Premium takes effect.	<p>The IP address that network acceleration provides is used when no DDoS attacks are launched against your service. If DDoS attacks are launched, Anti-DDoS Premium takes effect.</p> 

## Limits

The following table describes the limits of the features provided by Sec-Traffic Manager.

Feature	Limit	Description
Cloud service interaction	Specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance	The specifications of an Anti-DDoS Pro or Anti-DDoS Premium instance, such as the queries per second (QPS) and clean bandwidth, are sufficient to protect your service.

Feature	Limit	Description
	Settings for Anti-DDoS Pro and Anti-DDoS Premium	You must complete the forwarding settings for an Anti-DDoS Pro or Anti-DDoS Premium instance before user traffic is rerouted to the instance.
Tiered protection	Anti-DDoS Origin	You must purchase Anti-DDoS Origin Enterprise.
	Specifications of an Anti-DDoS Origin instance	The clean bandwidth of an Anti-DDoS Origin instance must meet protection requirements.
	Settings for Anti-DDoS Pro and Anti-DDoS Premium	You must complete the forwarding settings for an Anti-DDoS Pro or Anti-DDoS Premium instance before user traffic is rerouted to the instance.
	Settings for Anti-DDoS Origin	The protected cloud resource must be included in the objects protected by Anti-DDoS Origin Enterprise.
Network acceleration	Specifications of an Anti-DDoS Premium instance	The specifications of an Anti-DDoS Premium instance, such as the QPS and clean bandwidth, are sufficient to protect your service.
	Settings for Anti-DDoS Premium	You must complete the forwarding settings for an Anti-DDoS Premium instance before user traffic is rerouted to the instance.
CDN interaction	State of the domain name in CDN	Domain names cannot be in a sandbox.   <b>Note:</b> If a domain name is added to a sandbox by CDN, we recommend that you use Anti-DDoS Pro or Anti-DDoS Premium without CDN interaction enabled.
	Attack frequency	This feature does not apply to websites that are attacked more than three times per week.



**Note:**

This feature is available only for Anti-DDoS Premium.

**Note:**

If a domain name is added to a sandbox by CDN, we recommend that you use Anti-DDoS Pro or Anti-DDoS Premium without CDN interaction enabled.



Feature	Limit	Description
	Response time of anti-DDoS protection	<p>This feature does not apply to scenarios where anti-DDoS protection is required to take effect in a short time.</p> <div>  <b>Note:</b>            After your service traffic is switched to an Anti-DDoS Pro or Anti-DDoS Premium instance, the time required for anti-DDoS protection to take effect depends on the time to live (TTL) of the DNS records on the protected websites.         </div>
	Service bandwidth	<p>This feature does not apply to services with a high bandwidth or large QPS.</p> <div>  <b>Note:</b>            If the service bandwidth exceeds 3 Gbit/s or the QPS exceeds 10,000, submit a ticket to request an analysis on whether the feature is suitable for this website.         </div>
	Service type	<p>This feature applies to HTTP and HTTPS requests only. Video live streaming is not supported.</p>
	Function plan of the Anti-DDoS Pro or Anti-DDoS Premium instance	<p>The Anti-DDoS Pro or Anti-DDoS Premium instance must use the enhanced function plan.</p>

### Switch between CDN and Anti-DDoS Pro or CDN and Anti-DDoS Premium

To enable CDN, you must set the QPS threshold to trigger the traffic switchover between CDN and Anti-DDoS Pro or Anti-DDoS Premium. The traffic switchover is subject to the following limits:

- From CDN to Anti-DDoS Pro or Anti-DDoS Premium
  - If the QPS exceeds the threshold three times within three minutes or more than six times within 10 minutes, a switchover is triggered.
  - The bandwidth of the service on CDN must be lower than or equal to 10 Gbit/s.






**Note:**



The maximum bandwidth that an Anti-DDoS Pro or Anti-DDoS Premium instance can protect is lower than 10 Gbit/s.

- From Anti-DDoS Pro or Anti-DDoS Premium to CDN
  - If the QPS remains less than 80% of the threshold and the protection success rate for HTTP flood attacks remains less than 10% for more than 12 consecutive hours, the traffic is switched from Anti-DDoS Pro or Anti-DDoS Premium to CDN.
  - The IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance cannot be in a black hole, and no traffic is scrubbed or routed to a black hole in the last 60 minutes.
  - Switchovers can be triggered only from 08:00 to 23:00.

## Configure Sec-Traffic Manager

Feature	Description
Cloud service interaction	<p>Cloud service interaction switches service traffic between an Anti-DDoS Pro or Anti-DDoS Premium instance and one or more protected cloud resources. The configuration procedure is as follows:</p> <ol style="list-style-type: none"> <li>1. Configure traffic forwarding for Anti-DDoS Pro or Anti-DDoS Premium. For more information, see <a href="#">Add a website</a>.</li> <li>2. Verify that the Anti-DDoS Pro or Anti-DDoS Premium instance can forward traffic to the origin server. For more information, see <a href="#">Verify the forwarding configuration on your local machine</a>.</li> <li>3. Configure Sec-Traffic Manager. <ul style="list-style-type: none"> <li>• To switch service traffic between an Anti-DDoS Pro or Anti-DDoS Premium instance and a protected resource, see <a href="#">Create general scheduling rules</a>.</li> <li>• To switch service traffic between an Anti-DDoS Pro or Anti-DDoS Premium instance and multiple protected resources, use one of the following modes: <ul style="list-style-type: none"> <li>- Service traffic is rerouted to Anti-DDoS Pro or Anti-DDoS Premium only if all protected cloud resources are overwhelmed by inbound traffic. To use this interaction mode, create a scheduling rule in the same way as you switch service traffic between an Anti-DDoS Pro or Anti-DDoS Premium instance and a protected cloud resource but specify multiple protected resources for interaction.</li> <li>- Protected cloud resources share the inbound traffic of a service. If a protected resource is attacked, the traffic on the protected cloud resource is switched to an Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see <a href="#">Configure protected resources to share the inbound traffic of a service</a>.</li> </ul> </li> </ul> </li> <li>4. Modify the DNS record to reroute traffic to Sec-Traffic Manager. Modify the CNAME record to resolve domain names to the CNAME record assigned by Sec-Traffic Manager.</li> </ol> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;">  <b>Note:</b>  For information about how to modify the CNAME record of DNS, see <a href="#">Modify the CNAME record to reroute traffic by using Sec-Traffic Manager</a>. </div>

Feature	Description
Tiered protection	Tiered protection switches service traffic between an Anti-DDoS Pro or Anti-DDoS Premium instance and one or more cloud resources protected by Anti-DDoS Origin. The procedure for configuring tiered protection is the same as you configure cloud service interaction.
Network acceleration  <div>  <b>Note:</b>            This feature is available for Anti-DDoS Premium.         </div>	<p>The configuration procedure is as follows:</p> <ol style="list-style-type: none"> <li>1. Configure traffic forwarding for Anti-DDoS Pro or Anti-DDoS Premium. For more information, see <a href="#">Add a website</a>.</li> <li>2. Verify that the Anti-DDoS Pro or Anti-DDoS Premium instance can forward traffic to the origin server. For more information, see <a href="#">Verify the forwarding configuration on your local machine</a>.</li> <li>3. Configure Sec-Traffic Manager. For more information, see <a href="#">Create general scheduling rules</a>.</li> <li>4. Modify the DNS record to reroute traffic to Sec-Traffic Manager. Modify the CNAME record to resolve domain names to the CNAME record assigned by Sec-Traffic Manager.</li> </ol> <div>  <b>Note:</b>            For information about how to modify the CNAME record of DNS, see <a href="#">Modify the CNAME record to reroute traffic by using Sec-Traffic Manager</a>.         </div>

Feature	Description
CDN interaction	<p>The configuration procedure is as follows:</p> <ol style="list-style-type: none"><li>1. Configure CDN and add the protected domain to CDN. Make sure that the settings take effect. For more information, see <a href="#">#unique_82</a>.</li></ol> <div> <b>Note:</b> If a security group is configured for the origin server, you must add the back-to-origin IP addresses of CDN to the whitelist of the origin server.</div> <ol style="list-style-type: none"><li>2. Configure traffic forwarding for Anti-DDoS Pro or Anti-DDoS Premium. For more information, see <a href="#">Add a website</a>.</li><li>3. Verify that the Anti-DDoS Pro or Anti-DDoS Premium instance can forward traffic to the origin server. For more information, see <a href="#">Verify the forwarding configuration on your local machine</a>.</li><li>4. Configure Sec-Traffic Manager. For more information, see <a href="#">Create a CDN interaction rule</a>.</li><li>5. Modify the DNS record to reroute traffic to Sec-Traffic Manager. Modify the CNAME record to resolve domain names to the CNAME record assigned by Sec-Traffic Manager.</li></ol> <div> <b>Note:</b> For information about how to modify the CNAME record of DNS, see <a href="#">Modify the CNAME record to reroute traffic by using Sec-Traffic Manager</a>.</div>

### Create general scheduling rules

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Sec-Traffic Manager**.

4. On the **General** tab, click **Create Rule**.

## Sec-Traffic Manager

General

CDN Interaction

Create Rule

Search by rule name

Q

Name	CNAME	Interaction Scenario
------	-------	----------------------

5. In the **Create Rule** pane, set the parameters and click **Next**.

**Figure 8-1: An example on how to configure a cloud service interaction rule in the Anti-DDoS Pro console**

Create Rule

\* Interaction Scenario:

Cloud Service Interaction

Tiered Protection

\* Name:

doctest

The name must be 1 to 128 characters in length and contain letters, numbers, or underscores (\_).

\* Anti-DDoS Instance IP:

203. .210 □ tpro

▼

\* Cloud Resource:

East China 1

▼

47. .33

+ Add Cloud Resource IP

\* The waiting time of switching back

60

Minute(s)

After switch to Anti-DDoS Pro or Premium , the waiting time for triggering the switching back process is at least 30 minutes and at most 120 minutes.

Next

Cancel

**Figure 8-2: An example on how to configure network acceleration in the Anti-DDoS Premium console**

Create Rule

\* Interaction Scenario:

Network Acceleration

Cloud Service Interaction

Tiered Protection

\* Name:

doctest

The name must be 1 to 128 characters in length and contain letters, numbers, or underscores (\_).

\* Anti-DDoS Instance IP:

170. .224 □ 1

▼

\* Mainland China Acceleration IP:

170. .39 □ ddosDip-cn- .

▼

\* The waiting time of switching back




60

Minute(s)

After switch to Anti-DDoS Pro or Premium , the waiting time for triggering the switching back process is at least 30 minutes and at most 120 minutes.

Next

Cancel

Parameter	Description
<b>Interaction Scenario</b>	<p>The scenario where the rule is applied. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>Network Acceleration</b></li> </ul> <div>  <b>Note:</b> This option is available only for Anti-DDoS Premium.         </div> <ul style="list-style-type: none"> <li>• <b>Tiered Protection</b></li> </ul> <div>  <b>Note:</b> Only cloud resources protected by Anti-DDoS Origin are supported, such as ECS, EIP, SLB, and WAF instances.         </div> <ul style="list-style-type: none"> <li>• <b>Cloud Service Interaction</b></li> </ul>
<b>Name</b>	The name of the rule that you want to create. The rule name can be up to 128 characters in length and can contain letters, digits, and underscores (_).
<b>Anti-DDoS Instance IP</b>	The IP address of the target Anti-DDoS Pro or Anti-DDoS Premium instance.
<b>Mainland China Acceleration IP</b>	<p>The IP address that you use to accelerate user access in the <b>Network Acceleration</b> interaction scenario.</p> <div>  <b>Note:</b> This parameter is available only for Anti-DDoS Premium.         </div>
<b>Cloud Resource</b>	The cloud resources for which you want to create an interaction in the <b>Cloud Service Interaction</b> and <b>Tiered Protection</b> interaction scenarios. You must select the region where the target cloud resources are deployed and enter the IP addresses of cloud resources. You can click <b>Add Cloud Resource IP</b> to add more cloud resources as required. You can add a maximum of 20 resources.



Parameter	Description
<b>The waiting time of switching back</b>	<p>The waiting time to switch service traffic back to cloud resources after service traffic is switched to Anti-DDoS Pro or Anti-DDoS Premium.</p> <p>To meet the requirements of deactivating the blackhole status and avoid frequent switchover, the minimum value of this parameter is 30 minutes. We recommend that you set this parameter to 60 minutes.</p>

After a scheduling rule is created, Sec-Traffic Manager assigns a CNAME record to the scheduling rule. To apply the scheduling rule, you must go to the DNS provider of the cloud resource to modify the DNS record. Modify the CNAME record and configure it to resolve the domain name to the CNAME record assigned by Sec-Traffic Manager. Scheduling rules and their CNAME records are displayed in the list.

General		CDN Interaction			
Create Rule		Search by rule name			
Name	CNAME	Interaction Scenario	Anti-DDoS Instance	Cloud Service	Actions
	aliyunddos0001.com	Cloud Service Interaction	203.107.53.98		Edit Delete

### Manully switch traffic from Anti-DDoS Pro or Anti-DDoS Premium to cloud resources

After a scheduling rule takes effect, if the traffic on cloud resources is switched to Anti-DDoS Pro or Anti-DDoS Premium, you can switch the traffic back to the cloud resources as required.

The following exceptions may occur when you perform this operation:

- If all the cloud resources are in the black hole state, this operation will fail.
- If some of the cloud resources are in the black hole state, traffic is switched to the cloud resources that are not in the black hole state. After the black hole state of a cloud resource is deactivated, traffic can be switched to the cloud resource.

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning** > **Sec-Traffic Manager**.

4. On the **General** tab, find the target scheduling rule, click **Switch back** in the Actions column, and click OK in the message that appears.

**Note:**

The **Switch back** action is available only if the duration that traffic has been switched to Anti-DDoS or Anti-DDoS Premium is greater than the value of **The waiting time of switching back**.

General		CDN Interaction			
Create Rule		Search by rule name			
Name	CNAME	Interaction Scenario	Anti-DDoS Instance	Cloud Service	Actions
aliyunddos0001.com	aliyunddos0001.com	Tiered Protection	<div><div></div></div>	47.92.70.77	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Switch back</a>

## Create a CDN interaction rule

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning** > **Sec-Traffic Manager**.
4. Click the **CDN Interaction** tab.

The **CDN Interaction** tab displays all the websites added to Anti-DDoS Pro or Anti-DDoS Premium.

5. Find the website for which you want to create a CDN interaction rule and click **Add Interaction**.

General		CDN Interaction			
Search by domain					
Domain	CNAME	Anti-DDoS Instance	CDN Interaction	Trigger Condition	Actions
aliyunddos0001.com	--	<div><div></div></div>	Disabled	--	<a href="#">Add Interaction</a>

6. On the **Add Interaction** page, verify **Domain** and set **Trigger Condition** to the lowest request rate that triggers a switchover. Click **Next**.

To create a CDN interaction rule, Domain must meet the following requirements:

- The **Anti-DDoS Instance** for which you want to create a CDN interaction rule must use the enhanced function plan.
- The **Cloud Service** for which you want to create a CDN interaction rule must be configured in Alibaba Cloud CDN.



#### Note:

We recommend that you set Request per Second to at least two times greater than the historical traffic peak in case of a traffic spike, and set Request per Second to more than 500 for websites that have a low QPS.

After a scheduling rule is created, Sec-Traffic Manager assigns a CNAME record to this rule. To apply the scheduling rule, you must go to the DNS provider of the cloud resource to modify the DNS record. Modify the CNAME record and configure it to resolve the domain name to the CNAME record assigned by Sec-Traffic Manager. Then, the state of **CDN Interaction** that corresponds to the target website becomes **Enabled**. The CNAME record is also displayed on the tab.

General		CDN Interaction			
Search by domain					
Domain	CNAME	Anti-DDoS Instance	CDN Interaction	Trigger Condition	Actions
aliyunddos0001.com	aliyunddos0001.com	Enabled	Enabled	Minimum Request QPS:50	Edit   Delete

## Configure protected resources to share the inbound traffic of a service

The following example shows how to configure the traffic switchover between an Anti-DDoS Pro or Anti-DDoS Premium instance and multiple cloud resources protected by Anti-DDoS Origin. In this scenario, protected resources share the inbound traffic of a service. If any protected resource is attacked, the traffic on the resource is rerouted to an Anti-DDoS Pro or Anti-DDoS Premium instance.

1. Configure Anti-DDoS Origin. Add multiple resources to Anti-DDoS Origin for protection. For example, three IP addresses are added. For more information, see [#unique\\_83](#).
2. Configure Sec-Traffic Manager. Create a tiered protection rule for each of the added IP addresses and associate the three rules with the same Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see [Create general scheduling rules](#).
3. Modify DNS records. Add three CNAME records that use the same host record. Set the record values to the CNAME records of the three tiered protection rules created in step 2. For more information, see [Modify the CNAME record to reroute traffic by using Sec-Traffic Manager](#).
4. Verify the DNS records. At the DNS verification website, check whether the added CNAME records take effect.

## 8.5 CNAME reuse

If you want to add multiple domain names that are hosted by the same server to an Anti-DDoS Premium instance, we recommend that you apply for CNAME reuse. This feature allows you to configure the instance only once and map multiple domain names hosted by the same server to a CNAME record. After CNAME reuse is enabled, you can modify the CNAME record to map the domain names hosted by the same server to the CNAME record assigned by Anti-DDoS Premium.

### Prerequisites

The CNAME reuse feature is enabled. To enable this feature, you must submit a ticket.

**Note:**

Only Anti-DDoS Premium supports CNAME reuse.

### Scenarios

CNAME reuse is suitable for the following scenarios:

- Customers, such as agents, independent software vendors (ISVs), and distributors that want to add a large number of domain names to an Anti-DDoS Premium instance. Most of the domain names are hosted by the same server and the number of domain names changes frequently.
- Multiple top-level domain names are used for the promotion and search engine optimization (SEO) of the same service, and the domain names need to be added to an Anti-DDoS Premium instance.
- Multiple backup domain names are required for a service, and the domain names need to be added to an Anti-DDoS Premium instance.

## Limits

The following table describes the limits of CNAME reuse.

Limit	Description
Protocol	Only HTTP is supported.
Origin server	The domain names that are mapped to the same CNAME record must be hosted by the same origin server.

## Enable CNAME reuse

You can use the CNAME reuse feature together with Sec-Traffic Manager. If you enable CNAME reuse, you can choose whether to use Sec-Traffic Manager. For more information about Sec-Traffic Manager, see [Sec-Traffic Manager](#).

- To use the CNAME reuse feature together with Sec-Traffic Manager, you must select a scheduling rule. Then, the CNAME record configured in the scheduling rule is reused.
- If you do not use Sec-Traffic Manager, the CNAME record assigned by Anti-DDoS Premium is reused.

The following configuration descriptions are based on the following assumptions:

- The origin server has two IP addresses: 1.1.1.1 and 2.2.2.2.
- IP address 1.1.1.1 hosts three domain names: a.test, b.test, and c.test.

The following procedure describes how to use the CNAME reuse feature to add multiple domain names, such as a.test, b.test, and c.test, that are hosted on the IP address 1.1.1.1 to an Anti-DDoS Premium instance.

**1. Enable CNAME reuse when you configure a website.**

- a) Log on to the [Anti-DDoS Premium console](#).
- b) In the top navigation bar, select **Outside Mainland China**.
- c) In the left-side navigation pane, choose **Provisioning > Website Config**.
- d) Add a domain name and enable **CNAME Reuse**, or enable this feature for an existing domain name. For more information about how to add a domain name, see [Add a website](#).

Assume that the IP address of the origin server is 1.1.1.1 and the domain name is a.test.

The screenshot displays the 'Add Website' configuration page in the Anti-DDoS Premium console. The page is divided into two main sections: '1 Enter Site Information' and '2 Complete'. The 'Enter Site Information' section contains the following fields and options:

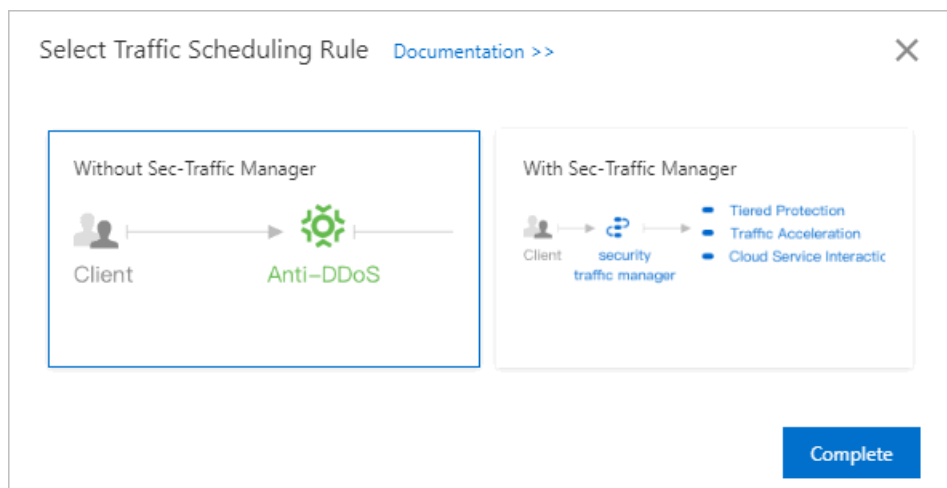
- Function Plan:** Two tabs, 'Standard Function' and 'Enhanced Function'.
- Instance:** A list of instance checkboxes. An example IP address '9.9.9.9' is shown in red text. A note states: '(You can associate a domain with a maximum of eight Anti-DDoS Pro instances. You have selected 0 instances.)'
- Website domain:** A text input field containing 'a.test'. Below it, a note says: 'Support Top Level Domain: e.g. "test.com" and Second Level Domain: e.g. www.test.com'.
- Protocol:** Checkboxes for 'HTTP' (checked), 'HTTPS' (checked), 'Websocket', and 'Websockets'.
- Origin server:** Radio buttons for 'IP' (selected) and 'Domain'. Below the 'IP' button, the text '1.1.1.1' is entered in the input field.
- Origin server ports:** Text labels for 'HTTP 80' and 'HTTPS 443', with a 'Custom' link to the right.
- CnameReuse:** A toggle switch that is currently turned on (green). A link to 'Documentation' is next to it.

At the bottom of the form is a button labeled 'Add website'.

2. Specify whether to use Sec-Traffic Manager. Update the CNAME record of the protected domain name.

If you enable CNAME reuse, you must specify whether to use Sec-Traffic Manager.

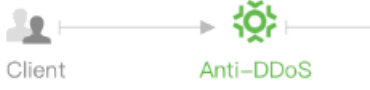
- Enable CNAME reuse without Sec-Traffic Manager.
  - a. In the **Select Traffic Scheduling Rule** dialog box, select **Without Sec-Traffic Manager** and click **OK**.



- b. After a domain name is added, record the CNAME record assigned for the domain name.
  - c. Go to the DNS provider that has the protected domain name and modify the DNS records for all the domain names (a.test, b.test, and c.test) that are hosted on the IP address 1.1.1.1. Use the obtained CNAME record to enable CNAME reuse.
- Enable CNAME reuse with Sec-Traffic Manager.
    - a. In the **Select Traffic Scheduling Rule** dialog box, select **With Sec-Traffic Manager**, specify a Sec-Traffic Manager rule, and click **OK**.


Select Traffic Scheduling Rule [Documentation >>](#)

Without Sec-Traffic Manager



Client → Anti-DDoS

With Sec-Traffic Manager



Client → security traffic manager → Tiered Protection, Traffic Acceleration, Cloud Service Interac

\* Select Rule

doctest

[Create Sec-Traffic Manager Rule](#)

Complete

If you enable CNAME reuse with Sec-Traffic Manager, the Sec-Traffic Manager rule must be associated with the IP address 1.1.1.1 and the IP address of the Anti-DDoS Premium instance used in the website configuration. If no rule is available, click **Create Sec-Traffic Manager Rule** to create a rule.

**Note:**



The IP address of the Anti-DDoS Premium instance in the Sec-Traffic Manager rule must be the same as that used in the domain name configuration.

Create Rule

\* Interaction: Network Acceleration | **Cloud Service Interaction** | Tiered Protection

Scenario:

\* Name: CnameReuse\_example  
**Example: 9.9.9.9**

\* Anti-DDoS Pro: Select  
Instance:

\* Cloud Resource: US East 1 (Vi...  
+ Add Cloud Resource IP  
Enter the cloud service's IP addi  
**Example: 1.1.1.1**

Next Cancel

- b. After you specify a Sec-Traffic Manager rule, record the CNAME record of the rule.

CnameReuse: ☒ Domains that utilize the CNAME Reuse of Sec-Traffic Manager k244f80yeqg...

- c. Go to the DNS provider that has the protected domain name and modify the DNS records of all the domain names (a.test, b.test, and c.test) that are hosted on the IP address 1.1.1.1. Use the obtained CNAME record to enable CNAME reuse.
3. Optional: To add domain names that are hosted by another origin server, perform step 1 and step 2 for this server.

### Disable CNAME reuse

You can disable CNAME reuse on the Website Config page.



#### Notice:

Before you disable this feature, make sure that the service traffic of all the domain names mapped the CNAME record is no longer rerouted to Anti-DDoS Premium. Otherwise, the inbound traffic cannot be forwarded to the origin server.

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select **Outside Mainland China**.

3. In the left-side navigation pane, choose **Provisioning > Website Config**.
4. In the target website configuration, disable **CNAME Reuse**.
5. Specify whether to retain the website configuration and the Sec-Traffic Manager rule.
  - If you retain a website configuration, the traffic forwarding rules still take effect.
  - If you retain the Sec-Traffic Manager rule, Sec-Traffic Manager still takes effect.

## 8.6 Allow back-to-origin IP addresses to access the origin server

To use Anti-DDoS Pro or Anti-DDoS Premium to protect your website, we recommend that you add the back-to-origin IP addresses to the whitelist of the origin server. This ensures that the traffic from Anti-DDoS Pro or Anti-DDoS Premium is not blocked by security software on your origin server.

### Context

If you deploy third-party security software on your origin server, such as a firewall, add the back-to-origin IP addresses of Anti-DDoS Pro or Anti-DDoS Premium to the whitelist of the security software.



#### Notice:

After you switch service traffic to Anti-DDoS Pro or Anti-DDoS Premium, the instance scrubs the traffic and uses back-to-origin IP addresses to forward the traffic to the origin server. If the back-to-origin IP addresses are not in the whitelist on your firewall, the traffic from Anti-DDoS Pro or Anti-DDoS Premium may be blocked. This results in a failure to access your website.

If you use Anti-DDoS Pro or Anti-DDoS Premium to protect your website, the inbound traffic is rerouted to Anti-DDoS Pro or Anti-DDoS Premium for scrubbing. Then, Anti-DDoS Pro or Anti-DDoS Premium forwards the normal traffic to the origin server. In the back-to-origin process, network traffic is forwarded to the origin server by an Anti-DDoS Pro or Anti-DDoS Premium instance.

Anti-DDoS Pro and Anti-DDoS Premium function as reverse proxies and support the Full NAT mode.

Before Anti-DDoS Pro or Anti-DDoS Premium is used, the origin server receives requests from the distributed IP addresses of clients. If no attacks are launched against your services, each source IP address sends a small number of requests.

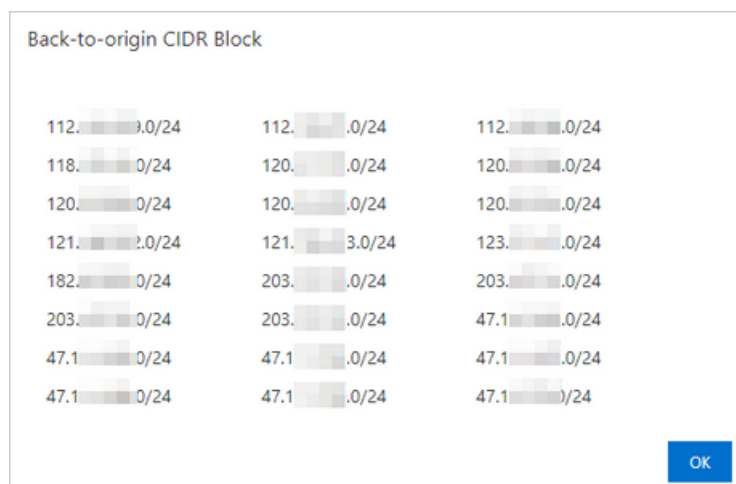
After Anti-DDoS Pro or Anti-DDoS Premium is used, the origin server receives all requests from a limited number of back-to-origin IP addresses. Each IP address forwards a larger number of requests than the client. As a result, the back-to-origin IP addresses may be regarded as malicious. If other DDoS protection policies are configured on the origin server, these back-to-origin IP addresses may be blocked or subject to bandwidth limits.

For example, the most common 502 error indicates that the origin server does not respond to the requests forwarded from back-to-origin IP addresses, and the back-to-origin IP addresses may be blocked by the firewall on the origin server.

Therefore, we recommend that you disable the firewall and other security software on the origin server after you set up forwarding rules. This ensures that the back-to-origin IP addresses of Anti-DDoS Pro or Anti-DDoS Premium are not affected by the protection policies on the origin server. Alternatively, you can perform the following steps to find the back-to-origin IP addresses of Anti-DDoS Pro and Anti-DDoS Premium and add them to the whitelist of the security software on the origin server.

#### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Website Config**.
4. On the **Website Config** page, click **View Back-To-Source CIDR Blocks** in the upper-right corner.
5. In the **Back-To-Source CIDR Block** dialog box, copy the back-to-origin IP addresses used by Anti-DDoS Pro or Anti-DDoS Premium.



6. Add the back-to-origin IP addresses to the whitelist of the security software on your origin server.

## 8.7 Verify the forwarding configuration on your local machine

After you add a domain name or a port to an instance, Anti-DDoS Pro or Anti-DDoS Premium forwards the packets received by the port to the port of the origin server.

To ensure service stability, we recommend that you verify whether the forwarding configuration takes effect on your local machine before the inbound traffic is rerouted to Anti-DDoS Pro or Anti-DDoS Premium. This topic describes how to verify the configuration.

### Prerequisites

- A website or port is added to Anti-DDoS Pro or Premium. For more information, see [Add a website](#) and [Create forwarding rules](#).
- The back-to-origin IP address of Anti-DDoS Pro or Anti-DDoS Premium is added to the whitelist of the origin server. For more information, see [Allow back-to-origin IP addresses to access the origin server](#).

### Context

To protect a service that is associated by using a domain name instead of an IP address, you must add a website to Anti-DDoS Pro or Anti-DDoS Premium. After you add a website configuration, you can modify the hosts file or use the CNAME record of Anti-DDoS Pro or Anti-DDoS Premium to connect to the server and check whether the forwarding configuration takes effect.

Requests to access Layer 4 services, such as games, are processed by using IP addresses instead of domain names. You must add port forwarding rules to Anti-DDoS Pro or Anti-DDoS Premium to protect these services. Then, you can verify the forwarding configuration by using the IP address of Anti-DDoS Pro or Anti-DDoS Premium to access the server.



#### Notice:

If you switch your service traffic to Anti-DDoS Pro or Anti-DDoS Premium before the forwarding configuration takes effect, your services may be interrupted.

## Modify the local hosts file

1. Modify the hosts file to reroute the inbound traffic of the protected website to Anti-DDoS Pro or Anti-DDoS Premium. The following procedure shows how to modify the hosts file on a Windows server.

- a) Find the hosts file, which is typically stored in C:\Windows\System32\drivers\etc\.
- b) Open the hosts file by using a text editor, such as Notepad or Notepad++.
- c) Add the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance and the protected domain name at the end of the file.

Assume that the IP address of the instance is `180.xx.xx.173` and the domain name is `www.aliyundemo.com`. You must add `180.xx.xx.173 www.aliyundemo.com` at the end of the file.

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1            localhost

180.███.███.173 www.aliyundemo.com
```

- d) Save the file.
2. Ping the IP address of the protected domain name from your local machine.  
The IP address of the domain name is expected to be resolved into the IP address of the instance in the hosts file. If the domain name is still resolved into the IP address of the origin server, refresh the local DNS cache by running `ipconfig/flushdns` in the CLI.
  3. After you verify that the IP address of the protected domain name is resolved to the IP address of the instance, try to access the service by using the domain name. If you can access the service, the configuration has taken effect.

## Use the CNAME record assigned by Anti-DDoS Pro or Anti-DDoS Premium to access the origin server

If the client allows users to enter the domain name of the origin server, replace the domain name with the CNAME record assigned by Anti-DDoS Pro or Anti-DDoS Premium and check whether the origin server can be accessed.



### Note:

After you add a domain name for protection, Anti-DDoS Pro or Anti-DDoS Premium assigns a CNAME record to the domain name. You can view the CNAME record on the Website Config page.

If the client cannot connect to the service, check whether the prerequisites are met. If the fault persists, contact Alibaba Cloud technical support.

### Use the IP address of the instance to access the origin server

Assume that the IP address of the instance is 99.99.99.99, the forwarding port is 1234, the IP address of the origin server is 11.11.11.11, and the port of the origin server is 1234.

If you can use telnet commands to access the IP address of the instance by using port 1234, the forwarding rule has taken effect.

If the client allows users to enter the IP address of the origin server, you can enter the IP address of the instance for verification.

## 8.8 Change the public IP address of an ECS origin server

If the IP address of your origin server is exposed, we recommend that you change the public IP address of your ECS instance to prevent attackers from bypassing Anti-DDoS Pro or Anti-DDoS Premium to attack the origin server. You can change the public IP address of an ECS instance in the Anti-DDoS Pro or Anti-DDoS Premium console up to 10 times.

### Context

You can only change the public IP addresses of ECS instances that are connected to classic networks.

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning** > **Website Config**.
4. In the upper-right corner of the **Website Config** page, click **Change ECS IP**.



#### Notice:

If you change the public IP address of an ECS instance, your service is interrupted for a few minutes. We recommend that you back up your data before you perform this operation.

5. You must stop the ECS instance before you change its IP address. If you have already stopped the ECS instance, go to step 6. In the **Change ECS IP** dialog box, click **Go to ECS**. In the ECS console, perform the following steps to stop the target instance:

- a) Find the ECS instance whose public IP address you want to change in the instance list and click the instance ID.
- b) On the instance details page, click **Stop**.
- c) Select a method and click **OK**.

**Notice:**

Identity authentication is required to stop an ECS instance. Enter the verification code that is sent to your mobile phone.

- d) Wait until the state of the instance becomes **Stopped**.

6. Return to the **Change ECS IP** dialog box, specify **ECS Instance ID**, and click **Next**.

7. Make sure that the ECS instance information is valid, and then click **release**.

8. After the IP address is released, click **Next**. Anti-DDoS Pro or Anti-DDoS Premium automatically assigns a new IP address to the ECS instance.

9. Click **OK**.

**Note:**

After you change the IP address of an ECS origin server, set up Anti-DDoS Pro or Anti-DDoS Premium and do not expose the new IP address.

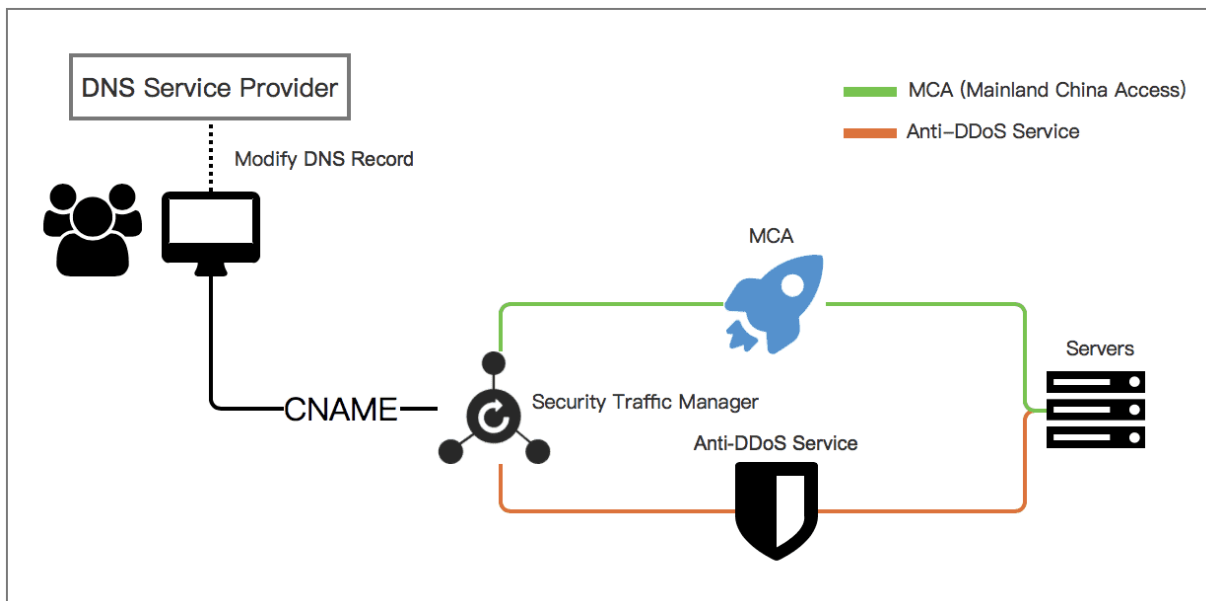
## 8.9 Configure Anti-DDoS Premium MCA

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 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](#).



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

Security Traffic Manager



Add Rule

Name	CNAME①	Nodes	Operations
jiasu1		Low Priority  High Priority 	<a href="#">Edit</a> <a href="#">Delete</a>

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

**Add Rule** [X]

Name :

Nodes :

High Priority :  Select the Dedicated IP of MCA instance

Low Priority :  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.

- 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.

## 9 Protection settings

---

### 9.1 Protection for infrastructure

#### 9.1.1 Configure a blacklist or whitelist for destination IP addresses

This topic describes how to configure the Black Lists and White Lists (Destination IP) policy to deny or allow access requests to an Anti-DDoS Pro instance from certain source IP addresses. You can add IP addresses to or remove IP addresses from a blacklist or whitelist as required. IP addresses that are marked as malicious addresses by the intelligent protection algorithms are added to a blacklist. You can export blacklists and whitelists to local devices.

##### Prerequisites

An Anti-DDoS Pro instance is available.



##### Note:

Only Anti-DDoS Pro supports the Black Lists and White Lists (Destination IP) policy.

##### Context



##### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

The Black Lists and White Lists (Destination IP) policy takes effect only on certain instances.

- Requests from IP addresses in a blacklist are dropped by an Anti-DDoS Pro instance. Each IP address in a blacklist is blocked for a specified period of time. An IP address is automatically removed from a blacklist after its blocking period expires.
  - Intelligent protection algorithms automatically calculate the blocking periods of malicious IP addresses. The minimum blocking period is five minutes, and the

maximum is one hour. If a malicious IP address is continuously used to attack your website, the system automatically extends its blocking period.

- If you add an IP address to a blacklist, you must specify the blocking period.
- Requests from IP addresses in a whitelist are allowed by an Anti-DDoS Pro instance. The IP addresses in a whitelist can only be manually removed.

If IP addresses in a whitelist and blacklist overlap, the whitelist prevails. A whitelisted IP address cannot be added to a blacklist.

#### Procedure

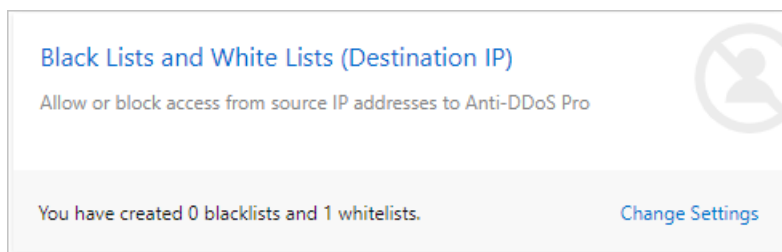
1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select **Mainland China**.
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **Protection for Infrastructure** tab, select the target instance from the list on the left side.



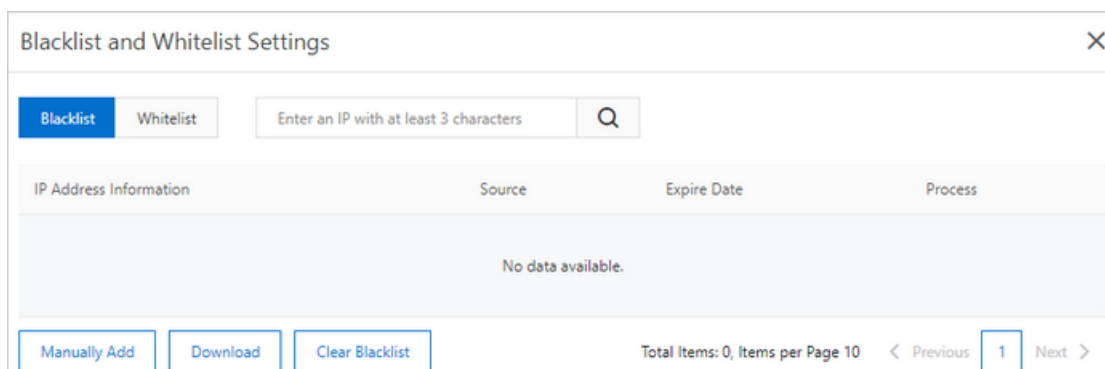
#### Note:

You can search for instances by instance ID or description.

5. In the **Black Lists and White Lists (Destination IP)** section, click **Change Settings**.



6. In the **Blacklist and Whitelist Settings** pane, click **Blacklist** or **Whitelist** to manage a blacklist or whitelist.



- For more information about blacklist management, see [step 7](#).
- For more information about whitelist management, see [step 8](#).

7. Optional: Manage a blacklist.

- Add an IP address to the blacklist.

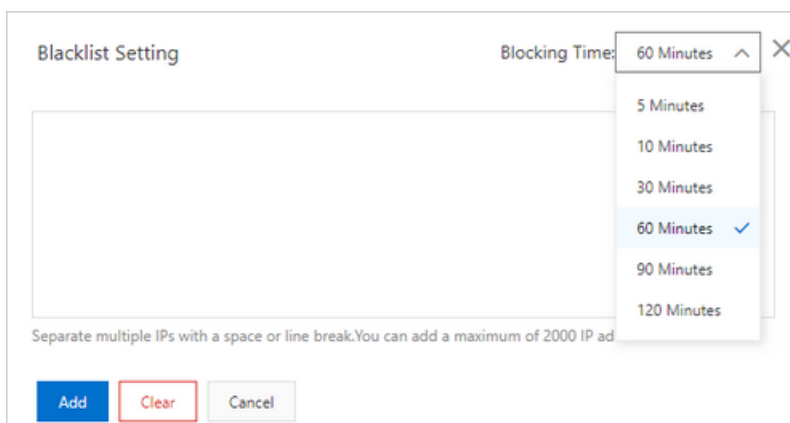
a. Click **Manually Add**.

b. In the **Blacklist Setting** dialog box, enter the IP address and set **Blocking Time**.



**Note:**

You can add up to 2,000 IP addresses to the blacklist.



The dialog box titled "Blacklist Setting" has a "Blocking Time:" dropdown menu set to "60 Minutes". The dropdown menu is open, showing options: 5 Minutes, 10 Minutes, 30 Minutes, 60 Minutes (selected with a checkmark), 90 Minutes, and 120 Minutes. Below the dropdown is a large text input field. At the bottom, there are three buttons: "Add" (blue), "Clear" (red), and "Cancel" (gray). A small note at the bottom of the input field says: "Separate multiple IPs with a space or line break. You can add a maximum of 2000 IP ad".

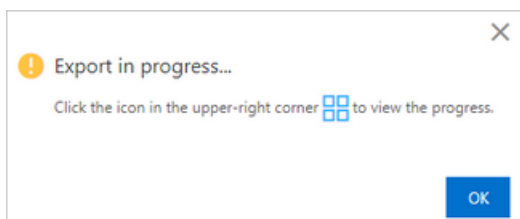
c. Click **Add**.

After the IP address is added to the blacklist, requests from the newly added IP address are dropped during **Blocking Time** of the IP address. After Blocking Time of the IP address expires, the block on this IP address is removed.

- Search for IP addresses in the blacklist: Enter a keyword in the search box to search for IP addresses that contain the keyword.
- Clear the blacklist: Click **Clear Blacklist** to remove all IP addresses from the blacklist. You can also click **Delete** next to an IP address to remove it from the blacklist.
- Download the blacklist.

a. Click **Download** to start a download task.

b. In the message that appears, click **OK**.



c. Close the **Blacklist and Whitelist Settings** pane.

d. Click [grid icon] in the upper-right corner to view the task list.

e. Find the download task. After **Status** of the task becomes **Exported**, click **Download** in the Actions column.

Tasks			
Name	Status	Start Time	Actions
Blacklist Export_ddoscoo-cn-mp...	● Exported	[blurred]	<a href="#">Delete</a> <a href="#">Download</a>

After you download the blacklist to your device, you can open the downloaded TXT file to view details about the blacklist.

**8. Optional: Manage a whitelist.**

- Add an IP address to the whitelist.
  - a.** Click **Manually Add**.
  - b.** In the **Whitelist Setting** dialog box, enter the IP address whose requests you want to allow to the whitelist.



**Note:**



You can add up to 2,000 IP addresses to the whitelist.



The dialog box is titled "Whitelist Setting" and has a close button (X) in the top right corner. It contains a large text input area for adding IP addresses. Below the input area, there is a note: "You can add up to 2,000 IP addresses or CIDR blocks to the whitelist. Separate multiple entries with spaces or line feeds." At the bottom, there are three buttons: "Add" (blue), "Clear" (red outline), and "Cancel" (gray).

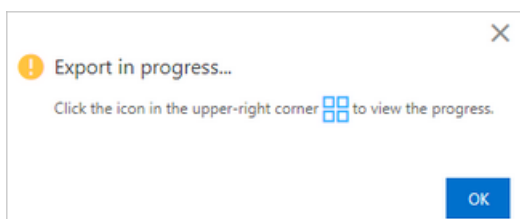
c. Click **Add**.

After the IP address is added to the whitelist, requests from the newly added IP address are directly forwarded to the origin server. IP addresses can only be manually removed from the whitelist.

- Search for IP addresses in the whitelist: Enter a keyword in the search box to search for IP addresses that contain the keyword.
- Clear the whitelist: Click **Clear Whitelist** to remove all IP addresses from the whitelist. You can also click **Delete** next to an IP address to remove it from the whitelist.
- Download the whitelist.

a. Click **Download** to start a download task.

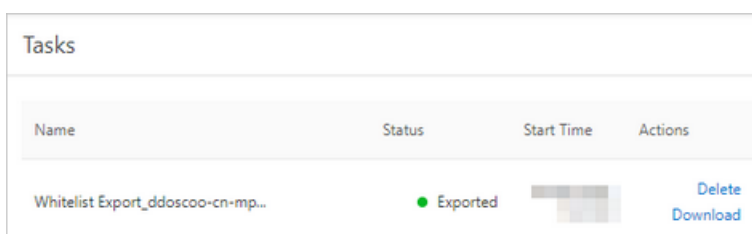
b. In the message that appears, click **OK**.



c. Close the **Blacklist and Whitelist Settings** pane.

d. Click [grid icon] in the upper-right corner to view the task list.

e. Find the download task. After **Status** of the task becomes **Exported**, click **Download** in the Actions column.



Name	Status	Start Time	Actions
Whitelist Export_ddoscoo-cn-mp...	Exported		Delete Download

After you download the whitelist to your device, you can open the downloaded TXT file to view details about the whitelist.

## 9.1.2 Configure diversion from the origin server

This topic describes how to configure the Diversion from Origin Server policy to block network traffic transmitted from regions outside mainland China through China Telecom or China Unicom lines. Each Alibaba Cloud account can enable this policy up to 10 times and disable it at any time.

### Prerequisites

An Anti-DDoS Pro instance is available.



#### Note:

The Diversion from Origin Server policy is available only for Anti-DDoS Pro.

### Context



#### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

We recommend that you enable this policy if your Anti-DDoS Pro instance is under volumetric attacks that are about to exceed the protection capability. For example, if 30% of the attacks are launched from regions outside mainland China, you can use this policy to block these attacks in order to reduce the stress on your Anti-DDoS Pro instance.

After the Diversion from Origin Server policy is enabled, the specified network traffic is dropped at the data center. This minimizes the possibility of triggering a black hole. This way, you can protect your China Telecom or China Unicom lines. A black hole is triggered based on the same rules as Diversion from Origin Server, such as the volume of attack traffic and attack source. Therefore, the Diversion from Origin Server policy can minimize the possibility of triggering a black hole.

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select **Mainland China**.

3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **Protection for Infrastructure** tab, select the target instance from the list on the left side.

**Note:**

You can also search for instances by instance ID or description.

5. In the **Diversion from Origin Server** section, perform the following operations as required.

### Diversion from Origin Server

Block access from source IP addresses to Anti-DDoS Pro. You can perform one-click blocking by using backbone routers of service providers based on geolocation.

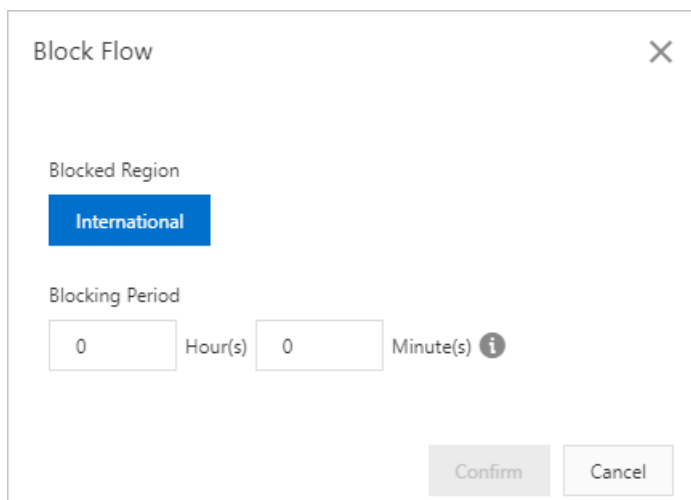
Blocked Regions:China Telecom (International) <a href="#">Blocked</a>	Blocked Regions:China Unicom (International) <a href="#">Deactivate Blackhole</a>	<a href="#">View Blocked Region</a>
--	--	-------------------------------------

You have 9 time(s) remaining to deactivate the blackhole state (10 time(s) in total)

- Block network traffic transmitted from regions outside mainland China through China Telecom lines: Click **Blocked** next to **Blocked Regions:China Telecom (International)**. In the **Block Flow** dialog box, set **Blocking Period** and click **Confirm**.

**Note:**

The minimum blocking period is 15 minutes, and the maximum is 23 hours and 59 minutes.

A screenshot of the 'Block Flow' dialog box. It has a title bar with a close button (X). Inside, there's a 'Blocked Region' section with a blue button labeled 'International'. Below that is a 'Blocking Period' section with two input fields: 'Hour(s)' and 'Minute(s)', both containing the number '0'. There's an information icon (i) next to the 'Minute(s)' field. At the bottom right are 'Confirm' and 'Cancel' buttons.

Block Flow

Blocked Region

International

Blocking Period

0 Hour(s) 0 Minute(s) ⓘ

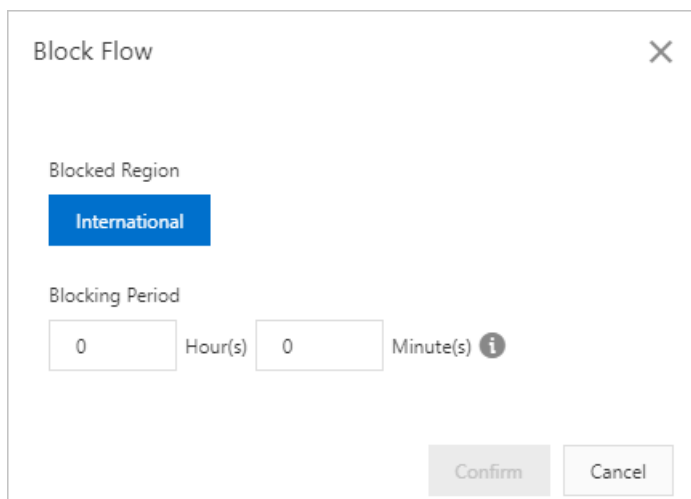
Confirm Cancel

- Block network traffic transmitted from regions outside mainland China through China Unicom lines: Click Blocked next to **Blocked Regions:China Unicom (International)**. In the **Block Flow** dialog box, set **Blocking Period** and click **Confirm**.



**Note:**

The minimum blocking period is 15 minutes, and the maximum is 23 hours and 59 minutes.

A screenshot of the 'Block Flow' dialog box, identical to the one above. It shows the 'Blocked Region' set to 'International' and the 'Blocking Period' set to 0 hours and 0 minutes.

Block Flow

Blocked Region

International

Blocking Period

0 Hour(s) 0 Minute(s) ⓘ

Confirm Cancel



**Note:**

- We recommend that you block network traffic transmitted from regions outside mainland China through China Telecom lines. You also need to monitor the changes in the volume of attack traffic. If the volume of attack traffic is about to exceed the

protection capability of your instance, block the network traffic transmitted from regions outside mainland China through China Unicom lines.

- Each Alibaba Cloud account can enable this policy up to 10 times. Each time you enable this policy, the remaining quota is reduced by one.

If you fail to enable this policy, an error message appears. Follow the instructions to troubleshoot the error and try again. If no message appears, this policy is enabled.

- Optional: In the **Diversion from Origin Server** section, click **View Blocked Region**. In the **Flow Blocking for Source** pane, you can view the blocked regions and the blocking periods.

Flow Blocking for Source <span>×</span>						
You have 9 time(s) remaining to deactivate the blackhole state (10 time(s) in total)						
Service Address	ISP	Blocked Region	Status	Blocking Period	Deactivated Time	Blocked Time
203.199	China Telecom	International	Normal	--	--	--
203.199	China Unicom (Beta)	International	Blocking	03/05/2020, 13:52:01	03/05/2020, 14:52:01	1 Minutes 6 Seconds

- Optional: Unblock network traffic.

To **unblock** the network traffic that you have **blocked** before the blocking period expires, click **Deactivate Blackhole**.

### 9.1.3 Configure blocked regions

This topic describes how to configure and enable the Blocked Regions policy. This policy allows you to block requests initiated from IP addresses in specific regions (regions inside and outside China) for an Anti-DDoS Pro or Anti-DDoS Premium instance. Anti-DDoS Pro or Anti-DDoS Premium instances that use the enhanced function plan support this policy. After you enable this policy, requests from the specified regions to access Anti-DDoS Pro or Anti-DDoS Premium instances are dropped.

#### Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance that uses the enhanced function plan is available. For more information, see [Purchase Anti-DDoS Pro or Anti-DDoS Premium instances](#).

#### Context



#### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

This policy directly drops requests initiated from IP addresses in specific regions (regions inside and outside China) to block the sources of requests. If most requests are sent from regions inside China that include Hong Kong S.A.R, Macao S.A.R, and Taiwan to an Anti-DDoS Pro or Anti-DDoS Premium instance, deny requests from regions outside China.

**Note:**

This policy takes effect on Anti-DDoS Pro or Anti-DDoS Premium instances. You must configure this policy separately for each Anti-DDoS Pro or Anti-DDoS Premium instance.

**Blocked Regions and Diversion from Origin Server**

The Blocked Regions policy blocks requests from specific regions in scrubbing centers. This policy drops blocked requests near the destination servers. Anti-DDoS Pro or Anti-DDoS Premium instances identify and filter requests based on the region of the source IP addresses. This policy cannot reduce the volume of attack traffic. Therefore, it is suitable for blocking attacks that consume system resources.

The Diversion from Origin Server policy drops requests from specific regions based on the attack source by using core routers on the network provided by an ISP. For more information, see [Configure diversion from the origin server](#).

**Note:**

The Diversion from Origin Server policy is available only for Anti-DDoS Pro.

**Blocked Regions and Blocked Regions (Domain Names)**

The Blocked Regions policy configured for Anti-DDoS Pro or Anti-DDoS Premium instances has a higher priority than the Blocked Regions (Domain Names) policy when they are used together.

For example, if you have enabled Blocked Regions for an Anti-DDoS Pro or Anti-DDoS Premium instance to block requests from regions outside China, users outside China cannot access domain names associated with this instance regardless of whether Blocked Regions

(Domain Names) is enabled for the domain names. If you want to block regions outside China for some services, we recommend that you configure blocked regions for domain names rather than Anti-DDoS Pro or Anti-DDoS Premium instances. For more information, see [Configure blocked regions for domain names](#).

#### Procedure

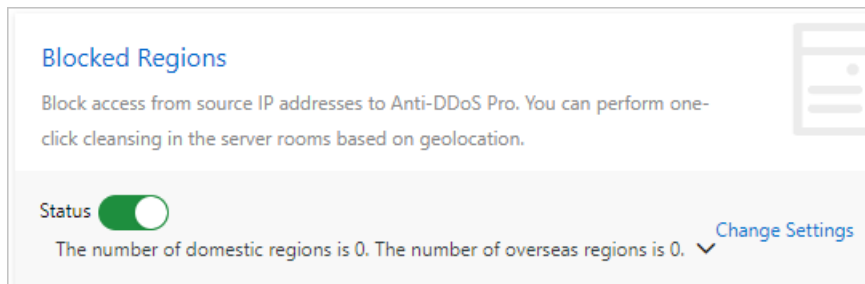
1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **Protection for Infrastructure** tab, select the target instance from the list on the left side.



#### Note:

You can also search for instances by instance ID or description.

5. In the **Blocked Regions** section, click **Change Settings**.



6. In the **Configure Blocked Regions** pane, select the regions that you want to block and then click **OK**.
7. Go back to the **Blocked Regions** section and turn on **Status** to apply the settings.

### 9.1.4 Deactivate a black hole

After you set up an Anti-DDoS Pro instance to protect your services, black holes may be triggered due to insufficient basic or burstable protection bandwidth. In this case, you can manually deactivate black holes in the Anti-DDoS Pro console to recover services. The Deactivate Blackhole Status policy allows you to quickly recover your services. We recommend that you make sure that the basic or burstable protection capabilities meet your requirements before you deactivate black holes. This prevents Anti-DDoS Pro instances from being thrown into black holes again.

## Prerequisites

An Anti-DDoS Pro instance is available.



### Note:

The Deactivate Blackhole Status policy is available only for Anti-DDoS Pro.

## Context



### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

Each Alibaba Cloud account can deactivate black holes up to five times a day. The limit is reset at 00:00 the next day. You consume a chance to deactivate a black hole only when the black hole is successfully deactivated. You can immediately deactivate the first black hole of a day. However, you cannot deactivate more than one black hole every 10 minutes.

## Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select **Mainland China**.
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **Protection for Infrastructure** tab, select the target instance from the list on the left side.

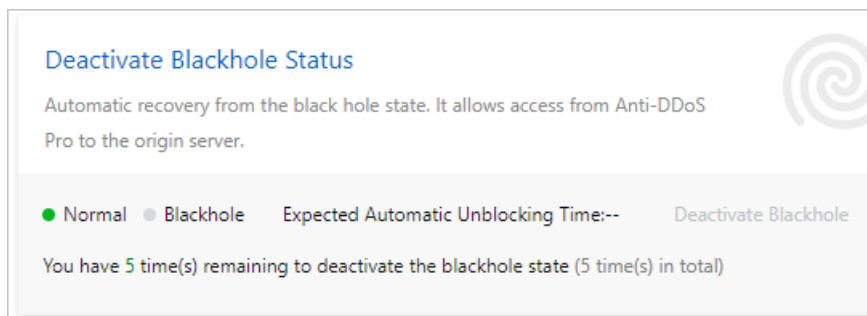


### Note:

You can also search for instances by instance ID or description.



5. In the **Deactivate Blackhole Status** section, deactivate black holes based on the instance status.



- If the instance is in the **Blackhole** state, and you do not want to wait for the black hole to be automatically deactivated, click **Deactivate Blackhole** and wait for the black hole to be deactivated.
- If the instance is in the **Normal** state, the **Deactivate Blackhole** button is dimmed.

## Result

- Black holes are a risk management strategy used by the backend servers of Alibaba Cloud. If your attempts to deactivate black holes fail, your deactivation quota for the day is not affected, and an error message appears. In this case, wait and try again later.
- If the message "Cannot deactivate the black hole status due to risk management. Wait 10 minutes and try again." appears, wait 10 minutes and try again.
- If no error message appears, black holes are deactivated. You can refresh the page to check whether network access is restored.

## 9.2 Protection for website services

### 9.2.1 Configure intelligent protection

This topic describes how to use Intelligent Protection provided by Anti-DDoS Pro and Anti-DDoS Premium to protect website services. Intelligent Protection is developed based on the big data technologies of Alibaba Cloud. It automatically learns traffic patterns and uses algorithms to analyze attacks. It then implements accurate access control rules to adjust protection modes and to quickly detect and block attacks, such as malicious bots and HTTP flood attacks.

#### Prerequisites

- A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Add a website](#).

- Protection settings in Anti-DDoS Pro or Anti-DDoS Premium of the latest version are enabled.

## Context



### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect website services, you can enable Intelligent Protection. The intelligent protection engine automatically learns traffic patterns and protects the website against web attacks by using accurate access control rules.

### Intelligent Protection mode

Intelligent Protection supports the following protection modes:

- **Warning:** In this mode, when Anti-DDoS Pro or Anti-DDoS Premium detects malicious requests, it records the attacks but does not block any request. You can use this mode to learn how Intelligent Protection safeguards your website.

You can use this mode and the Log Analysis feature to query warnings recorded by Intelligent Protection and verify its protection capabilities. For more information, see [View attack warning logs](#).

- **Defense:** In this mode, when Anti-DDoS Pro or Anti-DDoS Premium detects malicious requests, it directly applies accurate access control rules to block malicious requests.



### Note:

Intelligent Protection uses accurate access control rules to trigger actions. To make sure that Intelligent Protection works as expected, you must enable Accurate Access Control. For more information, see [Configure accurate access control rules](#).

We recommend that you use the Warning mode and the Log Analysis feature to analyze the attack logs. Enable the Defense mode only when Intelligent Protection works as expected for this policy to take effect.

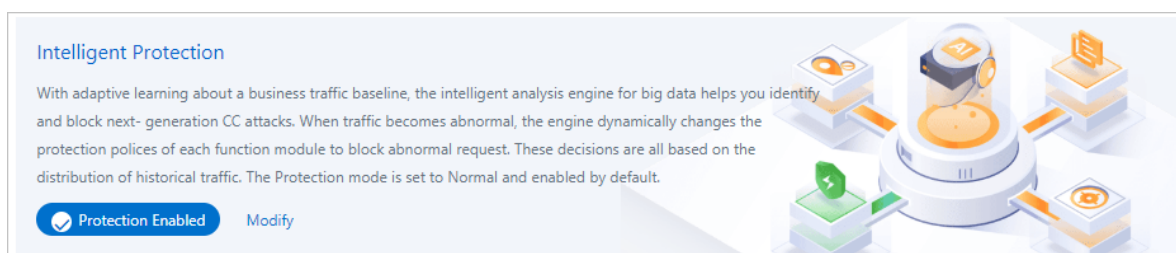
### Intelligent Protection level

If you enable Intelligent Protection, you can select a protection level as required. The following table describes the protection levels provided by Intelligent Protection.

Level	Effect	Scenario
<b>Low</b>	Blocks specific attacks and allows normal requests.	Large websites with high processing capabilities, and specific scenarios such as sales promotions
<b>Normal</b> (recommended)	Does not process requests in most cases. When detecting traffic that poses a threat to the protected website, Anti-DDoS Pro or Anti-DDoS Premium protects the website and minimizes the negative impacts on the website services.	Scenarios where the number of requests does not greatly fluctuate and the servers have additional resources other than managing normal network traffic
<b>Strict</b>	Strictly and intelligently blocks attacks but may block normal requests.	Websites that have weak protection capabilities

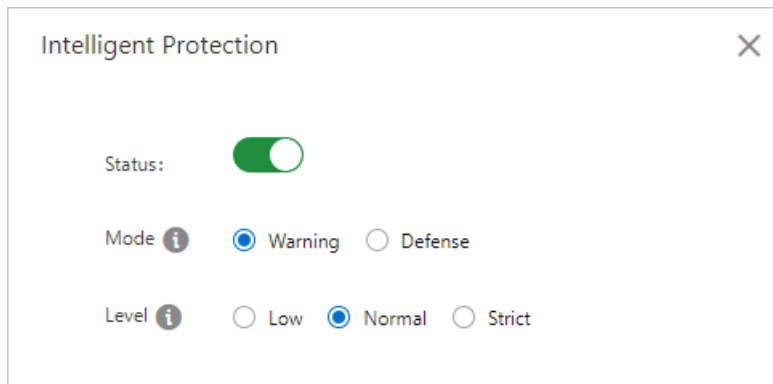
## Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **General Policies** page, click the **Protection for Website Services** tab. On the tab that appears, select the target domain name from the list on the left side.
5. In the **Intelligent Protection** section, click **Modify**.



6. In the **Intelligent Protection** dialog box, set **Mode** and **Level**, and turn on **Status**.

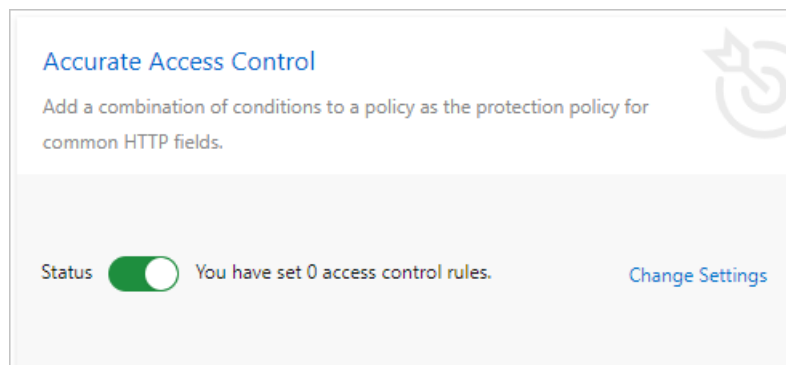
- **Mode:** Set this parameter to **Warning** or **Defense**.
- **Level:** Set this parameter to **Low**, **Normal**, or **Strict**.



After Intelligent Protection is enabled, Anti-DDoS Pro or Anti-DDoS Premium automatically generates accurate access control rules when it detects malicious attacks. You can view the rules in the Accurate Access Control section.

### View accurate access control rules

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **General Policies** page, click the **Protection for Website Services** tab. On the tab that appears, select the target domain name from the list on the left side.
5. In the **Accurate Access Control** section, click **Change Settings**.



## 6. On the **Accurate Access Control** page, view the rules that start with **smartcc\_**.

Accurate access control rules created by Intelligent Protection start with smartcc\_.

Compared with user-defined accurate access control rules, those created by Intelligent Protection have the following characteristics:

- The action of a rule may be a warning. In Warning mode, the action specified in an accurate access control rule that is created by Intelligent Protection is a warning. In this case, Anti-DDoS Pro or Anti-DDoS Premium records attacks but does not block attacks.
- Each rule has a validity period. After a rule expires, it becomes invalid and is automatically deleted.
- Rules cannot be manually deleted. If you disable Intelligent Protection, rules created by Intelligent Protection are immediately deleted.

### View attack warning logs

After you enable Intelligent Protection for website services, the Log Analysis feature records detected attacks that hit Intelligent Protection rules. You can query the attack warning logs associated with the Intelligent Protection rules on the Log Analysis page. This allows you to check the performance levels of Intelligent Protection.

#### Prerequisites

- The Log Analysis feature is enabled for a website. For more information, see [Full log](#).
- The Intelligent Protection policy is enabled for a website and set to the Warning mode.

#### Queries

Log on to the Anti-DDoS Pro or Anti-DDoS Premium console and choose **Investigation > Log Analysis**. On the page that appears, select a domain name and enter the following query statement to view the attack warning logs related to Intelligent Protection:



#### Note:

Replace test.aliyundemo.com with the actual website domain.

```
matched_host:"test.aliyundemo.com" and cc_action:alarm
```

## 9.2.2 Configure blacklists and whitelists for domain names

This topic describes how to configure the Black Lists and White Lists (Domain Names) policy in Anti-DDoS Pro or Anti-DDoS Premium to protect website services. After you enable this

policy, access requests from the IP addresses or CIDR blocks in the blacklist are blocked, while access requests from the IP addresses or CIDR blocks in the whitelist are allowed.

### Prerequisites

A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Add a website](#).

### Context



#### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect website services, you can add malicious IP addresses to the blacklist to block requests from them. You can add trusted IP addresses to the whitelist. Requests received from whitelisted IP addresses are forwarded directly to the website.

### Precautions

- You can only enable the Black Lists and White Lists (Domain Names) policy for website services. You can configure a blacklist or whitelist on the Protection for Infrastructure tab for non-website services. For more information, see [Configure a blacklist or whitelist for destination IP addresses](#).



#### Note:

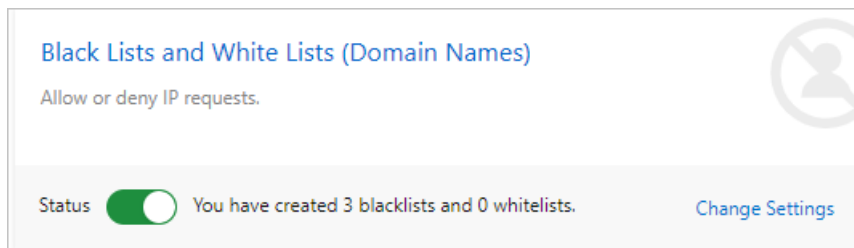
The Black Lists and White Lists (Destination IP) policy is available only for Anti-DDoS Pro.

- The Black Lists and White Lists (Domain Names) policy only takes effect on a single domain name. It does not take effect on an Anti-DDoS Pro or Anti-DDoS Premium instance.
- You can configure up to 200 IP addresses or CIDR blocks in a blacklist or whitelist for a domain name.

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).

2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **General Policies** page, click the **Protection for Website Services** tab and select the target domain name from the list on the left side.
5. In the **Black Lists and White Lists (Domain Names)** section, click **Change Settings**.



6. In the **Blacklist and Whitelist Settings** dialog box, configure the blacklist and whitelist and then click **OK**.
  - On the **Blacklist** tab, enter the malicious IP addresses or CIDR blocks that you want to block.
  - On the **Whitelist** tab, enter the IP addresses or CIDR blocks that you want to allow to pass through.

**Note:**

- You can enter IP addresses or CIDR blocks. CIDR blocks must be in the format of IP address/Subnet mask.
- You can add up to 200 IP addresses or CIDR blocks to a whitelist or blacklist. Separate multiple IP addresses or CIDR blocks with commas (,).

- You can add 0.0.0.0/0 to the blacklist to block requests from all IP addresses except those added to the whitelist.

Blacklist and Whitelist Settings

Blacklist Whitelist

IP addresses in the blacklist will be blocked:

1. 1/24, 2. 2/32, 5. 5/32

Enter IP addresses or IP address/CIDR. Separate multiple entries with commas (,). You can enter a maximum of 200 IP addresses.

OK Cancel

7. Go back to the **Black Lists and White Lists (Domain Names)** section and turn on **Status** to apply the settings.

**Note:**

If you use an earlier version, you must enable HTTP flood prevention for the blacklist and whitelist to take effect.

**Result**

After the policy is enabled, the settings apply to each Anti-DDoS Pro or Anti-DDoS Premium instance associated with domain names and take effect on access to the domain names immediately.

**Note:**

In some situations, the Black Lists and White Lists (Domain Names) policy takes effect only after your instance receives and processes certain inbound traffic. If the settings do not take effect after the policy is enabled, you can access the domain names several times to initiate the settings.

### 9.2.3 Configure blocked regions for domain names

This topic describes how to configure the Blocked Regions (Domain Names) policy in both Anti-DDoS Pro and Anti-DDoS Premium for protected website services. If this policy is



configured and enabled, you can block all access requests from IP addresses of specific regions, such as regions inside or outside China.

### Prerequisites

- A website is added to Anti-DDoS Pro or Anti-DDoS Premium and associated with an instance that uses the enhanced function plan. For more information, see [Add a website](#).
- Protection settings in Anti-DDoS Pro or Anti-DDoS Premium of the latest version are enabled.

### Context



#### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

If you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service and most requests are sent from regions inside China to your instance, deny requests from regions outside China. You can also block other regions as required. To use this policy, specify the regions that you want to block. Supported regions are as follows:

- Regions inside China

Shanghai, Yunnan, Nei Mongol, Beijing, Jilin, Sichuan, Tianjin, Ningxia, Anhui, Shandong, Shaanxi, Shanxi, Guangdong, Guangxi, Xinjiang, Jiangsu, Jiangxi, Hebei, Henan, Zhejiang, Hainan, Hubei, Hunan, Gansu, Fujian, Xizang, Guizhou, Liaoning, Chongqing, Qinghai, Heilongjiang, Hong Kong S.A.R, Macao S.A.R, and Taiwan

- Regions outside China

Asia (except for regions inside China), Europe, North America, South America, Africa, Oceania, and Antarctica

### Precautions

- This policy is available only for website services. To protect non-website services, we recommend that you configure the traffic block policies on the Protection for Infrastructure tab. For more information, see [Configure diversion from the origin server](#), which is only supported by Anti-DDoS Pro, and [Configure blocked regions](#).

- This policy is valid only for domain names. If you need to block regions for different domain names, you must specify the regions you want to block for the domain names separately.
- This policy only identifies and filters requests from IP addresses that are in the blocked regions. It cannot reduce the volume of transmitted attack traffic.

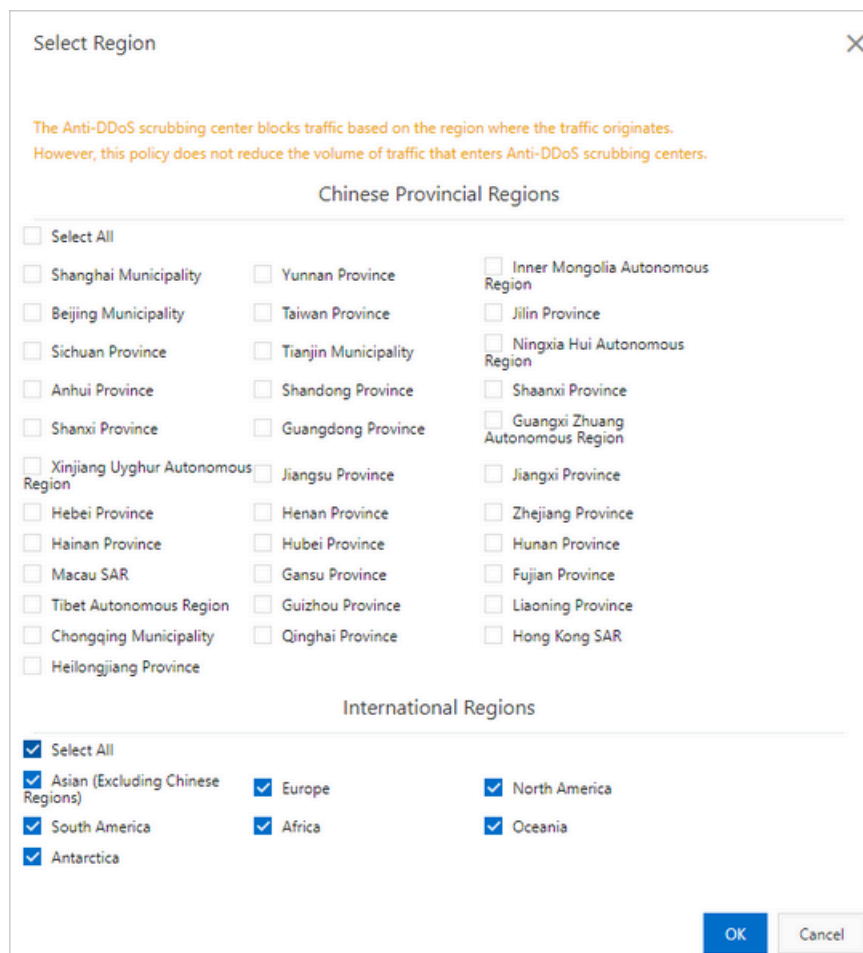
#### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **General Policies** page, click the **Protection for Website Services** tab. On the tab that appears, select the target domain name from the list on the left side.
5. In the **Blocked Regions (Domain Names)** section, click **Change Settings**.



6. In the **Select Region** dialog box, select the regions that you want to block and then click **OK**.

As shown in the following figure, requests from regions outside China cannot access your website after you configure the blocked regions.



7. Go back to the **Blocked Regions (Domain Names)** section and turn on **Status** to apply the configuration.

## Result

After this policy is enabled, the configuration takes effect immediately on all Anti-DDoS Pro or Anti-DDoS Premium instances associated with a domain name.

## 9.2.4 Configure accurate access control rules

Both Anti-DDoS Pro and Anti-DDoS Premium allow you to create accurate access control rules for website services that they protect. The Accurate Access Control policy allows you to customize access control rules. You can filter access requests based on commonly used HTTP fields, such as IP, URI, Referer, User-Agent, and Params. For requests that meet the filter conditions, you can allow, block, or verify them. This policy supports custom

protection policies for different scenarios, such as hotlinking protection and management console protection.

### Prerequisites

- A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Add a website](#).
- Protection settings in Anti-DDoS Pro or Anti-DDoS Premium of the latest version are enabled.

### Context

If your website is protected by Anti-DDoS Pro or Anti-DDoS Premium and you want to manage requests that have specific characteristics, you can enable Accurate Access Control for your website and create accurate access control rules. Each accurate access control rule consists of one or more match conditions and one action.

- Match conditions specify the HTTP fields to be recognized. The following table describes the HTTP fields supported by accurate access control rules.

**Note:**

Different HTTP fields use different logical operators. For example, the source IP field uses the Is Part Of or Is Not Part Of logical operator. The URI field uses the Contains or Does Not Contain logical operator. For more information, see the Supported logical operator column in the following table.

Field	Description	Supported logical operator
IP	The source IP address of the request.	Is Part Of and Is Not Part Of
URI	The request URI.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, and Is Longer Than
User-Agent	The information about the client browser that sends the request.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, and Is Longer Than
Cookie	The cookie in the request.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, Is Longer Than, and Does Not Exist

Field	Description	Supported logical operator
Referer	The source URI of the request, namely, the page from which the access request is redirected.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, Is Longer Than, and Does Not Exist
Content-Type	The HTTP content type of the response specified by the request, namely, MIME type information.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, and Is Longer Than
X-Forwarded-For	The actual client IP address of the request.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, Is Longer Than, and Does Not Exist
Content-Length	The amount of bytes in the HTTP body of the request.	Is Smaller Than, Has a Value Of, and Is Larger Than
Post-Body	The content of the request.	Contains, Does Not Contain, Equals, and Does Not Equal
Http-Method	The request method. Valid values: GET, POST, DELETE, PUT, OPTIONS, CONNECT, HEAD, and TRACE.	Equals and Does Not Equal
Header	The request header that is used to customize the HTTP header field and value.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, Is Longer Than, and Does Not Exist
Params	The parameters in the request URI. The parameter part of the URI usually follows a question mark (?). For example, in URI <code>www.abc.com/index.html? action =login</code> , the parameter part is <code>action=login</code> .	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, and Is Longer Than

- An action defines how the request is handled if a request meets the match conditions. Actions include Clear, Blocked, and JS Challenge. The challenge action verifies the source IP address by using JavaScript.

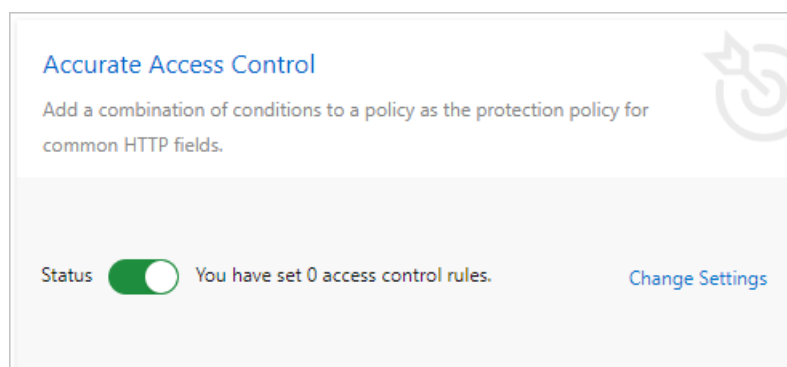
## Limits

The following table describes the limits on Accurate Access Control based on the function plan of an Anti-DDoS Pro or Anti-DDoS Premium instance.

Limit	Standard function plan	Enhanced function plan
Number of custom rules	≤ 5	≤ 10
Supported match fields	IP, URI, Referer, and User-Agent	All fields that support matching

## Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **General Policies** page, click the **Protection for Website Services** tab. On the tab that appears, select the target domain name from the list on the left side.
5. In the **Accurate Access Control** section, click **Change Settings**.



## 6. Configure accurate access control rules for the domain name.

Name	Match Condition	Action	Expire Time	Actions
test_rule1	Request URI Equals /login Request User-Agent Contains chrome	JS Challenge	03/05/2020, 16:45:08	<a href="#">Edit</a> <a href="#">Delete</a>
test_rule2	Request IP Is Part Of 1...1	Blocked	Permanent	<a href="#">Edit</a> <a href="#">Delete</a>

- Create a rule

### a. Click **Create Rule**.



#### Note:

If the number of custom rules reaches the upper limit, the **Create Rule** button is unavailable.

- b. In the **Create Rule** dialog box, specify the required parameters and then click **OK**.

**Create Rule**

\* Name: test\_rule

\* Match:

Field Name	Logical Relation	Field Value (Case sensitive)	
URI	Equals	/login	<a href="#">Remove</a>
User-Agent	Contains	chrome	<a href="#">Remove</a>

+ Add Condition

\* Action: JS Challenge

\* Validity: 120 Minutes

[OK](#) [Cancel](#)

Parameter	Description
<b>Name</b>	The name of the rule. The name can be up to 128 characters in length and can contain letters, digits, and underscores (_).

Parameter	Description
<b>Match Conditions</b>	<p>The match condition of the rule. To add match conditions of a rule, click <b>Add Condition</b>. Each condition consists of <b>Field Name</b>, <b>Logical Relation</b>, and <b>Field Value</b>.</p> <ul style="list-style-type: none"> <li>- Set Field Name and Logical Relation based on <a href="#">Supported match field</a>.</li> <li>- Set Field Value based on Field Name. The value of Field Value is case sensitive. Field Value does not support regular expressions, but can be left blank.</li> </ul> <p>You can add multiple match conditions. If multiple match conditions are specified, a request matches the rule only when all the conditions are met.</p>
<b>Action</b>	<p>The operation that is performed when a request meets the match conditions. Valid values:</p> <ul style="list-style-type: none"> <li>- <b>Blocked</b>: Requests that meet match conditions are blocked.</li> <li>- <b>Clear</b>: Requests that meet match conditions are allowed.</li> <li>- <b>JS Challenge</b>: JavaScript verification is required for the source IP address of the request that meets the match conditions.</li> </ul>
<b>Validity</b>	<p>The validity period of the rule. You can set this parameter to 5 Minutes, 10 Minutes, 30 Minutes, 60 Minutes, 90 Minutes, 120 Minutes, or Permanent.</p>

In this example, after configurations are complete, if a request is sent to a `/login` page and the User-Agent field of the request contains `chrome`, the source IP address must pass JavaScript verification. The rule remains effective 120 minutes after it is created.

You can create multiple rules as required.



**Note:**

- If you create multiple rules, the priority of a rule depends on its rank in the rule list. The higher the rank, the higher the priority. The system compares a request against rules based on their priorities. The higher the rule priority, the sooner the rule is compared.



- If a request meets multiple match conditions of different rules, the action of the rule with the highest priority takes effect.

### Examples

- Block specific requests

In most cases, the root directory of a website does not receive POST requests. If HTTP flood attacks occur, your website may receive a large number of POST requests that target the root directory. We recommend that you check whether these requests are valid. If these requests are invalid, you can use accurate access control rules to block them. The following figure shows sample configurations.

The screenshot shows a 'Create Rule' dialog box with the following configuration:

- Name:** POST\_ROOT
- Match Conditions:**
  - Field Name: URI, Logical Relation: Equals, Field Value: /
  - Field Name: Http-Method, Logical Relation: Equals, Field Value: POST
- Action:** Blocked
- Validity:** Permanent

Buttons: OK, Cancel

- Block web crawlers

If your website receives a large number of crawler requests within a certain period of time, which may be HTTP flood attacks initiated from bots that simulate

crawlers, you can block these requests. The following figure shows sample configurations.

The screenshot shows a 'Create Rule' dialog box. It has a title bar with 'Create Rule' and a close button. The main area contains the following fields:

- Name:** A text input field containing 'Spider'.
- Match:** A table with three columns: 'Field Name', 'Logical Relation', and 'Field Value'. The first row contains 'User-Agent', 'Contains', and 'spider'. There is a 'Remove' button next to the 'Field Value' input.
- Conditions:** A section with a '+ Add Condition' link.
- Action:** A dropdown menu set to 'Blocked'.
- Validity:** A dropdown menu set to '120 Minutes'.

At the bottom right, there are 'OK' and 'Cancel' buttons.

- Edit a rule
    - a. In the rule list, find the target rule and click **Edit** in the Actions column.
    - b. In the **Edit Rule** dialog box, modify the rule settings and click **OK**. Configure the rule settings in the same way you create a rule. However, you cannot change the value of **Name**.
  - Delete a rule
    - a. In the rule list, find the target rule and click **Delete** in the Actions column.
    - b. In the message that appears, click **OK**.
7. Go back to the **Accurate Access Control** section and turn on **Status** to apply the settings.

## 9.2.5 Configure frequency control

Both Anti-DDoS Pro and Anti-DDoS Premium allow you to configure the Frequency Control policy for protected website services. You can use this policy to control the frequency of requests sent to your website from specific IP addresses. Frequency Control takes effect immediately after it is enabled. By default, the Normal mode is used to protect website services against common HTTP flood attacks. Frequency Control supports multiple modes for different scenarios. You can also create custom frequency control rules to prevent a specific IP address from frequently visiting a page in a short period of time.

### Prerequisites

- A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see [Add a website](#).
- Protection settings in Anti-DDoS Pro or Anti-DDoS Premium of the latest version are enabled.

## Context



### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service, you can enable Frequency Control to protect the website against HTTP flood attacks . Frequency Control supports multiple modes and allows you to adjust the mode in real time based on the traffic status of the website.

- Normal: We recommend that you use this mode if the website traffic is normal. By default, this mode is used. In this mode, Frequency Control protects websites against common HTTP flood attacks but does not block normal requests.
- Emergency: You can enable this mode when you detect HTTP response errors, traffic anomalies, or CPU and memory usage spikes. The Emergency mode provides relatively rigorous protection compared to the Normal mode. In this mode, Frequency Control protects websites against more complicated HTTP flood attacks but may block a few normal requests.
- Strict: This mode provides rigorous protection. It uses Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) to verify the identities of all visitors. Only verified visitors are allowed to access the website.



### Note:

The CAPTCHA verification mechanism of this mode allows the requests that are initiated by real users from browsers. However, if the protected website provides API or native application services, requests to the website cannot pass the verification and will fail to access the services provided by the website.

- **Super Strict:** This mode provides the most rigorous protection against HTTP flood attacks. It uses CAPTCHA to verify the identities of all visitors. Only verified visitors are allowed to access the website. Compared to the Strict mode, this mode combines CAPTCHA verification with anti-debugging and anti-machine verification technologies to enhance the protection of your website.

**Note:**

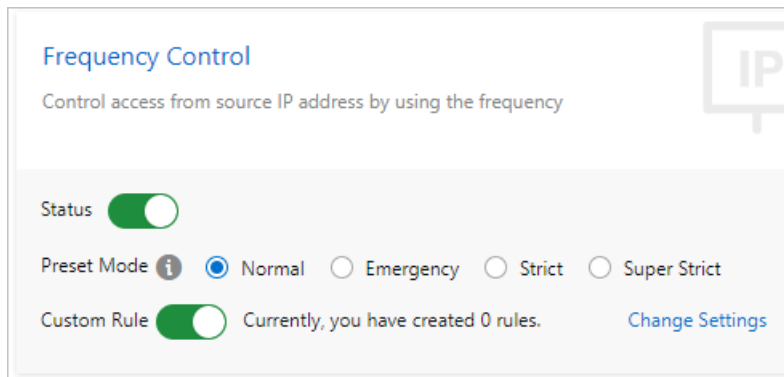
The CAPTCHA verification mechanism of this mode allows the requests that are initiated by real users from browsers. Exceptions may occur in some browsers and cause the website to be inaccessible. In this case, you can restart the browser and revisit the website. However, if the protected website provides API or native application services, requests to the website cannot pass the verification and will fail to access the services provided by the website.

In addition to the protection modes, Frequency Control also allows you to create custom rules to block attacks more precisely. You can create a custom rule to protect a specific URL. After a custom rule is created, the specified IP address cannot frequently access the URL in a short period of time.

**Configure a frequency control mode**

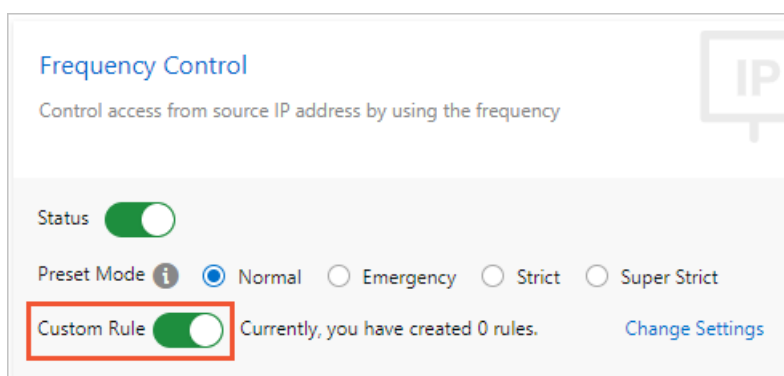
1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **General Policies** page, click the **Protection for Website Services** tab. On the tab that appears, select the target domain name from the list on the left side.

5. In the **Frequency Control** section, set **Preset Mode** as required and turn on **Status**. Supported modes include **Normal**, **Emergency**, **Strict**, and **Super Strict**.



### Create a custom frequency control rule

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **General Policies** page, click the **Protection for Website Services** tab. On the tab that appears, select the target domain name from the list on the left side.
5. In the **Frequency Control** section, turn on **Custom Rule** and then click **Change Settings**.



## 6. Create a frequency control rule for a domain name.

Domain:  com [Back](#)

Custom HTTP Flood Protection Rules Currently, 1 rules have been created. You can create 19 more rules. [Create Rule](#)

Name	Protected URI	Interval	Individual IP Visits	Matching Rule	Block Type	Block Duration	Actions
test_rule1	/abc	5 Seconds	2	Exact Match	Block	1 Minutes	<a href="#">Edit</a> <a href="#">Delete</a>

Total Items: 1, Items per Page 10 < Previous **1** Next >

- Create a rule

### a. Click **Create Rule**.



#### Note:

A maximum of 20 rules can be created. If the number of rules reaches the upper limit, the **Create Rule** button is dimmed.

- b. In the **Create Rule** dialog box, specify the required parameters and then click **OK**.

Create Rule ✕

\* Name:  Enter a maximum of 128 characters that can be letters, numbers, and ur

\* URI:  For example: /abc/a.php  
If one or more parameters are specified in a URL, we recommend that you use prefix matches.

\* Matching Rule: ☒ Exact Match ☐ Prefix Match

\* Interval:  5 Seconds  
Enter an integer from 5 to 10800.

\* Individual IP:  2 Requests  
Visits: Enter an integer from 2 to 2000.

\* Block Type: ☒ Block ☐ Captcha Verification  
 1 Minutes  
Enter an integer from 1 to 1440.

[OK](#) [Cancel](#)

Configuration	Description
<b>Name</b>	The name of this rule.
<b>URI</b>	The URI path to be protected. For example, /register. The path can contain parameters connected by "?". For example, you can use /user? action=login.

Configuration	Description
<b>Matching rule</b>	<ul style="list-style-type: none"> <li>- <b>Exact Match:</b> The request URI must be exactly the same as the configured URI here to get counted.</li> <li>- <b>URI Path Match:</b> When the request URI starts with the URI value configured here, the request is counted. For example, /register.html is counted if you use /register as the URI.</li> </ul>
<b>Interval</b>	The cycle for calculating the number of visits. It works in sync with <b>Visits from one single IP address</b> .
<b>Visits from a single IP address</b>	The number of visits allowed from a single source IP address to the URL during the <b>Interval</b> .
<b>Blocking type</b>	<p>The action to be performed after the condition is met. The operations can be Block or Human-Machine Identification.</p> <ul style="list-style-type: none"> <li>- <b>Block:</b> blocks accesses from the client after the condition is met.</li> <li>- <b>Man-Machine Identification:</b> accesses the client with redirection after the condition is met. Only the verified requests are forwarded to the origin.</li> </ul>

You can create multiple rules as required.

- Edit a rule
  - In the rule list, find the target rule and click **Edit** in the Actions column.
  - In the **Edit Rule** dialog box, modify the settings and click **OK**. Specify the parameters in the same way you create a rule. However, you cannot change **Name** and **URI**.
- Delete a rule
  - In the rule list, find the target rule and click **Delete** in the Actions column.
  - In the message that appears, click **OK**.

**7.** Go back to the **Frequency Control** section and turn on **Status** to apply the rule.

### Best practices

The protection intensities provided by different protection modes are listed in descending order: Super Strict > Strict > Emergency > Normal. The probabilities of false positives when you use these protection modes are listed in descending order: Super Strict > Strict > Emergency > Normal.

In normal situations, we recommend that you use the Normal mode for your protected website. In this mode, Frequency Control only blocks IP addresses that frequently send requests to your website. We recommend that you use the Emergency or Strict mode when your website is overwhelmed by HTTP flood attacks and the Normal mode fails to protect your website.

If your website provides API or native application services and the Strict or Super Strict mode is enabled, requests to the website cannot pass the verification. Therefore, these two modes are not suitable to protect this kind of website. You must create custom rules to protect specific URLs from HTTP flood attacks.

## 9.3 Protection for non-website services

### 9.3.1 Configure Layer 4 intelligent protection

The Intelligent Protection policy of Anti-DDoS Pro and Anti-DDoS Premium is enabled by default. This policy uses algorithms to learn the historical traffic patterns of protected services and then adjusts the traffic scrubbing policies of Layer 4 services to better safeguard the services. After your service is protected by Anti-DDoS Pro or Anti-DDoS Premium, the Intelligent Protection policy of the Normal level is enabled by default. If the Normal level cannot meet your requirements, you can set the level to Low or Strict as required.

#### Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is available. For more information, see [Purchase Anti-DDoS Pro or Anti-DDoS Premium instances](#).

#### Context



#### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

To protect your services against Layer 4 DDoS attacks, both Anti-DDoS Pro and Anti-DDoS Premium support the Low, Normal, and Strict levels of Intelligent Protection. These levels are provided based on historical traffic patterns of services and technical experience from



Alibaba Cloud attack and defense experts. The Intelligent Protection policy is enabled by default. The default protection level is Normal. You can change the level as required.

Intelligent Protection works based on historical traffic patterns. If this is your first time to set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your services, it takes about three days for Anti-DDoS Pro or Anti-DDoS Premium to learn the traffic patterns in order to provide optimal protection.

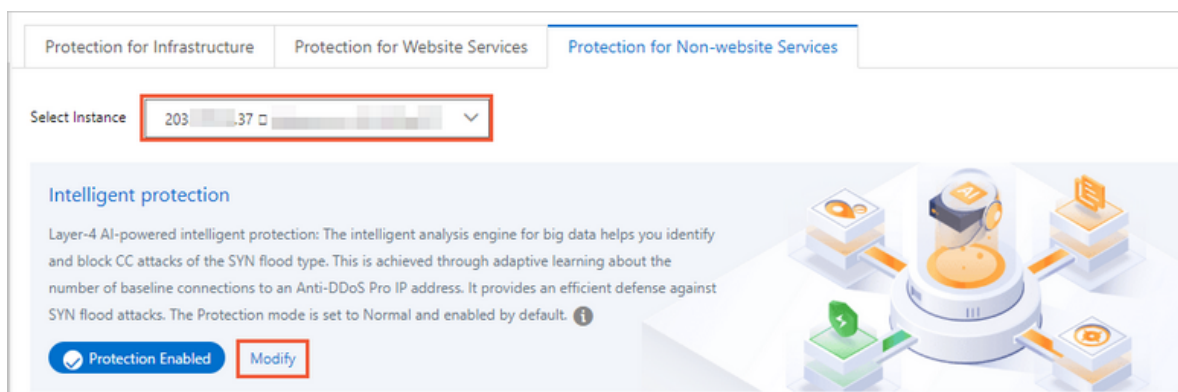
Intelligent protection algorithms automatically add malicious IP addresses to a blacklist and drop all requests from these IP addresses within a specific time period. You can view IP addresses and remove them from the blacklist, or manually add IP addresses to the blacklist. You can also add IP addresses to a whitelist. This ensures that requests from these IP addresses are allowed. For more information, see [Configure a blacklist or whitelist for destination IP addresses](#).

**Note:**

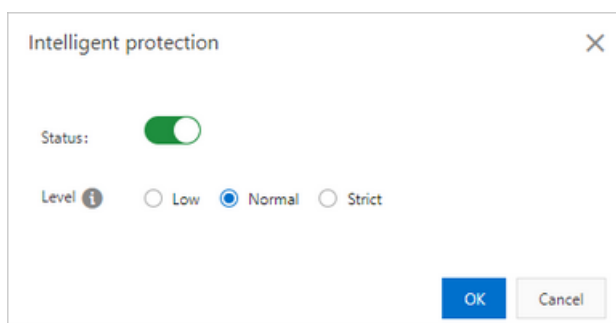
The Black Lists and White Lists (Destination IP) policy is available only for Anti-DDoS Pro.

**Procedure**

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **General Policies** page, click the **Protection for Non-website Services** tab and select the target instance from the Select Instance drop-down list.
5. In the **Intelligent protection** section, click **Modify**.



6. In the **Intelligent protection** dialog box, set **Level** as required and then click **OK**.



Protection levels are described as follows:

- **Low:** At this level, Intelligent Protection automatically scrubs traffic from malicious IP addresses. It may not be able to block all Layer 4 volumetric attacks but has a low false positive rate.
- **Normal:** At this level, Intelligent Protection automatically scrubs traffic from malicious and potentially malicious IP addresses. It is the default level. Intelligent Protection protects services against DDoS attacks while maintaining a low false positive rate at this level. We recommend that you use this level for most scenarios.
- **Strict:** At this level, Intelligent Protection provides the strongest protection against DDoS attacks but may cause false positives.

After the protection level is set, the Anti-DDoS Pro or Anti-DDoS Premium instance will protect services based on the configured level.

### 9.3.2 Create an anti-DDoS protection policy

This topic describes how to create anti-DDoS protection policies. Both Anti-DDoS Pro and Anti-DDoS Premium allow you to create the following anti-DDoS protection policies to protect non-website services against Layer 4 DDoS attacks: False Source, Empty Connection, Speed Limit for Source, and Speed Limit for Destination. You can create an anti-DDoS protection policy for a specific port forwarding rule. This is applicable after you create port forwarding rules for an Anti-DDoS Pro or Anti-DDoS Premium instance and associate a non-website service with the instance. You can also create anti-DDoS protection policies for multiple port forwarding rules at a time.

#### Prerequisites

A port forwarding rule for a non-website service is configured on the Port Config page. For more information, see [Create forwarding rules](#).

#### Context

**Notice:**

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

For non-website services, anti-DDoS protection policies are configured based on IP addresses and ports. To mitigate connection-oriented DDoS attacks, you can set the request rate, packet length, and other parameters as required. Anti-DDoS protection settings only apply to ports.

Both Anti-DDoS Pro and Anti-DDoS Premium allow you to create the following types of anti-DDoS protection policies for non-website services:

- **False Source:** verifies and filters DDoS attacks initiated from forged IP addresses.
- **Speed Limit for Destination:** The data transfer rate of the port that exceeds the maximum visit frequency is limited based on the IP address and port of your Anti-DDoS Pro or Anti-DDoS Premium instance. The data transfer rates of other ports are not limited.
- **Packet Length Limit:** specifies the minimum and maximum lengths of packets that are allowed to pass through. Packets with invalid lengths are dropped.
- **Speed Limit for Source:** The data transfer rate of a source IP address that exceeds the maximum visit frequency is limited based on the IP address and port of your Anti-DDoS Pro or Anti-DDoS Premium instance. The data transfer rates of other source IP addresses are not limited. This policy also supports the IP address blacklist policy. An IP address from which access requests exceed the maximum visit frequency five times within 60 seconds can be added to a blacklist. You can also specify the blocking period.

### Create an anti-DDoS protection policy

The following procedure shows how to create an anti-DDoS protection policy for a specific port forwarding rule. You can also create anti-DDoS protection policies for multiple port forwarding rules at a time. For more information, see [Create anti-DDoS protection policies for multiple port forwarding rules at a time](#).

1. Log on to the [Anti-DDoS Pro console](#).

2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > General Policies**.
4. On the **General Policies** page, click the **Protection for Non-website Services** tab. On the tab that appears, select the target instance from the Select Instance drop-down list.
5. Select the forwarding rule for which you want to create a policy from the list on the left side.

The screenshot shows the 'Protection Policies' page for 'Protection for Non-website Services'. At the top, there's a navigation bar with 'Protection Policies', a welcome message, and links for 'Product Updates' and 'Buy Instance'. Below this, there are three tabs: 'Protection for Infrastructure', 'Protection for Website Services', and 'Protection for Non-website Services'. The 'Select Instance' dropdown is set to '203.132'. The main content area is titled 'Intelligent protection' and describes Layer-4 AI-powered protection. Below this, there's a 'Forwarding Port' list on the left with four entries. The entry 'Forwarding Port: 234' is selected and highlighted with a red box. To the right of the list are three configuration panels: 'False Source' (with 'False Source' and 'Empty Connection' toggles), 'Packet Length Limit' (showing a range of 8 to 6000 bytes), and 'Speed Limit for Destination' (showing a rate limit of 100000). There is also a 'Speed Limit for Source' panel at the bottom right.

Protection Policies The new version of the protection strategy is open, welcome to experience Details>> Product Updates Buy Instance

Protection for Infrastructure Protection for Website Services Protection for Non-website Services

Select Instance 203.132

**Intelligent protection**

Layer-4 AI-powered intelligent protection: The intelligent analysis engine for big data helps you identify and block CC attacks of the SYN flood type. This is achieved through adaptive learning about the number of baseline connections to an Anti-DDoS Pro IP address. It provides an efficient defense against SYN flood attacks. The Protection mode is set to Normal and enabled by default.

Protection Enabled Modify

**Forwarding Port**

Forwarding Port	Origin Server Port	Protocol	Action
Forwarding Port: 80	Origin Server Port: 80	tcp	Forwarding
Forwarding Port: 443	Origin Server Port: 443	tcp	Forwarding
Forwarding Port: 234	Origin Server Port: 456	tcp	Forwarding
Forwarding Port: 345	Origin Server Port: 222	tcp	Forwarding

**False Source**

Screen DDoS attacks from fake IP addresses

False Source ☒ Empty Connection ☐

**Packet Length Limit**

Packets whose length is smaller than the minimum length or larger than the maximum length are discarded.

The length of the packet exceeds 8 - 6000 specified byte range, the packet will be dropped

**Speed Limit for Destination**

When the request frequency per second exceeds the specified threshold, Anti-DDoS Pro performs throttling on the port of an Anti-DDoS IP address. This configuration is based on and only applied to the specified Anti-DDoS IP address and port. Other ports are unaffected.


Destination New Connection Rate Limit: 100000 Destination Concurrent Connection Rate Limit: Disabled


**Speed Limit for Source**

When the request frequency per second exceeds the specified threshold, Anti-DDoS Pro performs throttling on the port of an Anti-DDoS IP address. This configuration is based on and only applied to the specified Anti-DDoS IP address and port. Other ports are unaffected.

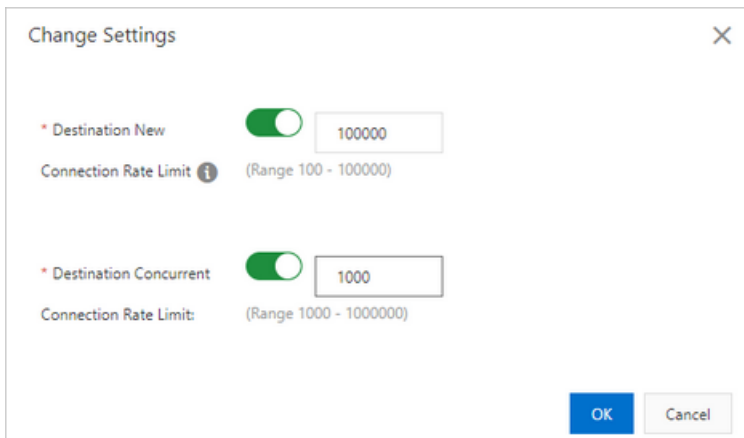
6. Configure settings in the **False Source**, **Speed Limit for Destination**, **Packet Length Limit**, and **Speed Limit for Source** sections.

- **False Source:** In the **False Source** section, turn on or off **False Source** or **Empty Connection**.


Description	
<p><b>False Source</b> on this switch to block requests from forged IP addresses. After you turn on the switch, Anti-DDoS Pro or Anti-DDoS Premium automatically filters requests initiated from forged IP addresses.</p> <div> <b>Note:</b> This policy only applies to TCP rules.</div>	

Description	
<p><b>Empty Connection</b> Turn on this switch to filter requests that attempt to establish null sessions. After you turn on the switch, Anti-DDoS Pro or Anti-DDoS Premium automatically filters requests that attempt to establish null sessions.</p> <div data-bbox="323 701 636 1028"> <b>Note:</b> This policy only applies to TCP rules. To enable this policy, you must first enable the False Source policy.</div>	

- **Speed Limit for Destination:** In the **Speed Limit for Destination** section, click **Change Settings**. In the **Change Settings** dialog box, specify the required parameters and then click **OK**.

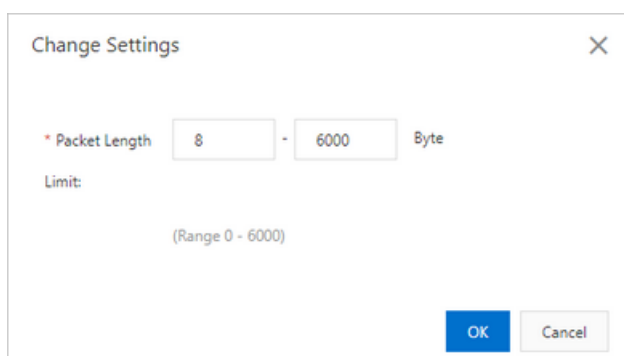


The 'Change Settings' dialog box contains two sections for configuring connection rate limits. The first section, 'Destination New', has a toggle switch turned on and a text box with the value '100000'. Below it, the text 'Connection Rate Limit' is followed by a range '(Range 100 - 100000)'. The second section, 'Destination Concurrent', also has a toggle switch turned on and a text box with the value '1000'. Below it, the text 'Connection Rate Limit' is followed by a range '(Range 1000 - 1000000)'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Description	
<p><b>Destination New Connection Rate Limit</b> meter specifies the maximum number of new connections per second that can be established on an Anti-DDoS Pro or Anti-DDoS Premium port. The value ranges from 100 to 100000. Requests sent to the port after the upper limit is reached are dropped.</p> <div data-bbox="320 824 639 1193"><b>Note:</b> The limit on new connections may be slightly different from actual scenarios because scrubbing nodes are deployed in clusters.</div>	

Description	
<p><b>Destination Connection Rate Limit</b></p> <p>Destination Connection Rate Limit specifies the maximum number of concurrent connections that can be established on an Anti-DDoS Pro or Anti-DDoS Premium port. The value ranges from 1000 to 1000000. Requests sent to the port after the upper limit is reached are dropped.</p>	

- **Packet Length Limit:** In the **Packet Length Limit** section, click **Change Settings**. In the **Change Settings** dialog box, set the minimum and maximum lengths of the payload contained in a packet and then click **OK**. The value ranges from 0 to 6000. Unit: bytes.



The image shows a 'Change Settings' dialog box with a close button (X) in the top right corner. Inside the dialog, there is a label '\* Packet Length' followed by two input fields: the first contains '8' and the second contains '6000', separated by a hyphen. To the right of these fields is the text 'Byte'. Below this, the word 'Limit:' is displayed. At the bottom of the dialog, there is a note '(Range 0 - 6000)' and two buttons: 'OK' (in blue) and 'Cancel' (in grey).

- **Speed Limit for Source:** In the **Speed Limit for Source** section, click **Change Settings**. In the **Configure Speed Limit for Source** pane, specify the required parameters and then click **OK**.



Configure Speed Limit for Source

\* Source New Connection

☒ Automatic ☐ Manual ☐ Close

Rate Limit ⓘ:

When the number of new connections reaches , the speed is limited.

(Range 1 - 50000)

☐ When the number of new connections from a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.

\* Source Concurrent

☒

Connection Rate Limit:

☒

\* PPS Limit for Source

☒

\* Bandwidth Limit for Source


☒

OK

Cancel

Issue: 20200529

219

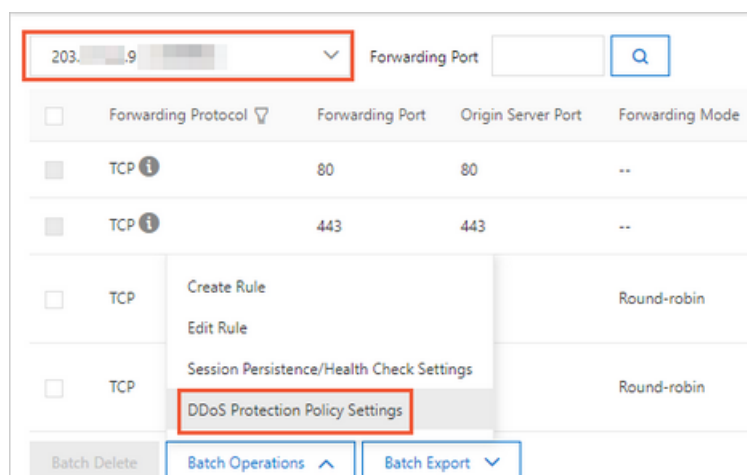
Parameter	Description
<b>Source New Connection Rate Limit</b>	<p>This parameter specifies the maximum number of new connections per second that can be initiated from a single IP address. The value ranges from 1 to 50000. Requests initiated from the IP address after the upper limit is reached are dropped. This policy supports <b>Automatic</b> and <b>Manual</b> modes.</p> <ul style="list-style-type: none"> <li>- If you select Automatic, Anti-DDoS Pro or Anti-DDoS Premium dynamically calculates the maximum number of new connections per second that can be initiated from a single source IP address.</li> <li>- If you select Manual, you need to manually specify the maximum number of new connections per second that can be initiated from a single source IP address.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;">  <b>Note:</b>  The limit on new connections may be slightly different from actual scenarios because scrubbing nodes are deployed in clusters. </div> <p>Blacklist policy</p> <ul style="list-style-type: none"> <li>- If you select the <b>When the number of new connections from a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.</b> check box, all requests from IP addresses in the blacklist are dropped.</li> <li>- To enable the blacklist policy, you must set <b>Validity Period for Blacklist</b>. The value ranges from 1 to 10080. The default value is 30. Unit: minutes. An IP address added to a blacklist is removed from the blacklist when the validity period ends.</li> </ul>

Parameter	Description
<b>Source Concurrent Connection Rate Limit</b>	<p>This parameter specifies the maximum number of concurrent connections that can be initiated from a single IP address. The value ranges from 1 to 50000. Requests initiated from the IP address after the upper limit is reached are dropped.</p> <p>Blacklist policy</p> <ul style="list-style-type: none"> <li>- If you select the <b>When the number of concurrent connections from a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.</b> check box, all requests from IP addresses in the blacklist are dropped.</li> <li>- To enable the blacklist policy, you must set <b>Validity Period for Blacklist.</b> The value ranges from 1 to 10080. The default value is 30. Unit: minutes. An IP address added to a blacklist is removed from the blacklist when the validity period ends.</li> </ul>
<b>PPS Limit for Source</b>	<p>This parameter specifies the maximum number of packets per second that can be allowed from a single IP address. The value ranges from 1 to 100000. Unit: packet/s. Packets initiated from the IP address after the upper limit is reached are dropped.</p> <p>Blacklist policy</p> <ul style="list-style-type: none"> <li>- If you select the <b>When the source packets per second (PPS) of a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.</b> check box, all requests from IP addresses in the blacklist are dropped.</li> <li>- To enable the blacklist policy, you must set <b>Validity Period for Blacklist.</b> The value ranges from 1 to 10080. The default value is 30. Unit: minutes. An IP address added to a blacklist is removed from the blacklist when the validity period ends.</li> </ul>

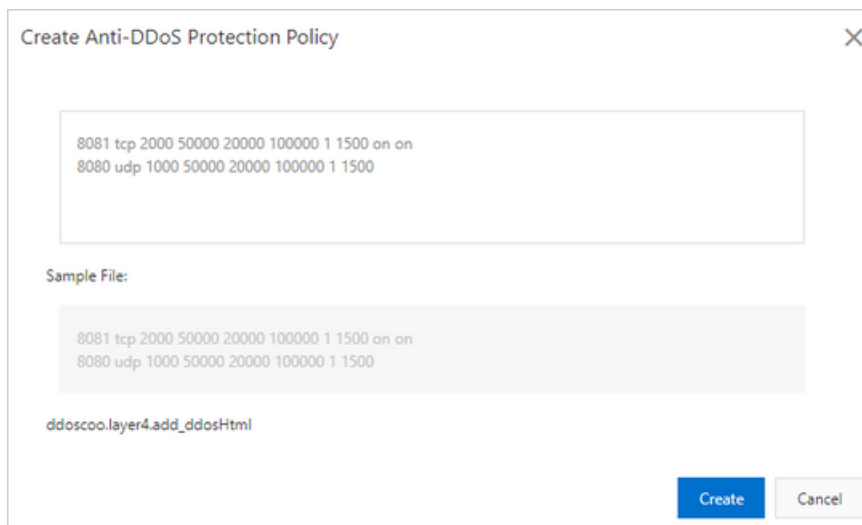
Parameter	Description
<b>Bandwidth Limit for Source</b>	<p>This parameter specifies the maximum bandwidth of a single IP address. The value ranges from 1024 to 268435456. Unit: bytes/s.</p> <p>Blacklist policy</p> <ul style="list-style-type: none"> <li>- If you select the <b>When the source bandwidth of a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.</b> check box, all requests from IP addresses in the blacklist are dropped.</li> <li>- To enable the blacklist policy, you must set <b>Validity Period for Blacklist.</b> The value ranges from 1 to 10080. The default value is 30. Unit: minutes. An IP address added to a blacklist is removed from the blacklist when the validity period ends.</li> </ul>

### Create anti-DDoS protection policies for multiple port forwarding rules at a time

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.
4. On the **Port Config** page, select the target instance, click **Batch Operations** below the rule list, and select **DDoS Protection Policy Settings**.



5. In the **Create Anti-DDoS Protection Policy** dialog box, follow the required formats to enter the content of anti-DDoS protection policies and then click **Create**.



Create Anti-DDoS Protection Policy

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

Sample File:

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

ddoscoo.layer4.add\_ddosHtml

Create Cancel

The following section describes the formats of anti-DDoS protection policies.



**Note:**

You can also export anti-DDoS protection policies to a TXT file, modify the content in the TXT file, and then copy and paste the modified content to the target fields. The formats of anti-DDoS protection policies in the exported file must be the same as those of the policies that you want to create. For more information, see [Export multiple port configurations](#).

- Enter one policy in each row.
- Each anti-DDoS protection policy must contain the following fields from left to right: forwarding port, forwarding protocol, source new connection rate limit, source concurrent connection rate limit, destination new connection rate limit, destination concurrent connection rate limit, minimum packet length, maximum packet length, false source status, and empty connection status. The forwarding protocol can be TCP or UDP. For more information about the fields and valid values, see [Parameters and descriptions of anti-DDoS protection policies](#). Fields are separated with spaces.
- The forwarding port must be a port specified in a forwarding rule.
- The valid values of both False Source and Empty Connection are on and off. If any of these parameters is not set, the switch is turned off.

### 9.3.3 Configure the speed limit for source IP addresses

This topic describes how to configure and use the Speed Limit for Source policy. This policy allows you to set the maximum visit frequency and traffic volume from specific source IP

addresses. If this policy is enabled, Anti-DDoS Pro or Anti-DDoS Premium adds IP addresses that exceed the maximum visit frequency or traffic volume to the blacklist or limits the data transfer rates from the IP addresses. After a source IP address is added to a blacklist, all requests from this IP address are dropped.

### Prerequisites

A port forwarding rule for a non-website service is configured on the Port Config page. For more information, see [Create forwarding rules](#).

### Context

Both Anti-DDoS Pro and Anti-DDoS Premium allow you to set the maximum visit frequency from a source IP address to the port of your instance by limiting the numbers of new connections and concurrent connections. You can also limit the traffic volume to the port by limiting the bandwidth (bit/s) and packets per second (pps) of the source IP address. If an IP address exceeds the maximum visit frequency or traffic volume, Anti-DDoS Pro or Anti-DDoS Premium adds it to the blacklist or limits the data transfer rates. This policy can be used to block Layer 4 HTTP flood attacks that create a large number of connections. It can directly block the source IP addresses of attacks.

For example, assume that a source IP address accesses port 8000 of your instance, and the number of new connections is more than 10 times the normal level. You can set Source New Connection Rate Limit and enable the blacklist policy for port 8000. If the number of new connections from a source IP address repeatedly exceeds the limit, the IP address is added to the blacklist, and requests from this IP address are dropped.



#### Note:

The Speed Limit for Source policy takes effect on Anti-DDoS Pro or Anti-DDoS Premium ports. You must enable this policy for different Anti-DDoS Premium or Anti-DDoS Pro ports separately.

### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Provisioning > Port Config**.
4. On the **Port Config** page, select the target instance.

5. Find the target forwarding rule and click **Change** in the **Anti-DDoS Protection Policy** column.

203.132.132.132	Forwarding Port									You can create a maximum of 50 rules. You have already created 8 rules.	Create Rule
<input type="checkbox"/>	Forwarding Protocol	Forwarding Port	Origin Server Port	Forwarding Mode	Origin Server IP	Session Persistence	Health Check	Anti-DDoS Protection Policy	Actions		
<input type="checkbox"/>	TCP	80	80	--	--	--	--	--	--		
<input type="checkbox"/>	TCP	443	443	--	--	--	--	--	--		
<input type="checkbox"/>	TCP	234	456	Round-robin	2.2	Disabled Change	Disabled Change	Enabled Change	Edit Delete		

6. In the **Speed Limit for Source** section, click **Change Settings**.

### Speed Limit for Source

When the request frequency per second exceeds the specified threshold, Anti-DDoS Pro performs throttling on the port of an Anti-DDoS IP address. This configuration is based on and only applied to the specified Anti-DDoS IP address and port. Other ports are unaffected.

[Change Settings](#)

7. In the **Configure Speed Limit for Source** pane, specify the required parameters.

In this example, after the settings take effect, the number of concurrent connections from a source IP address cannot exceed 50,000 per second. If this threshold is reached, the data transfer rate of the IP address is limited. If you select the **When the number of concurrent connections from a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.** check box, your instance collects the number of times when the number of concurrent connections

from a source IP address exceeds the threshold. If the number of times exceeds five, this IP address is added to the blacklist, and all requests from this IP address are dropped.

Configure Speed Limit for Source

\* Source New Connection ☐ Automatic ☐ Manual ☒ Close

Rate Limit ⓘ:

\* Source Concurrent ☒

Connection Rate Limit:

When the number of concurrent connections reaches  the speed is limited.

(Range 1- 50000)

☐ When the number of concurrent connections from a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.

\* PPS Limit for Source ☐

\* Bandwidth Limit for Source ☐

Source New Connection Rate Limit, PPS Limit for Source, and Bandwidth Limit for Source function the same way as Source Concurrent Connection Rate Limit. For more information, see [Create an anti-DDoS protection policy](#).

8. Click **OK** to apply the settings.

## 9.4 Configure static page caching

Integrated with web caching techniques, Anti-DDoS Pro and Anti-DDoS Premium provide scrubbing centers to protect your website services against DDoS attacks and reduce page load time.

### Prerequisites

Your website service is associated with an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the enhanced function plan.

### Context



#### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches

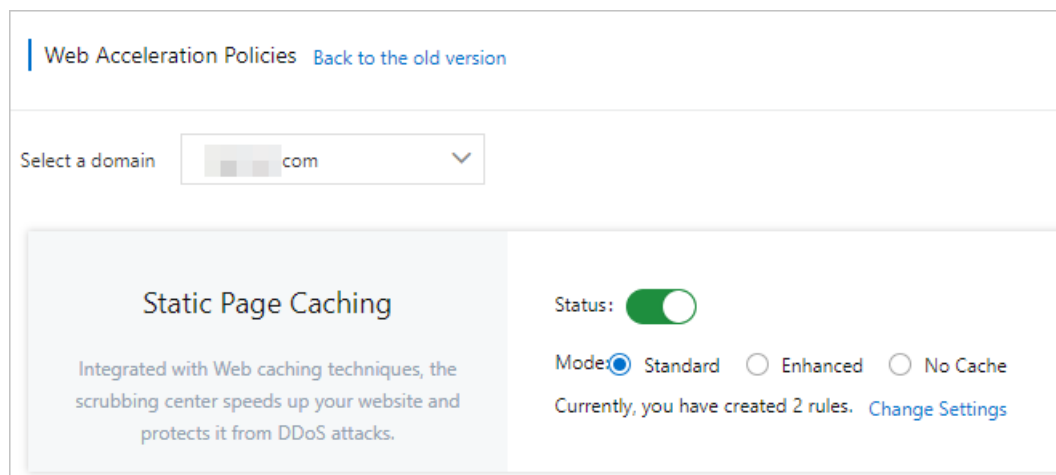


between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

You can use the Static Page Caching policy to accelerate requests to your website and configure custom rules to reduce the load time of specific pages.

#### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Anti-DDoS Lab > Web Acceleration**.
4. Select the domain name for which you want to configure the Static Page Caching policy.
5. In the **Static Page Caching** section, set **Mode** and turn on **Status**.



Static Page Caching supports the following modes: Standard, Enhanced, and No Cache.

- **Standard:** In this mode, the system attempts to cache requested pages that contain static resources, such as CSS, JS, and TXT files, on a website.
- **Enhanced:** In this mode, the system attempts to cache any requested page on a website.
- **No Cache:** In this mode, the system does not cache any requested page on a website.

## 6. Configure a custom caching rule for a specific URI.

- a) In the **Static Page Caching** section, click **Change Settings**.
- b) Click **Create Rule**.

Domain:  .com [Back](#)

Static Page Caching Custom Rules Currently, 2 rules have been created. You can create 1 more rules. [Create Rule](#)

Name	URI	Mode	Cache Expires In	Actions
asdf	/gasd	Enhanced	10 Days	<a href="#">Edit</a> <a href="#">Delete</a>
hehe	/alfjda.php	No Cache	1 Days	<a href="#">Edit</a> <a href="#">Delete</a>

- c) In the **Create Rule** dialog box, set **Name**, **URI**, **Mode**, and Cache Expires In.

Create Rule ✕

\* Name:  Enter a maximum of 128 characters that can be letters, numbers, and

\* URI:  For example: /abc/a.php

\* Mode: ☒ Standard ☐ Enhanced ☐ No Cache

\* Cache Expires In:  Use Origin Server Settings ▼

[OK](#) [Cancel](#)



### Note:

Do not enter parameters or wildcard characters in the **URI** field. For example, /a/ represents all pages under path `www.a.com/a/`.

- d) Click **OK**.

## 9.5 Create custom policies for specific scenarios

Both Anti-DDoS Pro and Anti-DDoS Premium allow you to create scenario-specific custom policies. A scenario-specific custom policy allows you to choose a scenario-specific template for high-traffic scenarios, such as new business launches and Double 11. You can create custom policies based on your business needs.

### Context



### Notice:

In the top navigation bar of the Anti-DDoS Pro or Anti-DDoS Premium console, you can switch the region (**Mainland China** and **Outside Mainland China**), and the system switches between Anti-DDoS Pro and Anti-DDoS Premium accordingly for you to manage and configure Anti-DDoS Pro or Premium instances. Ensure that you switch to the required region when you use Anti-DDoS Pro or Anti-DDoS Premium.

Scenario-specific templates are available when you create a custom policy. When you create a custom policy, you must select a template and specify a target to apply the policy. Currently, the target must be a domain name. A custom policy is valid only during the specified validity period. During the validity period, the custom policy takes precedence over standard protection policies.

**Notice:**

- If no traffic surge happens, we recommend that you use standard protection policies instead of custom policies.
- Custom policies are available only for the latest versions of Anti-DDoS Pro and Anti-DDoS Premium. If you want to create custom policies, we recommend that you update to the latest version of Anti-DDoS Pro or Anti-DDoS Premium.

**Policy Template**

Only the **Important Activity** template is available. We are working on support for more policy templates.

**Example**

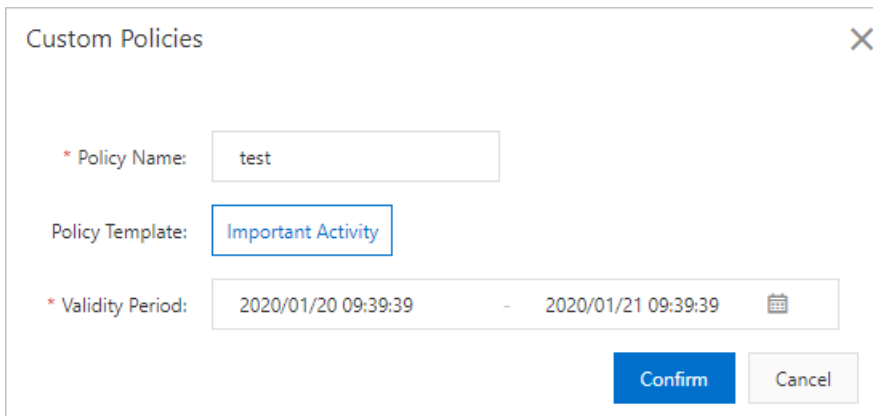
If a major activity is held on a website, a large number of requests are sent to visit the website. As a result, the throughput performance will vary. In this case, if you use the anti-DDoS protection policy of the normal level, false positives may occur. We recommend that you configure the **Important Activity** policy on the **Custom Policies** page. The Important Activity policy automatically adjusts the anti-DDoS protection policies during the specified period. Anti-DDoS protection policies are adjusted based on the following rules:

- At the beginning of an activity, the Important Activity policy records the status of the **Intelligent Protection** and **Frequency Control** policies and automatically disables them to avoid false positives.
- At the end of the activity, the Important Activity policy restores the configurations of these policies.

- If you enable these policies during an activity, the manual configuration takes precedence.

#### Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. In the top navigation bar, select the region of your Anti-DDoS instance.
  - **Mainland China:** Anti-DDoS Pro
  - **Outside Mainland China:** Anti-DDoS Premium
3. In the left-side navigation pane, choose **Mitigation Settings > Custom Policies**.
4. On the Custom Policies page, click **Create Policy**.
5. In the **Custom Policies** dialog box, specify the required parameters and then click **Confirm**.



Custom Policies


\* Policy Name: test

Policy Template: Important Activity

\* Validity Period: 2020/01/20 09:39:39 - 2020/01/21 09:39:39

Confirm Cancel



Parameter	Description
Policy Name	The name of the policy.
Policy Template	The template that you want to apply to the policy. Set the value to <b>Important Activity</b> .

Parameter	Description
<b>Validity Period</b>	<p>The validity period of the policy.</p> <div>  <b>Note:</b>            The validity periods of policies to which the same policy template is attached must not overlap.         </div>

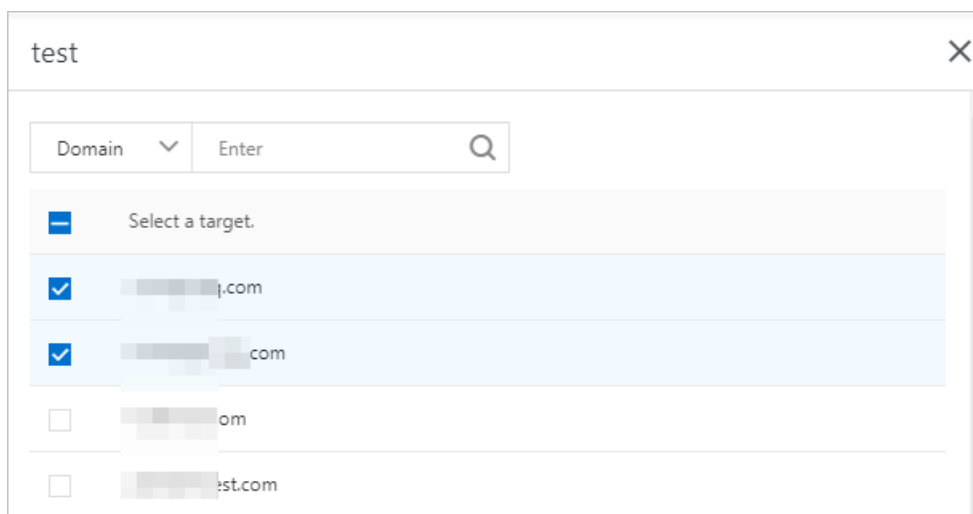
After a policy is created, the policy is automatically applied. You can view the policy on the Custom Policies page and check **Status** of the policy to determine whether the policy takes effect. Different states are described as follows:

- **Pending Enabled:** indicates that a policy is pending enabled. The current time is earlier than the start time of the specified validity period.
- **Updating:** indicates that a policy is expected to take effect. The process requires one or two minutes to complete.
- **Running:** indicates that a policy is valid. The current time is within the specified validity period.
- **Expired:** indicates that a policy has expired. The current time is not within the specified validity period.
- **Disabled:** indicates that a policy is disabled. The policy does not take effect even if the current time is within the specified validity period.

6. In the custom policy list, find the new policy and click **Configure Policy** in the Actions column.

Custom Policies <a href="#">Back to the old version</a>					
<div>  You can create custom policies to ensure effective protection for specific scenarios, such as big promotions and new game releases.           <span>×</span> </div>					
					<a href="#">Create Policy</a> 
Policy Name	Policy Template ▾	Validity Period	Status ▾	Protection Target	Actions
test	Important Activity	Apr 2, 2020, 00:00:00 - Apr 3, 2020, 00:00:00	<span style="color: blue;">●</span> Pending enabled	0.	<a href="#">Configure Policy</a> <a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Disable</a>

7. In the list of domain names that are protected by Anti-DDoS Pro or Anti-DDoS Premium, select one or more domain names to which you want to apply the policy and click **OK**.



After a policy is applied, the information in the **Protection Target** column is automatically updated. You can move the pointer over the protection target to view the domain name to which the policy is applied.

Policy Name	Policy Template ▾	Validity Period	Status ▾	Protection Target	Actions
test	Important Activity	Apr 2, 2020, 00:00:00 - Apr 3, 2020, 00:00:00	● Pending enabled	2. [redacted].com [redacted].com	<a href="#">View Policy</a>   <a href="#">Edit</a>   <a href="#">Delete</a>

## What's next

You can enable, disable, edit, or delete custom policies on the **Custom Policies** page based on your business needs.

# 10 Query and analysis

---

## 10.1 Full log

The access log provided by Anti-DDoS Pro is integrated with Alibaba Cloud Log Service to provide real-time analysis and reporting features. The access log contains log entries of HTTP flood attacks. The full log service is a value-added service. You must make a purchase to use it. After you activate the full log service, Log Service starts to collect access logs and attack logs in real time. You can query and analyze log data collected by Anti-DDoS Pro, and the results are displayed on dashboards.

### Context

The [APNIC DDoS threat landscape in 2017](#) states that more than 80% of DDoS attacks are combined with HTTP flood attacks, which can be difficult to detect. Therefore, it is important to analyze access logs in real time to identify attack behaviors and apply a suitable protection policy at the earliest opportunity.

The full log service is integrated with Log Service. You can query and analyze log data on dashboards. This helps you flexibly analyze and monitor your website services. After you activate full log, you can consume and ship logs through Log Service. This helps you manage website access logs collected by Anti-DDoS Pro.

Log Service is an all-in-one logging service developed by Alibaba Cloud. It has been tested in a wide array of big data scenarios. Log Service helps you quickly collect, consume, ship, query, and analyze log data without development work. It improves the O&M and operations efficiency, and provides the capability to process large volumes of data. For more information, see [What is Log Service](#).

### Activate the full log service

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose **Statistics > Full Log**.
3. On the **Log Service** page, click **Buy Now**.

4. On the [buy page of Log Service](#), set **Applicable Product** to **Anti-DDoS Pro**, and select the specification as needed.

- **Log Storage:** the log storage capacity. Unit: TB. After the log storage capacity is exhausted, new logs cannot be stored. We recommend that you monitor the remaining log storage space and expand the storage space as needed.
- **Duration:** the validity period of the full log service. After the full log service expires, new logs cannot be stored. If you do not renew the full log service within seven days after it expires, all log data will be automatically deleted.

The full log service is charged at a price rate of RMB 500/TB (log storage space)/month (service duration).



**Note:**

If the full log service has sufficient storage capacity within the validity period, it stores logs of the last 180 days. Logs from day 181 will overwrite the logs from day 1. Full log stores logs in the last 180 days only.

Example of how to select a log storage capacity

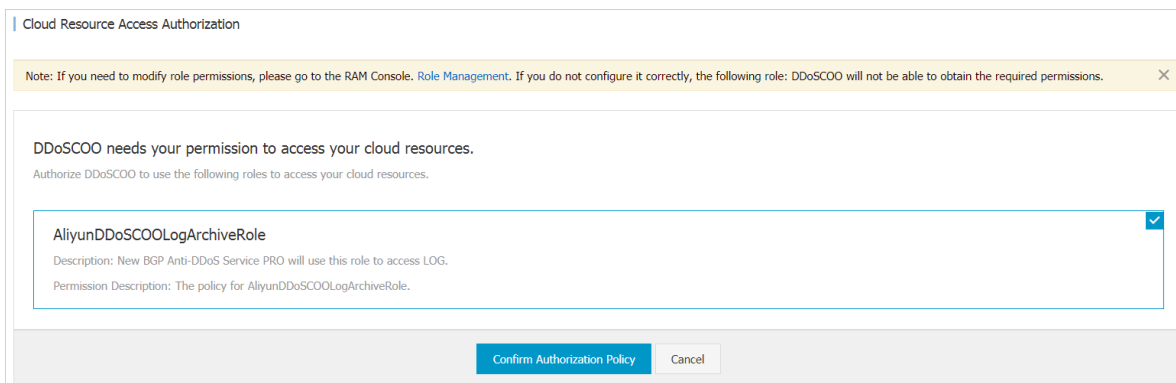
Typically, each request log occupies about 2 KB of storage space. If the average request volume of your workload is 500 queries per second (QPS), the storage space required for one day is:  $500 \times 60 \times 60 \times 24 \times 2 = 86,400,000$  KB (82 GB). By default, full log stores logs in the last 180 days. Therefore, you need to select a log storage capacity of 14,832 GB (14.5 TB).

5. Click **Buy Now** and settle the payment.

6. In the Anti-DDoS Pro console, navigate to the **Log Service** page and click **Authorize Now**.



7. On the **Cloud Resource Access Authorization** page, click **Authorize** to authorize Anti-DDoS Pro to store logs to the specified Logstore.



After the full log service is activated, you can go to the **Log Service** page and click **Details** to view the service specification.

**Note:**

We recommend that you pay close attention to the remaining log storage space and validity period during use.

- When the utilization of the log storage capacity reaches 70%, expand the log storage capacity to make sure that new logs can be stored.
- If a large amount of storage space remains unused for a long time, reduce the storage capacity as needed.

**Activate full log for a website**

1. Log on to the [Anti-DDoS Pro console](#).
2. In the left-side navigation pane, choose **Statistics > Full Log**.
3. On the **Log Service** page, select the target website domain, and turn on the Status switch to enable full log.

After you enable full log, you can query and analyze the collected logs in real time, view and edit dashboards, and set monitoring alerts on the **Log Service** page.

For more information about the analysis and reporting features, see [#unique\\_99](#) and [#unique\\_100](#).

**Use full log**

The full log service is integrated with Alibaba Cloud Log Service. After you enable this service, you can analyze access logs, attack logs, and defense logs collected by Log Service. You can also display data on dashboards, and set monitoring alerts by using thresholds.

Feature	Description	Reference
Query and analysis	<p>You can query and analyze collected log data in real time. A query consists of Search statements and Analytics statements. Separate Search and Analytics statements with vertical bars ( ).</p> <p>For example, the following Search statement is used to query the number of visits to a website.</p> <pre>*   SELECT COUNT(*) as times, host GROUP by host ORDER by times desc limit 100</pre> <p>For more sample statements, see the following section describing commonly used Search statements.</p>	<a href="#">Query and analysis</a>
Graphs	Search statements contain analytics syntax. After Search statements are executed, analysis results are displayed in charts by default. You can choose a line chart, bar chart, pie chart, and other types of charts.	<a href="#">Graphs</a>
Dashboards	<p>Analysis results are displayed on dashboards in real time. You can execute Search statements to display data in charts. Charts can be saved to dashboards.</p> <p>Full log provides two default dashboards: access center and operations center.</p> <p>You can also subscribe to dashboards, or sent dashboards to specific recipients through emails or DingTalk messages.</p>	<a href="#">Dashboards</a>
Monitoring and alerts	You can configure alerts based on the charts on a dashboard to monitor the service status in real time.	<a href="#">Alerts</a>

## Scenarios

The full log service is suitable for the following scenarios.

- Troubleshoot website access problems

After full log is enabled for your website, you can query and analyze the logs collected from your website in real time. You can use SQL statements to analyze the access log of your website. This allows you to quickly troubleshoot and analyze access problems, and view information about read/write latency and the distribution of ISPs.

For example, the following statement can be used to view access logs on your website:

```
__topic__: DDoS_access_log
```

- Track HTTP flood attack sources

Access logs record information about the sources and distribution of HTTP flood attacks. You can query and analyze access logs in real time to identify the origins of attacks, and use this information to select the most effective protection strategy.

- For example, the following statement can be used to analyze the geographical distribution of HTTP flood attacks:

```
__topic__: DDoS_access_log and cc_blocks > 0 | SELECT ip_to_country(if(real_client_ip = '-', remote_addr, real_client_ip)) as country, count(1) as "number of attacks" group by country
```

- For example, the following statement can be used to view PVs:

```
__topic__: DDoS_access_log | select count(1) as PV
```

- Analyze website operations

Access logs record information about website traffic in real time. You can use SQL queries to analyze log data and better understand your users. For example, you can identify the most visited web pages, the source IP addresses of the clients, the browsers that initiated the requests, and the distribution of client devices, which can help you analyze website operations.

For example, the following statement can be used to view the distribution of traffic by ISP:

```
__topic__: DDoS_access_log | select ip_to_provider(if(real_client_ip = '-', remote_addr, real_client_ip)) as provider, round(sum(request_length)/1024.0/1024.0, 3) as mb_in group by provider having ip_to_provider(if(real_client_ip = '-', remote_addr, real_client_ip)) <> " order by mb_in desc limit 10
```

## Commonly used Search statements

- Query types of blocked requests

```
* | select cc_action,cc_phase,count(*) as t group by cc_action,cc_phase order by t desc limit 10
```

- Query the number of queries per second

```
* | select time_series(__time__,'15m','%H:%i','0') as time,count(*)/900 as QPS group by time order by time
```

- Query attacked domains

```
* and cc_blocks:1 | select cc_action,cc_phase,count(*) as t group by cc_action,cc_phase order by t desc limit 10
```

- Query attacked URLs

```
* and cc_blocks:1 | select count(*) as times,host,request_path group by host,request_path order by times
```

- Query request details

```
* | select date_format(date_trunc('second',__time__),'%H:%i:%s') as time,host,request_uri,request_method,status,upstream_status,querystring limit 10
```

- Query 5XX HTTP status codes

```
* and status>499 | select host,status,upstream_status,count(*) as t group by host,status,upstream_status order by t desc
```

- Query the distribution of request latency

```
* | SELECT count_if(upstream_response_time<20) as "<20",  
count_if(upstream_response_time<50 and upstream_response_time>20) as "<50",  
count_if(upstream_response_time<100 and upstream_response_time>50) as "<100",  
count_if(upstream_response_time<500 and upstream_response_time>100) as "<500",  
count_if(upstream_response_time<1000 and upstream_response_time>500) as "<1000",  
count_if(upstream_response_time>1000) as ">1000"
```

## Related topics

- [Fields supported by full log](#)
- [Search syntax](#)
- [SQL query syntax](#)



## 10.2 Fields supported by full log








Anti-DDoS Pro provides the full log feature that supports a wide array of fields.

You can query and analyze collected logs in real time on the **Full Log** page. The following table describes the fields supported by full log.

Field	Description	Example
__topic__	The topic of the log entry. The value of this field is fixed to ddos_access_log.	-
body_bytes_sent	The size of the body in the access request. The body is measured in bytes.	2
content_type	The type of the content.	application/x-www-form-urlencoded
host	The source website.	api.abc.com
http_cookie	The request cookie.	k1=v1;k2=v2
http_referer	The request referer. If no referer exists, a hyphen (-) is displayed.	http://xyz.com
http_user_agent	The User-Agent of the request.	Dalvik/2.1.0 (Linux; U; Android 7.0; EDI-AL10 Build/HUAWEIEDISON-AL10)
http_x_forwarded_for	The IP address of the upstream user redirected by a proxy.	-
https	Indicates whether the request is an HTTPS request. <ul style="list-style-type: none"><li>true: The request is an HTTPS request.</li><li>false: The request is an HTTP request.</li></ul>	true
matched_host	The matching origin site, which may be a wildcard domain name. If no match is found, a hyphen (-) is displayed.	*.zhihu.com

Field	Description	Example
real_client_ip	The real IP address of the visitor. If the real IP address cannot be obtained, a hyphen (-) is returned.	1.2.3.4
isp_line	The information about the ISP line, such as BGP, China Telecom, and China Unicom.	China Telecom
remote_addr	The IP address of the client that initiates the connection request.	1.2.3.4
remote_port	The port number of the client that initiates the connection request.	23713
request_length	The size of the request, which is measured in bytes.	123
request_method	The HTTP method of the request.	GET
request_time_msec	The processing time of the request. The time is measured in milliseconds.	44
request_uri	The request URI.	/answers/377971214/ banner
server_name	The name of the matching host. If no match is found, the value is default.	api.abc.com
status	The HTTP status code.	200
time	The time when the log entry is generated.	2018-05-02T16:03:59+08:00
cc_action	The anti-HTTP flood protection action. Valid values include none, challenge, pass, close, captcha, wait, and login.	close

Field	Description	Example
cc_blocks	<p>Indicates whether the request is blocked by anti-HTTP flood protection.</p> <ul style="list-style-type: none"> <li>1: The request is blocked.</li> <li>Other values: The request is allowed.</li> </ul> <div>  <b>Note:</b>            In some cases, log entries may not contain this field. The last_result field is used instead to record whether a request is blocked by anti-HTTP flood protection.         </div>	1
last_result	<p>Indicates whether a request is blocked by anti-HTTP flood protection.</p> <ul style="list-style-type: none"> <li>ok: The request is allowed.</li> <li>failed: The request is blocked, or the verification fails.</li> </ul> <div>  <b>Note:</b>            In some cases, log entries may not contain this field. The cc_blocks field is used instead to record whether a request is blocked by anti-HTTP flood protection.         </div>	failed
cc_phase	The anti-HTTP flood protection policy. Valid values include seccookie, server_ip_blacklist, static_whitelist, server_header_blacklist, server_cookie_blacklist, server_arguments_blacklist, and qps_maximum.	server_ip_blacklist

Field	Description	Example
ua_browser	The browser.  <b>Note:</b> In some cases, log entries may not contain this field.	ie9
ua_browser_family	The browser series.  <b>Note:</b> In some cases, log entries may not contain this field.	internet explorer
ua_browser_type	The browser type.  <b>Note:</b> In some cases, log entries may not contain this field.	web_browser
ua_browser_version	The browser version.  <b>Note:</b> In some cases, log entries may not contain this field.	9.0
ua_device_type	The type of the client device.  <b>Note:</b> In some cases, log entries may not contain this field.	computer
ua_os	The operating system of the client.  <b>Note:</b> In some cases, log entries may not contain this field.	windows_7
ua_os_family	The operating system series of the client.  <b>Note:</b> In some cases, log entries may not contain this field.	windows



Field	Description	Example
upstream_addr	The list of origin addresses that are separated with commas (.). Each address follows the IP:Port format.	1.2.3.4:443
upstream_ip	The real origin IP address.	1.2.3.4
upstream_response_time	The response time of the back-to-origin process. The time is measured in seconds.	0.044
upstream_status	The HTTP status code of the back-to-origin request.	200
user_id	The ID of the Alibaba Cloud account.	12345678
querystring	The request string.	token=bbcd&abc=123

## 10.3 Operation logs

You can view records of operations in the last 30 days on the Operation Logs page in the Anti-DDoS Pro console.

**Note:**

Operation logs only record important operations in the last 30 days.

Recorded operation	Supported
Changes of ECS instance IP addresses	Yes
Deactivation of black holes	Yes
Blocking or unblocking traffic	Yes
Changes of scrubbing mode of Layer-4 traffic	Yes
Changes of HTTP flood protection modes	Yes
Changes of the burstable protection bandwidth	Yes

# 11 Best Practices

## 11.1 Create an Anti-DDoS Pro alert rule

This topic describes how to create Anti-DDoS Pro alert rules and add contact groups in the CloudMonitor console. Anti-DDoS Pro alert notifications provide you with up-to-date information about traffic and connection exceptions. You can troubleshoot errors and restore workloads as soon as possible.

### Context

CloudMonitor is a service that monitors applications and Alibaba Cloud resources. It sends you notifications when alerts are triggered. You can customize alert rules to specify how the alert system checks the monitoring data and when it sends alert notifications. After you set alert rules for important metrics, you are notified when exceptions are detected in these metrics. This enables you to manage exceptions quickly.

The alert feature provided by CloudMonitor is compatible with Anti-DDoS Pro. You can create and customize alert rules in the CloudMonitor console. CloudMonitor supports the following Anti-DDoS Pro metrics.



#### Note:

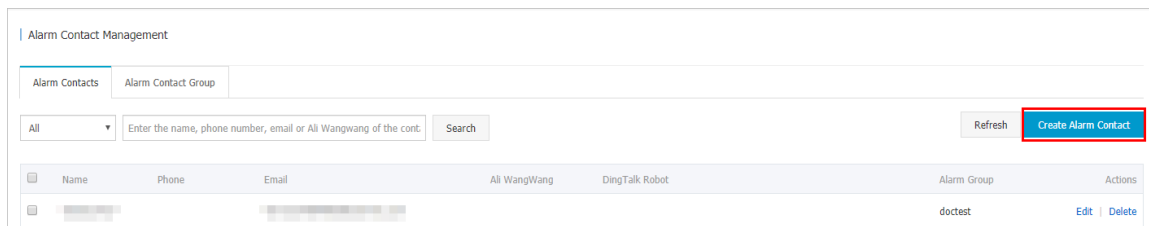
Anti-DDoS Pro back-to-origin traffic refers to the workload traffic that is scrubbed by Anti-DDoS Pro before it is forwarded to the origin server.

**Table 11-1: Anti-DDoS Pro metrics**

Metric	Dimension	Unit
Anti-DDoS Pro outbound traffic	Instance and IP address	bit/s
Anti-DDoS Pro inbound traffic	Instance and IP address	bit/s
Anti-DDoS Pro back-to-origin traffic	Instance and IP address	bit/s
Active connections	Instance and IP address	Count
Inactive connections	Instance and IP address	Count
New connections	Instance and IP address	Count

## Procedure

1. Log on to the [CloudMonitor console](#).
2. Optional: Add an alert recipient. If you have already specified a recipient, you can skip this step.
  - a) In the left-side navigation pane, choose **Alarms > Alarm Contacts**.
  - b) On the **Alarm Contacts** tab, click **Create Alarm Contact** in the upper-right corner.



- c) In the **Set Alarm Contact** dialog box that appears, enter the required contact information. Verify the **Phone** or **Email ID**, and then click **Save**.

The screenshot shows the 'Set Alarm Contact' dialog box. It has a close button (X) in the top right corner. The form contains the following fields:

- Name:** A text input field with the value 'doctest-mail'. Below it is a note: 'The name must be 2-40 characters, can include English letters, numbers, . , and underscores, and should start with a Chinese or English character.'
- Phone:** An empty text input field.
- Email ID:** A text input field with a blurred value.
- Ali WangWang:** An empty text input field.
- DingTalk Robot:** An empty text input field. Below it is a link: 'How to get the DingTalk robot address'.

At the bottom of the dialog box, there is a slider control with a double arrow icon and the text 'Please hold down the slider and drag it to the far right'. At the bottom right, there are 'Save' and 'Cancel' buttons.

The alert recipient is saved.

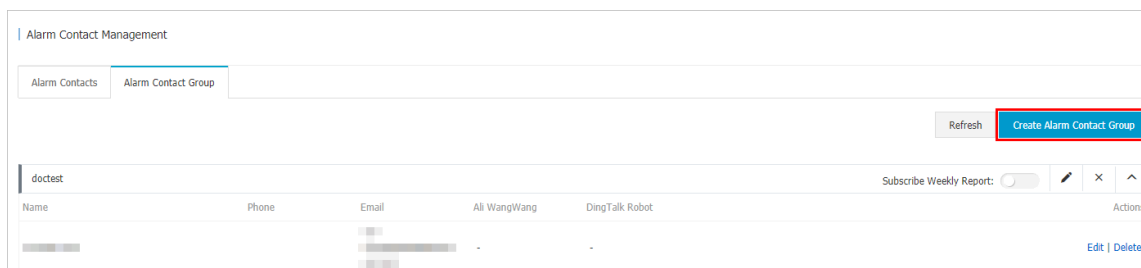
3. Optional: Create an alert contact group. If you have already created an alert contact group, you can skip this step.



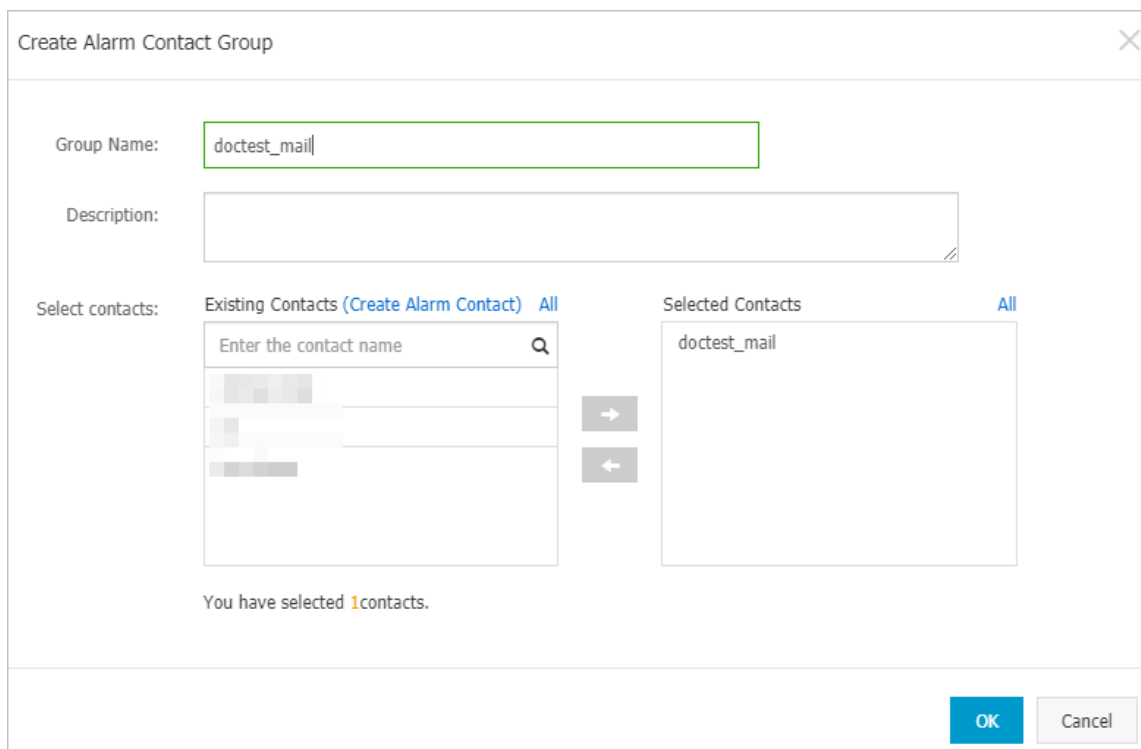
### Note:

The recipients of alert notifications must be contact groups. You can add one or more recipients to a contact group.

- a) In the left-side navigation pane, choose **Alarms > Alarm Contacts**.
- b) On the **Alarm Contact Group** tab, click **Create Alarm Contact Group** in the upper-right corner.



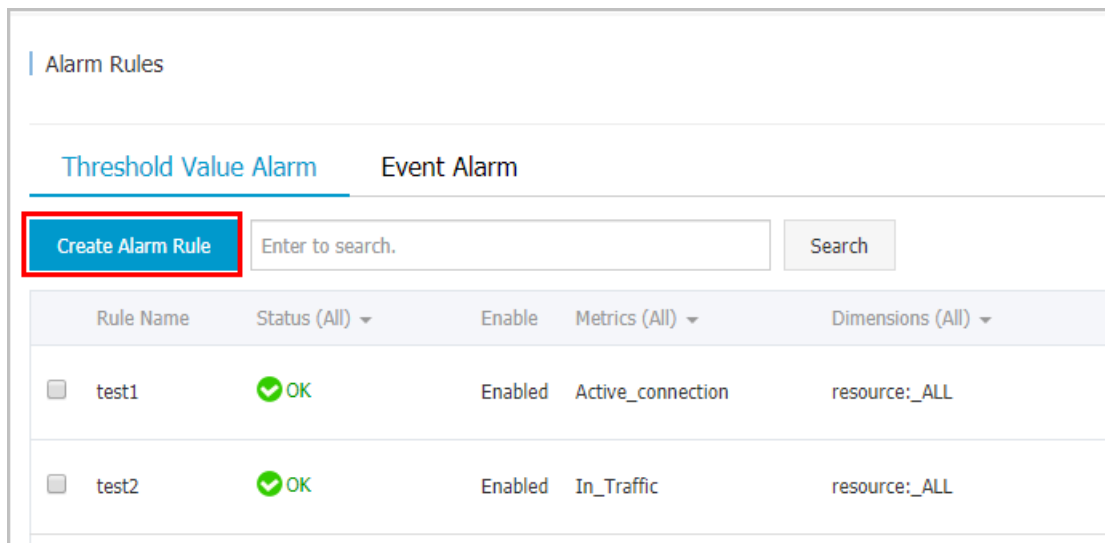
- c) In the **Create Alarm Contact Group** dialog box that appears, enter a group name in the **Group Name** field. Select recipients from the left-side **Existing Contacts** list and add them to the right-side Selected Contacts list. Click **OK**.



The contact group is created.


#### 4. Create an alert rule


- a) In the left-side navigation pane, choose **Alarms > Alarm Rules**.
- b) On the **Threshold Value Alarm** tab, click **Create Alarm Rule**.



- c) On the **Create Alarm Rule** page, set the parameters and click **Confirm**. The following table lists the parameters and descriptions.

Category	Parameter	Description
Related Resource	Product	Select <b>NewBGPDDoS</b> .
	Resource Range	<p>The resources to which the alert rule is applied. You can select <b>All Resources</b> or <b>Instances</b>.</p> <ul style="list-style-type: none"> <li><b>All Resources:</b> The alert rule is applied to all Anti-DDoS Pro instances. An alert is triggered when any of the Anti-DDoS Pro instances matches the specified rule.</li> <li><b>Instances:</b> The alert rule is applied to selected Anti-DDoS Pro instances. An alert is triggered when one of the selected instances matches the specified rule.</li> </ul>
Set Alert Rules	Alarm Rule	Specify a name for the alert rule.

Category	Parameter	Description
	<b>Rule Description</b>	<p>Set the conditions that are used to control how the alert rule is triggered.</p> <div>  <b>Note:</b>            We recommend that you set the threshold of metrics based on your actual business requirements. For more information, see <a href="#">Table 11-1: Anti-DDoS Pro metrics</a>. A low threshold may frequently trigger alerts and negatively impact user experience. A high threshold may leave insufficient time for you to manage attacks.         </div> <p>Default condition: An Anti-DDoS Pro metric generates a data point every 60 seconds. In the following examples, the Anti-DDoS Pro metrics generate five data points every five-minute detection period.</p> <ul style="list-style-type: none"> <li>• Sample rule description: New connection, 5 minute cycle, 3 periods, once, and &gt; 200. In this rule, the detection period is set to five minutes . CloudMonitor checks the data points (number of new connections) generated within three detection periods in a row, which are 15 data points in total. If any data point shows that the number of new connections has exceeded 200 , an alert is triggered.</li> <li>• Sample rule description: Out traffic, 5 minute cycle, 3 periods, and ≥ 50 Mbit/s. In this rule , the detection period is set to five minutes . CloudMonitor checks the data points ( outbound data transfer rate) generated within three detection periods in a row, which are 15 data points in total. If any data point shows that the outbound data transfer rate has exceeded 50 Mbit/s, an alert is triggered.</li> </ul> <p>You can click <b>Add Alarm Rule</b> to add more alert rules. Specify a <b>name</b> and <b>rule description</b> for each alert rule.</p>

Category	Parameter	Description
	<b>Mute for</b>	Set a mute period. If the alert is not cleared within the mute period, a new alert notification is sent when the mute period ends. The minimum value is 5 minutes and the maximum value is 24 hours.
	<b>Effective Period</b>	The time period during which the alert rule remains effective. The system only sends alerts within the effective period. The system records alerts if they occur during a non-effective period.
<b>Notification Method</b>	<b>Notification Contact</b>	The contact group that receives alerts.
	<b>Notification Methods</b>	<p>Alert levels include critical, warning, and info. Different levels of alerts are sent by using different methods.</p> <ul style="list-style-type: none"> <li>Phone + Text Message + Email + DingTalk (Critical)</li> </ul> <div>  <b>Note:</b>            You can select this notification method only after you purchase a notification plan that supports phone calls.         </div> <ul style="list-style-type: none"> <li>Test Message + Email + DingTalk (Warning)</li> <li>Email + DingTalk (Info)</li> </ul>
	<b>Auto Scaling</b>	After you specify a scaling rule, the specified scaling rule is triggered when an alert occurs. In this example, do not set this parameter.
	<b>Email Remark</b>	Optional. You can add remarks to email notifications. Remarks is included in email notifications.

Category	Parameter	Description
	<b>HTTP Callback</b>	CloudMonitor uses a POST request to push an alert to the specified public URL address. Currently, only HTTP requests are supported.



Create Alarm Rule [Back to](#)

1

Related Resource

Product: NewBGPDDoS

Resource Range: instance

instance: ddoscoo-cn-001

2

Set Alarm Rules

Alarm Rule: Example-1

Rule Description: New\_connection 5Minute cycle Continue for 3 Once >= 200 count

Alarm Rule: Example-2 [Delete](#)

Rule Description: Out\_Traffic 5Minute cycle Continue for 3 Once >= 50 Mbit/s

[+Add Alarm Rule](#)

Mute for: 24 h

Effective Period: 00:00 To: 23:59

Out\_Traffic-Maximum-ddoscoo-cn-4591euwia001

Warning Line (Value: 52428800)

3

Notification Method

Notification Contact: Contact Group All

Search

Quickly create a contact group

Selected Groups 1 count

doctest

Notification Methods: Phone + Text Message + Email + DingTalk (Critical) Text Message + Email + DingTalk (Warning) Email + DingTalk (Info)

☐ Auto Scaling (the corresponding scaling rule will be triggered when the alarm occurs)

Email Subject: The default format of email theme is Product Name + Metric Name + Instance ID.

Email Remark: Optional

HTTP Callback: for example: http://alert.aliyun.com:8080/callback

Confirm

Cancel

The Anti-DDoS Pro alert rule is created. When the Anti-DDoS Pro metric fits the alert rule description, an alert is sent to the specified contact group.

## 11.2 Monitor black hole events and traffic scrubbing events on Anti-DDoS Pro

This topic describes how to create rules to alert on black hole events and scrubbing events on Anti-DDoS Pro in the CloudMonitor console. The alerts can keep you informed of the latest black hole events and scrubbing events and allow you to troubleshoot errors and restore workloads as early as possible.

### Context

CloudMonitor is a service to monitor applications and Alibaba Cloud resources. The event monitoring feature of CloudMonitor provides you with a centralized platform to query and summarize the system events on cloud services. This allows you to track the use of cloud resources.

You can query the black hole events and scrubbing events on Anti-DDoS Pro and create alert rules based on the event level. You can receive notifications or configure alert callbacks through text messages, emails, or DingTalk. CloudMonitor notifies you of critical events at the earliest opportunity. This allows you to handle the events in time. For more information, see [An overview of event monitoring](#).

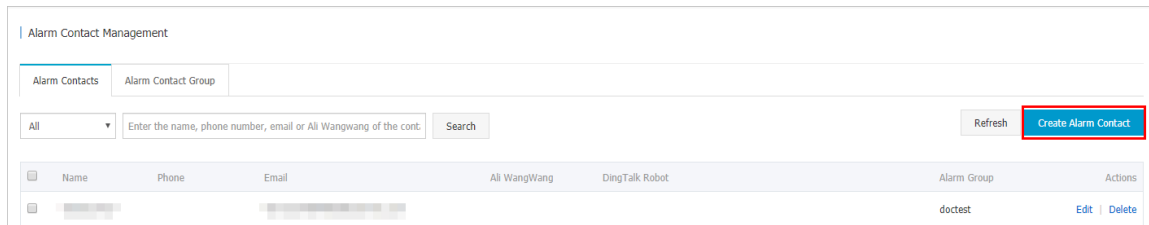
### Procedure

1. Log on to the [CloudMonitor console](#).

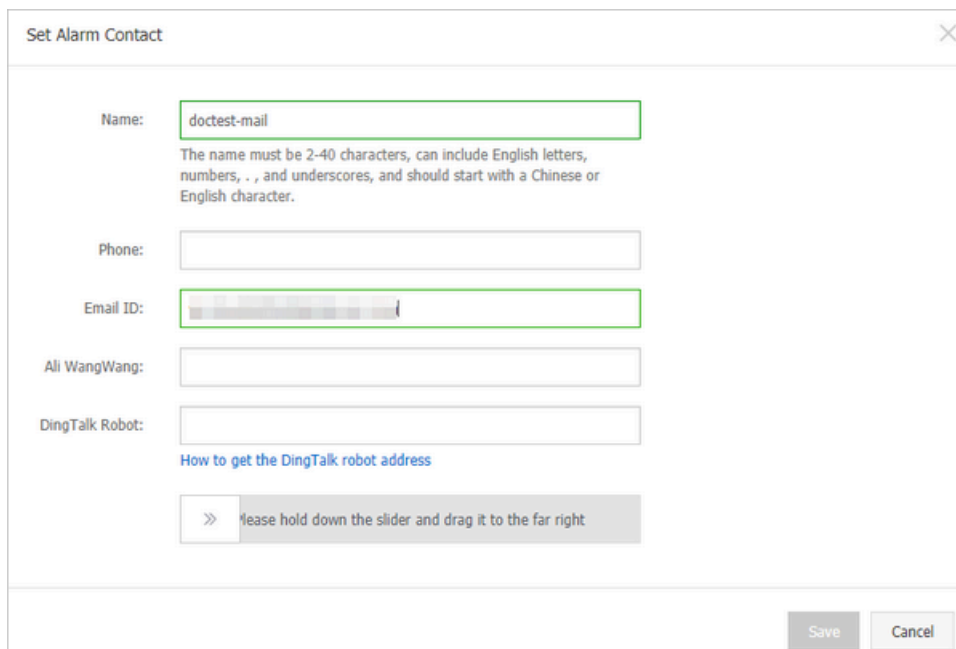
2. Optional: Add an alert recipient. If you have already specified a recipient, you can skip this step.

a) In the left-side navigation pane, choose **Alarms > Alarm Contacts**.

b) On the **Alarm Contacts** tab, click **Create Alarm Contact** in the upper-right corner.



c) In the **Set Alarm Contact** dialog box that appears, enter the required contact information. Verify the **Phone** or **Email ID**, and then click **Save**.



The alert recipient is saved.

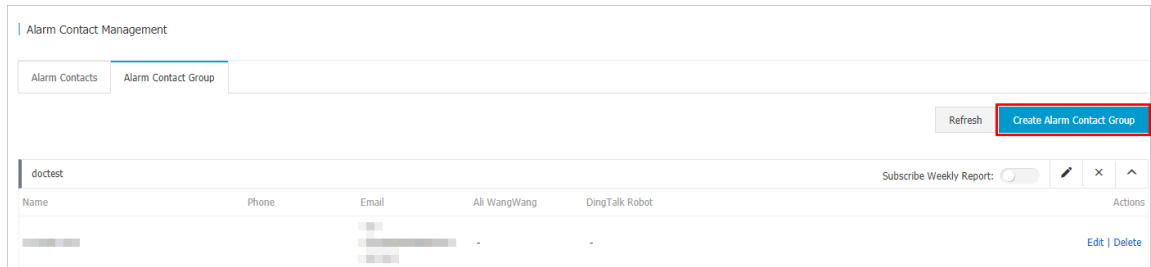
3. Optional: Create an alert contact group. If you have already created an alert contact group, you can skip this step.



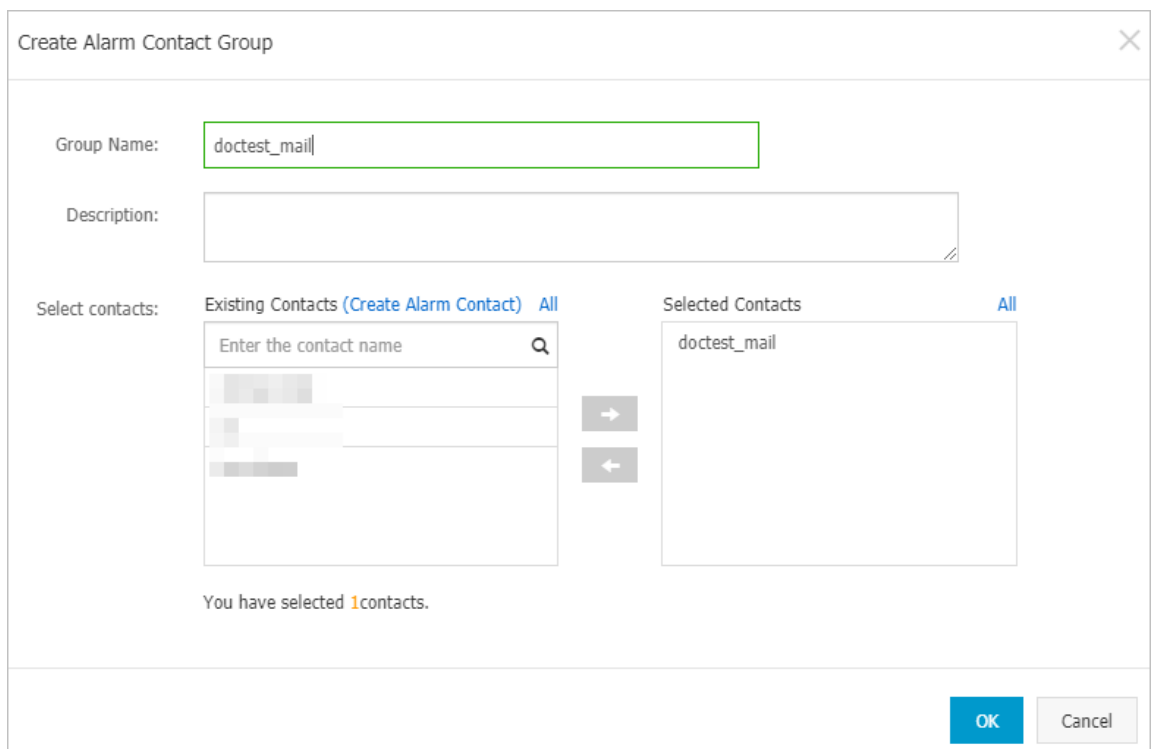
**Note:**

The recipients of alert notifications must be contact groups. You can add one or more recipients to a contact group.

- a) In the left-side navigation pane, choose **Alarms > Alarm Contacts**.
- b) On the **Alarm Contact Group** tab, click **Create Alarm Contact Group** in the upper-right corner.



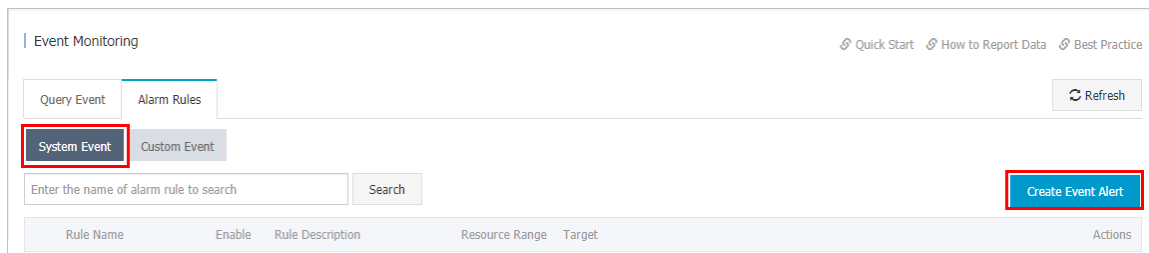
- c) In the **Create Alarm Contact Group** dialog box that appears, enter a group name in the **Group Name** field. Select recipients from the left-side **Existing Contacts** list and add them to the right-side Selected Contacts list. Click **OK**.



The contact group is created.

#### 4. Create an event alert rule for a cloud service.

- a) In the left-side navigation pane, click **Event Monitoring**.
- b) On the **Alarm Rules** tab, select **System Event**, and click **Create Event Alert**.



- c) In the **Create/Modify Event Alert** pane, configure the alert rule, and click **OK**. The parameters are described as follows.

Module	Parameter	Description
Basic Information	Alarm Rule Name	Enter the name of the alert rule.
Event alert	Event Type	Select <b>System Event</b> .
	Product Type	Select <b>NewBGPDDoS</b> .
	Event Type	Select the type of the events to alert on. Valid values include <b>Black hole</b> and <b>Traffic scrubbing</b> . You can select multiple event types.
	Event Level	Select the level of events to alert on. Valid values include <b>CRITICAL</b> , <b>WARN</b> , and <b>INFO</b> . You can select multiple levels and must select <b>CRITICAL</b> .
	Event Name	Select one or more events to alert on. <ul style="list-style-type: none"> <li>Black hole events include <b>In black hole</b> and <b>Black hole ended</b>. All black hole events are critical.</li> <li>Traffic scrubbing events include <b>Scrubbing</b> and <b>Scrubbing ended</b>. All scrubbing events are critical.</li> </ul>
	Resource Range	Select <b>All Resources</b> .

Module	Parameter	Description
Alarm Type	Alert Notification	Select <b>Alert Notification</b> . Select a <b>Contact Group</b> and a <b>Notification Method</b> . <ul style="list-style-type: none"><li>Contact Group: Select an existing contact group.</li><li>Notification Method: Select <b>Warning (Message +Email ID+DingTalk Robot)</b> or <b>Info (Email ID +DingTalk Robot)</b>.</li></ul> You can click <b>Add</b> to add more contact groups and notification methods.
	MNS queue	This option is not required.
	Function service	This option is not required.
	URL callback	This option is not required.

Module	Parameter	Description
	Log Service	This option is not required.

**Create / Modify Event Alert**

**Basic Information**

Alarm Rule Name

anti\_ddos\_event

**Event alert**

Event Type

☒ System Event

☐ Custom Event

Product Type

NewBGPDDoS

Event Type

All types ✕

Event Level

CRITICAL ✕

WARN ✕

INFO ✕

Event Name

ddoscoo\_event\_blackhole\_add ✕

Resource Range

☒ All Resources

☐ Application Groups

**Alarm Type**

☒ Alarm Notification

Contact Group

doctest

Delete

Notification Method

Warning (Message+Email ID+DingTalk Robot )

+Add

☐ MNS queue

☐ Function service (Best Practices)

☐ URL callback

OK

Cancel

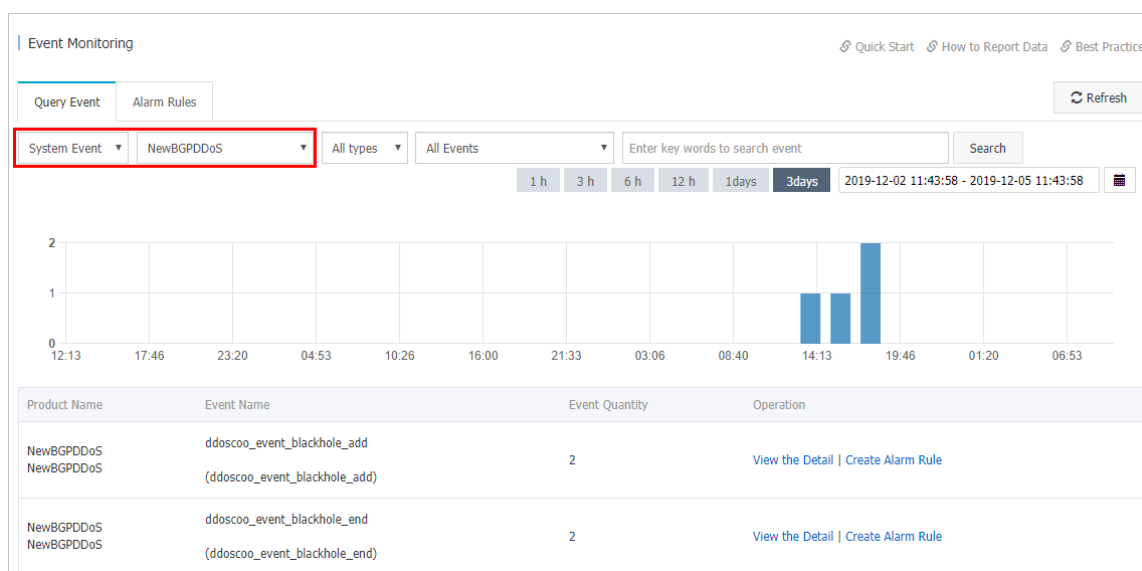


The alert rule is created. When a black hole event or traffic scrubbing event occurs on Anti-DDoS Pro, the specified contact group receives an alert.

5. Optional: Query events. You can query the recent black hole events and scrubbing events on Anti-DDoS Pro in the CloudMonitor console.

a) On the **Event Monitoring** page, click the **Query Event** tab.

b) Select **System Event** and **NewBGPDDoS**, and specify the event type and time period.



c) In the event list, click **View Details** to view the details of an event.

Time	Product Name	Event Name	Event Level	Status	Region	Resource	Contents	Close Detail
19-12-04 18:30:26	NewBGPDDoS	ddoscoo_event_blackhole_add (ddoscoo_event_blackhole_add)	CRITICAL	blackhole_begin	China East 1 (Hangzhou)	acs:yundun-ddoscoo:cn-hangzhou:1289654106023090:instance/ddoscoo-cn-	<pre>{   "event_time": "2019-12-04 18:30:24",   "event_type": "blackhole",   "instanceId": "ddoscoo-cn-0pp1e1ive006",   "ip": "203.104",   "status": "blackhole_begin",   "user_id": "1289654106023090" }</pre>	
19-12-04 15:54:25	NewBGPDDoS	ddoscoo_event_blackhole_add (ddoscoo_event_blackhole_add)	CRITICAL	blackhole_begin	China East 1 (Hangzhou)	acs:yundun-ddoscoo:cn-hangzhou:1289654106023090:instance/ddoscoo-cn-	<pre>{   "event_time": "2019-12-04 15:54:22",   "event_type": "blackhole",   "instanceId": "ddoscoo-cn-0pp1e1ive006",   "ip": "203.104",   "status": "blackhole_begin",   "user_id": "1289654106023090" }</pre>	

## 11.3 Create an Anti-DDoS Pro dashboard

This topic describes how to create a custom Anti-DDoS Pro dashboard and add charts to the dashboard in the CloudMonitor console. Custom Anti-DDoS Pro dashboards and charts help you monitor your workloads.

### Context

CloudMonitor is a service that monitors applications and Alibaba Cloud resources. CloudMonitor supports custom dashboards that display monitoring data. On a dashboard, you can view the monitoring data of multiple services and instances. This allows you to monitor the states of different instances that run the same workloads.

The dashboard feature provided by CloudMonitor is compatible with Anti-DDoS Pro. You can create and customize Anti-DDoS Pro dashboards in the CloudMonitor console. CloudMonitor supports the following Anti-DDoS Pro monitor metrics.

**Note:**

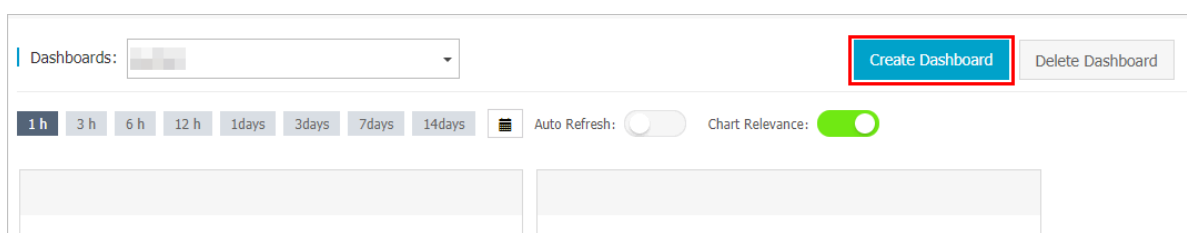
Anti-DDoS Pro back-to-origin traffic refers to the workload traffic that is scrubbed by Anti-DDoS Pro before it is forwarded to the origin server.

**Table 11-2: Anti-DDoS Pro metrics**

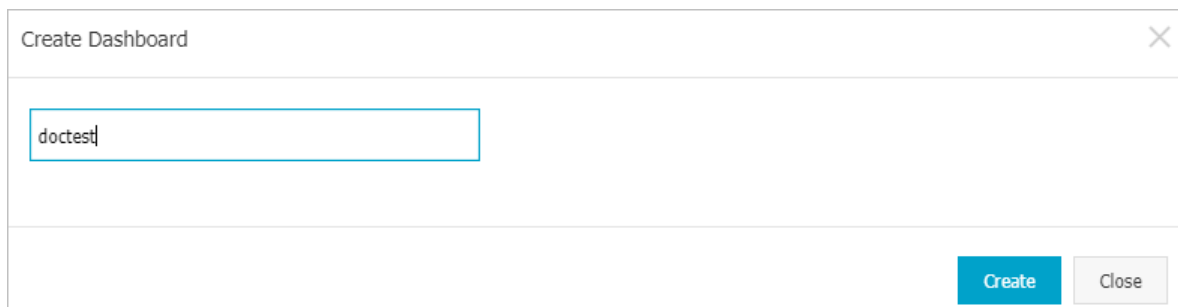
Metric	Dimension	Unit
Anti-DDoS Pro outbound traffic	Instance and IP address	bit/s
Anti-DDoS Pro inbound traffic	Instance and IP address	bit/s
Anti-DDoS Pro back-to-origin traffic	Instance and IP address	bit/s
Active connections	Instance and IP address	Count
Inactive connections	Instance and IP address	Count
New connections	Instance and IP address	Count

**Procedure**

1. Log on to the [CloudMonitor console](#).
2. Choose **Dashboard > Custom Dashboard**, and then click **Create Dashboard**.



3. In the **Create Dashboard** dialog box that appears, specify a name for the dashboard, and then click **Create**.



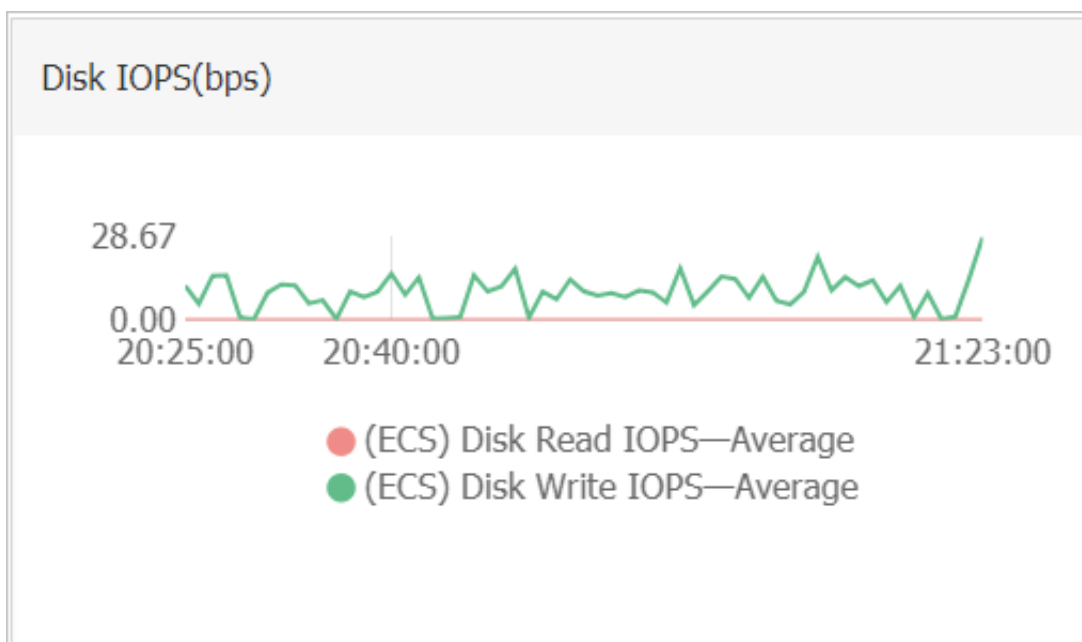
The screenshot shows a 'Create Dashboard' dialog box. The title bar at the top says 'Create Dashboard' and has a close button (X) on the right. Below the title bar is a large text input field. Inside this field, the text 'doctest' is entered. At the bottom right of the dialog, there are two buttons: a blue 'Create' button and a grey 'Close' button.

After the dashboard is created, you are redirected to the Dashboards page. You can select a dashboard from the **Dashboards** drop-down list to view or manage the selected dashboard.

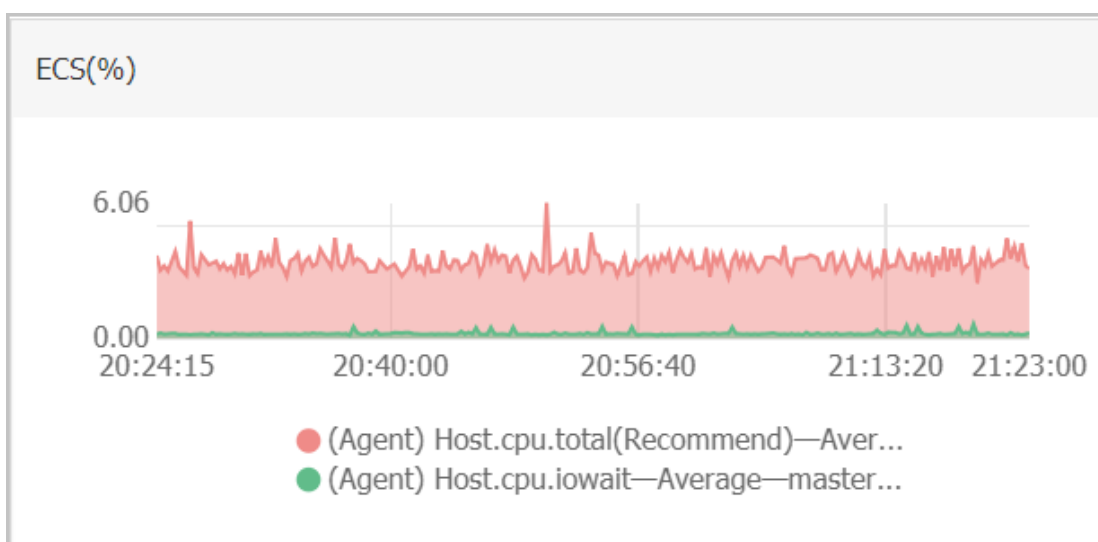
4. Open the dashboard, click **Add View**, and set the required parameters in the **Add View** page that appears on the right side to create a custom chart.

a) **Select a chart type.** Supported chart types include line, area, and pie charts, TopN tables, and heat maps.

- Line chart: Displays monitoring data on a basis of time series. Multiple metrics can be added.



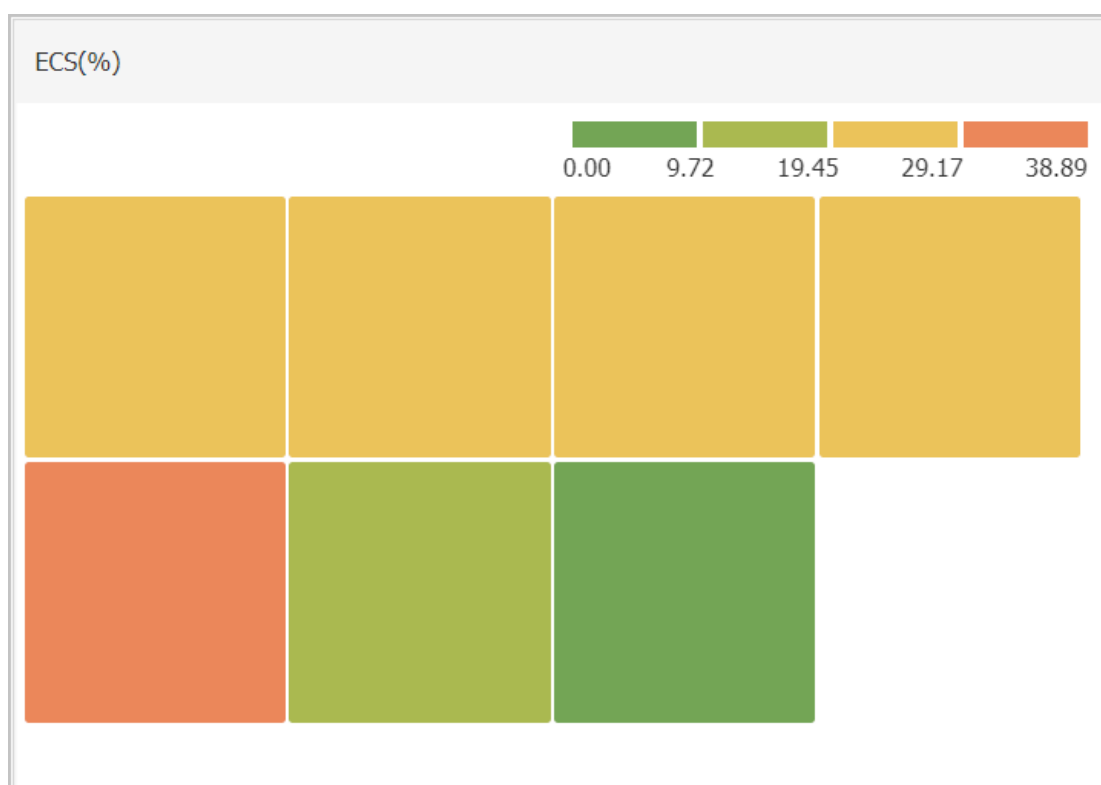
- Area chart: Displays monitoring data on a basis of time series. Multiple metrics can be added.



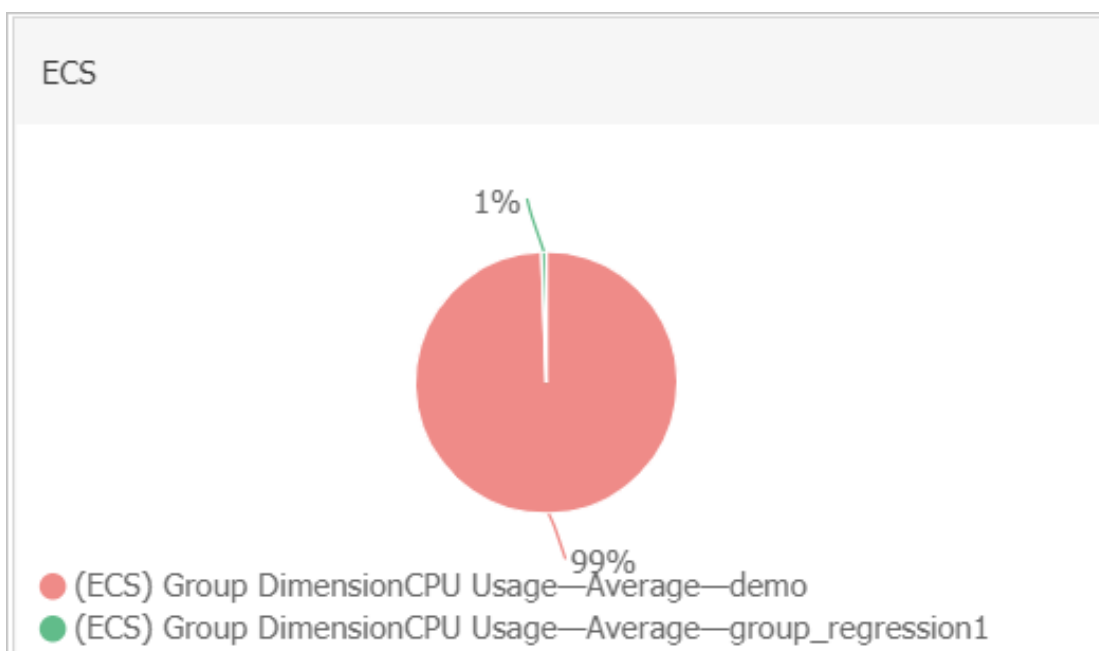
- Table: Displays real-time metric data in descending order. Each table displays up to 1,000 data records, which are either the first 1,000 records or the last 1,000 records. Only one metric can be added.

ECS(%)		
Time	Dimensions	Maximum Value
2018-12-06 21:25:00	ESS-asg-yinna_test	100
2018-12-06 21:20:00	node-0003-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	55.56
2018-12-06 21:25:00	master-02-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	38.89
2018-12-06 21:25:00	master-03-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	38.1
2018-12-06 21:00:00	master-01-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	37.5
2018-12-06 21:00:00	node-0001-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	35.29
2018-12-06 21:20:00	node-0002-k8s-for-cs-c9ebd45a41dd645a498a5c06af2b88c53	29.41

- Heat map: Displays real-time metric data. Heat maps show the distribution and comparison of real-time data of a specific metric for multiple instances. Only one metric can be added.

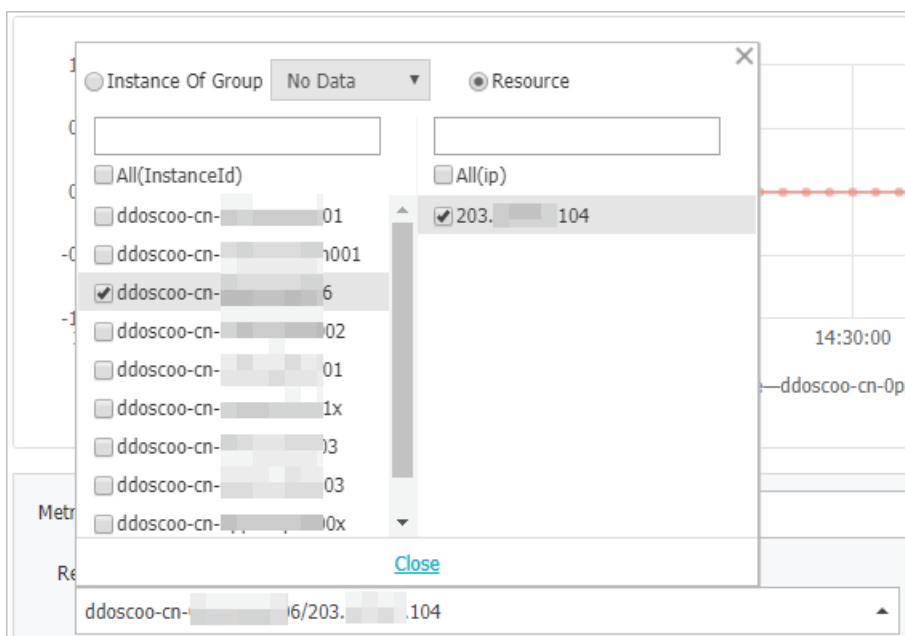


- Pie chart: Displays real-time metric data and can be used for data comparisons. Only one metric can be added.



b) **Select metrics.** Click the **Dashboards** tab and select **NewBGPDDoS**. Select metrics and resources from the **Metrics** and **Resource** drop-down lists, respectively.

- Metrics: Select the Anti-DDoS Pro metrics that you want to monitor. For more information, see [Anti-DDoS Pro metric](#).
- Resource: Select the Anti-DDoS Pro instances and IP addresses that you want to monitor.



You can click **Add Metrics** to add multiple metrics to the chart.

c) Click **Save** to create the chart.

Add View

1 Chart Type

Line

Area

Table

Heat Map

Pie Chart

2 Select Metrics

Dashboards

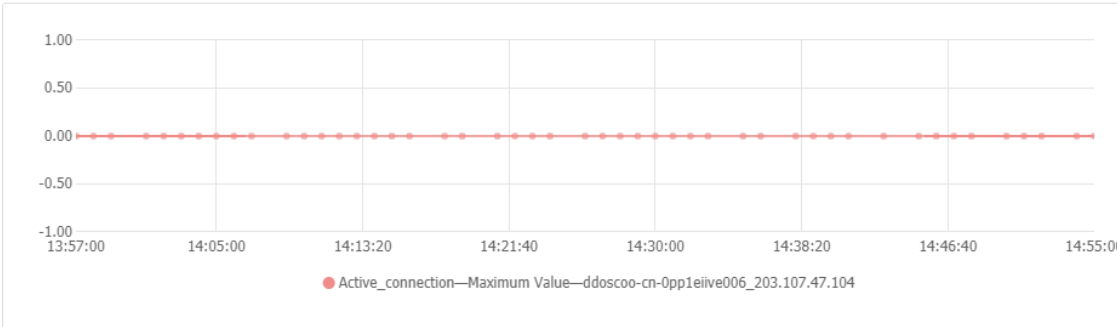
Log Monitoring

Custom

NewBGPDDoS

NewBGPDDoS

Heat Map Gradient Range: 0 auto



Metrics: Active\_connection Maximum Value

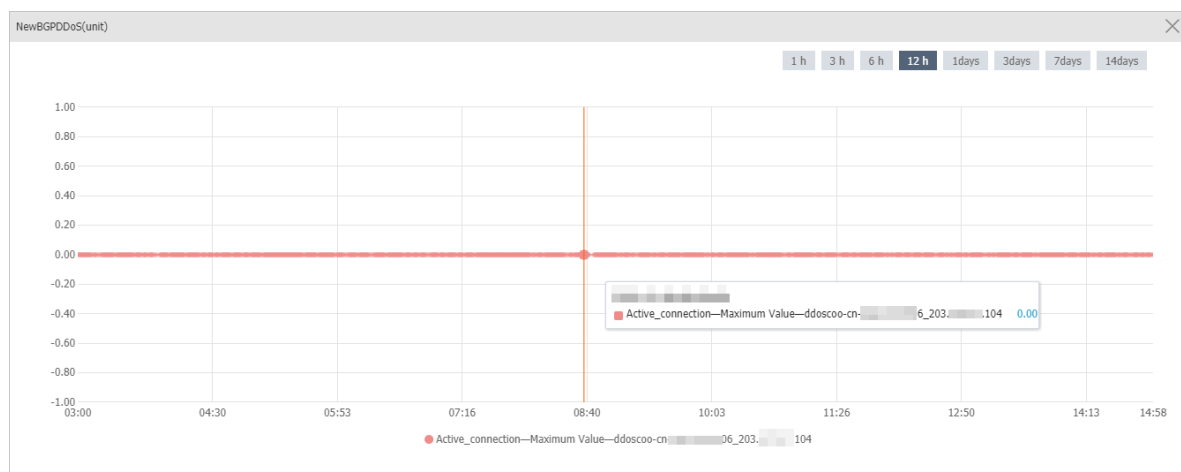
Resource: ddoscoo-cn- /203 104

+AddMetrics

Save

Cancel

You have created a chart that displays monitoring data of Anti-DDoS Pro.



5. To add more charts to the dashboard, repeat step 4. For more information, see [#unique\\_113](#) and [#unique\\_114](#).

## 12 API Reference

---

### 12.1 List of operations by function

The following tables list API operations available for use in Anti-DDoS Pro or Anti-DDoS Premium.

For more information, see [API Explorer](#).

#### Instance management

Operation	Description
<a href="#">DescribeInstanceIds</a>	Queries the IDs of all Anti-DDoS Pro or Anti-DDoS Premium instances.
<a href="#">DescribeInstances</a>	Queries the versions and status information of one or more Anti-DDoS Pro or Anti-DDoS Premium instances, such as traffic forwarding status, expiration status, and overdue payment status.
<a href="#">DescribeInstanceDetails</a>	Queries the IP addresses and Internet service provider (ISP) lines of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.
<a href="#">DescribeInstanceSpecs</a>	Queries the specifications of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.
<a href="#">DescribeInstanceStatistics</a>	Queries the statistics on one or more Anti-DDoS Pro or Anti-DDoS Premium instances, such as the numbers of protected domain names and ports.
<a href="#">ModifyInstanceRemark</a>	Modifies the description of an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">DescribeElasticBandwidthSpec</a>	Queries the available burstable protection bandwidth of an Anti-DDoS Pro instance.
<a href="#">ModifyElasticBandWidth</a>	Modifies the burstable protection bandwidth of an Anti-DDoS Pro instance.



Operation	Description
<a href="#">DescribeDefenseCountStatistics</a>	Queries the information of mitigation sessions of an Anti-DDoS Premium instance , such as the numbers of available and used advanced mitigation sessions.

## Access management

**Table 12-1: Domain name-based access**

Operation	Description
<a href="#">DescribeDomains</a>	Queries domain names for which the forwarding rules are created.
<a href="#">DescribeWebRules</a>	Queries the forwarding rules of a website.
<a href="#">CreateWebRule</a>	Creates a forwarding rule for a website.
<a href="#">ModifyWebRule</a>	Modifies the forwarding rule of a website.
<a href="#">DeleteWebRule</a>	Deletes the forwarding rule of a website.
<a href="#">DescribeWebInstanceRelations</a>	Queries the information of Anti-DDoS Pro or Anti-DDoS Premium instances that are associated with websites.
<a href="#">AssociateWebCert</a>	Associates an SSL certificate with the forwarding rule of a website.
<a href="#">ModifyTlsConfig</a>	Modifies the Transport Layer Security (TLS) policy configuration for the forwarding rule of a website.
<a href="#">DescribeWebCustomPorts</a>	Queries the supported custom ports of a website.
<a href="#">DescribeWebAccessMode</a>	Queries the access mode settings of a website.
<a href="#">ModifyWebAccessMode</a>	Modifies the access mode settings of a website.
<a href="#">DescribeCerts</a>	Queries the certificate information of a website.
<a href="#">DescribeCnameReuses</a>	Queries the CNAME reuse information of websites.
<a href="#">ModifyCnameReuse</a>	Enables or disables CNAME reuse for a website.

Operation	Description
<a href="#">ModifyHttp2Enable</a>	Enables or disables HTTP/2 for the forwarding rule of a website.

**Table 12-2: Port-based access**

Operation	Description
<a href="#">DescribeNetworkRules</a>	Queries port forwarding rules.
<a href="#">CreateNetworkRules</a>	Creates a port forwarding rule.
<a href="#">ConfigNetworkRules</a>	Modifies a port forwarding rule, namely, the IP addresses of the origin server.
<a href="#">DeleteNetworkRule</a>	Deletes a port forwarding rule.
<a href="#">DescribeHealthCheckList</a>	Queries the Layer 4 or Layer 7 health check configuration of a port forwarding rule.
<a href="#">ModifyHealthCheckConfig</a>	Modifies the Layer 4 or Layer 7 health check configuration of a port forwarding rule.
<a href="#">DescribeHealthCheckStatus</a>	Queries the health status of an origin server.

**Table 12-3: Sec-Traffic Manager**

Operation	Description
<a href="#">DescribeSchedulerRules</a>	Queries the scheduling rules that are created for Sec-Traffic Manager.
<a href="#">CreateSchedulerRule</a>	Creates a scheduling rule for Sec-Traffic Manager.
<a href="#">ModifySchedulerRule</a>	Modifies the scheduling rule of Sec-Traffic Manager.
<a href="#">DeleteSchedulerRule</a>	Deletes the scheduling rule of Sec-Traffic Manager.

## Protection settings

**Table 12-4: Protection policies for infrastructure**

Operation	Description
<a href="#">DescribeAutoCcListCount</a>	Queries the numbers of IP addresses in the whitelist and blacklist of an Anti-DDoS Pro or Anti-DDoS Premium instance.

Operation	Description
<a href="#">DescribeAutoCcBlacklist</a>	Queries IP addresses in the blacklist of an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">AddAutoCcBlacklist</a>	Adds IP addresses to the blacklist of an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">DeleteAutoCcBlacklist</a>	Removes IP addresses from the blacklist of an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">EmptyAutoCcBlacklist</a>	Clears IP addresses from the blacklist of an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">DescribeAutoCcWhitelist</a>	Queries IP addresses in the whitelist of an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">AddAutoCcWhitelist</a>	Adds IP addresses to the whitelist of an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">DeleteAutoCcWhitelist</a>	Removes IP addresses from the whitelist of an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">EmptyAutoCcWhitelist</a>	Clears IP addresses from the whitelist of an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">DescribeUnBlackholeCount</a>	Queries the total and remaining quotas that you can deactivate the black hole.
<a href="#">DescribeBlackholeStatus</a>	Queries the black hole status of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.
<a href="#">ModifyBlackholeStatus</a>	Deactivates the black hole.
<a href="#">DescribeNetworkRegionBlock</a>	Queries the blocked regions that are configured for an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">ConfigNetworkRegionBlock</a>	Configures blocked regions for an Anti-DDoS Pro or Anti-DDoS Premium instance.
<a href="#">DescribeBlockStatus</a>	Queries the Diversion from Origin Server configurations of one or more Anti-DDoS Pro instances.

Operation	Description
<a href="#">ModifyBlockStatus</a>	Modifies the Diversion from Origin Server configuration of an Anti-DDoS Pro instance.
<a href="#">DescribeUnBlockCount</a>	Queries the remaining quota that you can use the Diversion from Origin Server policy.

**Table 12-5: Protection policies for website services**

Operation	Description
<a href="#">DescribeWebCcProtectSwitch</a>	Queries the status of each protection policy for websites.
<a href="#">ModifyWebAIProtectSwitch</a>	Enables or disables the Intelligent Protection policy for a website.
<a href="#">ModifyWebAIProtectMode</a>	Modifies the mode settings of the Intelligent Protection policy for a website.
<a href="#">ModifyWebIpSetSwitch</a>	Enables or disables the Black Lists and White Lists (Domain Names) policy for a website.
<a href="#">ConfigWebIpSet</a>	Configures the IP address whitelist and blacklist for a website.
<a href="#">EnableWebCC</a>	Enables the Frequency Control policy for a website.
<a href="#">DisableWebCC</a>	Disables the Frequency Control policy for a website.
<a href="#">ConfigWebCCTemplate</a>	Configures the mode of the Frequency Control policy for a website.
<a href="#">EnableWebCCRule</a>	Turns on the Custom Rule switch of the Frequency Control policy for a website.
<a href="#">DisableWebCCRule</a>	Turns off the Custom Rule switch of the Frequency Control policy for a website.
<a href="#">DescribeWebCCRules</a>	Queries the custom frequency control rules that are created for a website.
<a href="#">CreateWebCCRule</a>	Creates a custom frequency control rule for a website.
<a href="#">ModifyWebCCRule</a>	Modifies the custom frequency control rule of a website.

Operation	Description
<a href="#">DeleteWebCCRule</a>	Deletes the custom frequency control rule of a website.
<a href="#">ModifyWebPreciseAccessSwitch</a>	Enables or disables the Accurate Access Control policy for a website.
<a href="#">DescribeWebPreciseAccessRule</a>	Queries the accurate access control rules that are created for websites.
<a href="#">ModifyWebPreciseAccessRule</a>	Modifies the accurate access control rule of a website.
<a href="#">DeleteWebPreciseAccessRule</a>	Deletes one or more accurate access control rules that are created for a website.
<a href="#">ModifyWebAreaBlockSwitch</a>	Enables or disables the Blocked Regions (Domain Names) policy for a website.
<a href="#">DescribeWebAreaBlockConfigs</a>	Queries the Blocked Regions (Domain Names) configurations for websites.
<a href="#">ModifyWebAreaBlock</a>	Modifies the blocked regions that are configured in the Blocked Regions (Domain Names) policy for a website.

**Table 12-6: Protection policies for non-website services**

Operation	Description
<a href="#">DescribePortAutoCcStatus</a>	Queries the Intelligent Protection configurations of non-website services.
<a href="#">ModifyPortAutoCcStatus</a>	Modifies the Intelligent Protection configuration of a non-website service.
<a href="#">DescribeNetworkRuleAttributes</a>	Queries the mitigation settings of the port forwarding rule for a non-website service, which include session persistence and anti-DDoS protection policies.
<a href="#">ModifyNetworkRuleAttribute</a>	Modifies the session persistence settings of a port forwarding rule.

**Table 12-7: Custom policies for specific scenarios**

Operation	Description
<a href="#">DescribeSceneDefensePolicies</a>	Queries details about a scenario-specific custom policy.

Operation	Description
<a href="#">CreateSceneDefensePolicy</a>	Creates a scenario-specific custom policy.
<a href="#">ModifySceneDefensePolicy</a>	Modifies a scenario-specific custom policy.
<a href="#">DeleteSceneDefensePolicy</a>	Deletes a scenario-specific custom policy.
<a href="#">DescribeSceneDefenseObjects</a>	Queries the protection target of a scenario-specific custom policy.
<a href="#">AttachSceneDefenseObject</a>	Attaches a protection target to a scenario-specific custom policy.
<a href="#">DetachSceneDefenseObject</a>	Deletes the protection target of a scenario-specific custom policy.
<a href="#">EnableSceneDefensePolicy</a>	Enables a scenario-specific custom policy.
<a href="#">DisableSceneDefensePolicy</a>	Disables a scenario-specific custom policy.

### Monitoring reports

Operation	Description
<a href="#">DescribeDDoSEvents</a>	Queries attack events launched against one or more Anti-DDoS Pro or Anti-DDoS Premium instances.
<a href="#">DescribePortFlowList</a>	Queries the traffic data of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.
<a href="#">DescribePortConnsList</a>	Queries the connections established over the ports of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.
<a href="#">DescribePortConnsCount</a>	Queries the statistics on the connections established over the ports of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.
<a href="#">DescribePortMaxConns</a>	Queries the maximum number of connections that can be established over the ports of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.
<a href="#">DescribePortAttackMaxFlow</a>	Queries the peak attack traffic bandwidth and peak attack traffic packet rates of one or more Anti-DDoS Pro or Anti-DDoS Premium instances within a specific period of time.

Operation	Description
<a href="#">DescribePortViewSourceCountries</a>	Queries the countries from which requests are sent to one or more Anti-DDoS Pro or Anti-DDoS Premium instances within a specific period of time.
<a href="#">DescribePortViewSourceProvinces</a>	Queries the regions inside China from which requests are sent to one or more Anti-DDoS Pro or Anti-DDoS Premium instances within a specific period of time.
<a href="#">DescribePortViewSourceIps</a>	Queries the ISPs from which requests are sent to one or more Anti-DDoS Pro or Anti-DDoS Premium instances within a specific period of time.
<a href="#">DescribeDomainAttackEvents</a>	Queries attack events launched against a website.
<a href="#">DescribeDomainQPSList</a>	Queries the statistics on the queries per second (QPS) of a website.
<a href="#">DescribeDomainQpsWithCache</a>	Queries the QPS information of a website , such as the total QPS, QPS blocked by different protection policies, and cache hit ratio.
<a href="#">DescribeDomainOverview</a>	Queries the attack overview of a website , such as the peak HTTP attack traffic and peak HTTPS attack traffic.
<a href="#">DescribeDomainStatusCodeList</a>	Queries the statistics on different response status codes of a website.
<a href="#">DescribeDomainStatusCodeCount</a>	Queries the statistics on different response status codes of a website within a specific period of time.
<a href="#">DescribeDomainTopAttackList</a>	Queries the peak QPS information of a website, such as the attack QPS and total QPS, within a specific period of time.
<a href="#">DescribeDomainViewSourceCountries</a>	Queries the countries from which requests are sent to a website within a specific period of time.
<a href="#">DescribeDomainViewSourceProvinces</a>	Queries the regions inside China from which requests are sent to a website within a specific period of time.

Operation	Description
<a href="#">DescribeDomainViewTopCostTime</a>	Queries the top N URLs that require the longest time to respond to requests within a specific period of time.
<a href="#">DescribeDomainViewTopUrl</a>	Queries the top N URLs that receive the most requests within a specific period of time.

## Log analysis

Operation	Description
<a href="#">DescribeSlsOpenStatus</a>	Checks whether Alibaba Cloud Log Service is activated.
<a href="#">DescribeSlsAuthStatus</a>	Checks whether Anti-DDoS Pro or Anti-DDoS Premium is authorized to access Log Service.
<a href="#">DescribeLogStoreExistStatus</a>	Checks whether a Logstore is created for Anti-DDoS Pro or Anti-DDoS Premium.
<a href="#">DescribeSlsLogstoreInfo</a>	Queries the Logstore information of Anti-DDoS Pro or Anti-DDoS Premium, such as log storage capacity and duration.
<a href="#">ModifyFullLogTtl</a>	Modifies the full log storage duration for Anti-DDoS Pro or Anti-DDoS Premium.
<a href="#">DescribeWebAccessLogDispatchStatus</a>	Checks whether the Log Analysis feature is enabled for all domain names.
<a href="#">DescribeWebAccessLogStatus</a>	Queries the Log Analysis configuration of a single website, such as the feature status and the Log Service project and Logstore that are used.
<a href="#">EnableWebAccessLogConfig</a>	Enables the Log Analysis feature for a website.
<a href="#">DisableWebAccessLogConfig</a>	Disables the Log Analysis feature for a website.
<a href="#">DescribeWebAccessLogEmptyCount</a>	Queries the remaining quota that you can clear the Logstore.
<a href="#">EmptySlsLogstore</a>	Clears the Logstore of Anti-DDoS Pro or Anti-DDoS Premium.



## Tag management

Operation	Description
<a href="#">DescribeTagKeys</a>	Queries all tag keys.
<a href="#">DescribeTagResources</a>	Queries the tags bound to resources.
<a href="#">CreateTagResources</a>	Binds tags to resources.
<a href="#">DeleteTagResources</a>	Unbinds tags from resources.

## Static page caching

Operation	Description
<a href="#">DescribeWebCacheConfigs</a>	Queries the Static Page Caching configurations of websites.
<a href="#">ModifyWebCacheSwitch</a>	Enables or disables the Static Page Caching policy for a website.
<a href="#">ModifyWebCacheMode</a>	Modifies the cache mode settings of the Static Page Caching policy for a website.
<a href="#">ModifyWebCacheCustomRule</a>	Modifies the custom rule of the Static Page Caching policy for a website.
<a href="#">DeleteWebCacheCustomRule</a>	Deletes custom rules of the Static Page Caching policy for a website.

## System configurations and logs

Operation	Description
<a href="#">DescribeStsGrantStatus</a>	Checks whether Anti-DDoS Pro or Anti-DDoS Premium is authorized to access other cloud services.
<a href="#">DescribeBackSourceCidr</a>	Queries the back-to-origin CIDR blocks of Anti-DDoS Pro or Anti-DDoS Premium.
<a href="#">DescribeOpEntities</a>	Queries the operations logs of Anti-DDoS Pro.
<a href="#">DescribeDefenseRecords</a>	Queries the advanced mitigation logs of Anti-DDoS Premium.
<a href="#">DescribeAsyncTasks</a>	Queries details about asynchronous export tasks, such as the task IDs, start time, end time, task status, task parameters, and task results.

Operation	Description
<a href="#">CreateAsyncTask</a>	Creates an asynchronous export task to export forwarding rules for websites, port forwarding rules, session persistence and health check settings, anti-DDoS protection policies, IP address blacklist, or IP address whitelist.
<a href="#">DeleteAsyncTask</a>	Deletes an asynchronous export task.

## 12.2 Make API requests

Anti-DDoS Pro or Anti-DDoS Premium allows you to call its API operations by using HTTP and OpenAPI Explorer. To send an Anti-DDoS Pro or Anti-DDoS Premium API request, you must send an HTTP GET request to the Anti-DDoS Pro or Anti-DDoS Premium endpoint. You must add the request parameters that correspond to the API operation being called. After you call the API operation, the system returns a response. The request and response are encoded in UTF-8.

### Call API operations by using HTTP

Anti-DDoS Pro or Anti-DDoS Premium API operations use the RPC protocol. You can call Anti-DDoS Pro or Anti-DDoS Premium API operations by sending HTTP GET requests.

The request syntax is as follows:

```
http://Endpoint/?Action=xx&Parameters
```

where:

- **Endpoint:** the endpoint of the Anti-DDoS Pro or Anti-DDoS Premium API. Valid values:
  - `ddoscoo.cn-hangzhou.aliyuncs.com`: the endpoint of the Anti-DDoS Pro API
  - `ddoscoo.ap-southeast-1.aliyuncs.com`: the endpoint of the Anti-DDoS Premium API
- **Action:** the name of the operation being performed. For example, to query the IDs of the created Anti-DDoS Pro or Anti-DDoS Premium instances, you must set the Action parameter to **DescribeInstanceIds**.
- **Version:** the version number of the API. Set the value to 2020-01-01.

- **Parameters:** the request parameters for the operation. Separate multiple parameters with ampersands (&).

Request parameters include both common parameters and operation-specific parameters. Common parameters include the API version and authentication information. For more information, see [#unique\\_251](#).

The following example demonstrates how to call the **DescribeInstanceIds** operation in Anti-DDoS Pro or Anti-DDoS Premium.

**Note:**

The following code has been formatted for ease reading.

```
https://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstanceIds
&Format=xml
&Version=2020-01-01
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2020-01-01T12:00:00Z
...
```

### Call API operations by using OpenAPI Explorer

OpenAPI Explorer is a visual tool for calling APIs. OpenAPI Explorer allows you to call APIs of Alibaba Cloud services and APIs provided in Alibaba Cloud Marketplace. You can call these APIs on a webpage or command-line interface (CLI). In addition, OpenAPI Explorer allows you to view the request and response of each API call and dynamically generates SDK sample code.

You can visit <https://api.aliyun.com/> or click the link in the Debugging section of the topic for each API operation to access OpenAPI Explorer.

## 12.3 Request signatures

You must sign all API requests to ensure security. Alibaba Cloud uses the request signature to verify the identity of the API caller. When you call an API operation by using HTTP or HTTPS, the request must include the signature information.

### Overview

You must add the signature to the Anti-DDoS Pro or Anti-DDoS Premium API request in the following format:

```
https://Endpoint?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

where:

- **SignatureMethod**: the encryption method of the signature string. Set the value to **HMAC-SHA1**.
- **SignatureVersion**: the version of the signature encryption algorithm. Set the value to **1.0**.
- **SignatureNonce**: a unique, random number used to prevent replay attacks. You must use different random numbers for different requests. We recommend that you use universally unique identifiers (UUIDs).
- **Signature**: the signature generated after the request has been symmetrically encrypted by using the AccessKey secret.

The signature algorithm complies with RFC 2104 HMAC-SHA1 specifications. The AccessKey secret is used to calculate the hash-based message authentication code (HMAC) value of the encoded and sorted query string, and the HMAC value is used as the signature string. Request signatures include operation-specific parameters. Therefore, the signature of a request varies depending on the request parameters. To calculate the signature string, you can follow the steps in this topic.

```
Signature = Base64( HMAC-SHA1( AccessSecret, UTF-8-Encoding-Of(
```

```
StringToSign)))
```

### Step 1: Compose and encode a string-to-sign

1. Create a canonicalized query string by arranging the request parameters.
  - a. Arrange the request parameters (including all common and operation-specific parameters except Signature) in alphabetical order.

**Note:**

If you use the GET method to submit the request, these parameters are the part located after the question mark (?) and connected by the ampersands (&) in the request uniform resource identifier (URI).

- b. Encode the canonicalized query string in UTF-8. The following table describes the encoding rules.

Character	Encoding rule
Uppercase letters, lowercase letters, digits , and some special characters such as hyphens (-), underscores (_), periods (.), and tildes (~)	These characters do not need to be encoded.
Other characters	Other characters must be percent encoded in %XY format. XY represents the ASCII code of the characters in hexadecimal notation. For example, double quotation marks (") are encoded as %22.
Extended UTF-8 characters	These characters are encoded in %XY%ZA... format.

Character	Encoding rule
Spaces	<p>Spaces must be encoded as %20. Do not encode spaces as plus signs (+).</p> <p>This encoding rule is different from the application/x-www-form-urlencoded MIME encoding algorithm, such as the <code>java.net.URLEncoder</code> class provided by the Java standard library. You can encode spaces according to the encoding rule for the standard library. Then, replace the plus sign (+) with %20, the asterisk (*) with %2A, and %7E with the tilde (~) in the encoded string to obtain an encoded string that complies with the preceding encoding rules. You can use the following <code>percentEncode</code> method to implement this algorithm.</p> <pre>private static final String ENCODING = "UTF-8"; private static String percentEncode(String value) throws UnsupportedOperationException {     return value != null ? URLEncoder.encode(value,     ENCODING).replace("+", "%20").replace("*", "%2A").     replace("%7E", "~") : null; }</pre>

- c. Connect the encoded parameter names and their values by using equal signs (=).
  - d. Sort the connected parameter name and value pairs in the order specified in step 1. i and connect the pairs by using ampersands (&) to obtain the canonicalized query string.
2. Create a string-to-sign from the encoded canonicalized query string.

```
StringToSign=
    HTTPMethod + "&" +
    percentEncode("/") + "&" +
    percentEncode(CanonicalizedQueryString)
```

where:

- **HTTPMethod** indicates the HTTP method used to send the request, such as GET.
- **percentEncode("/")** is the encoded value ("%2F") of a forward slash (/) based on the URL encoding rules described in step 1.i.
- **percentEncode(CanonicalizedQueryString)** is the string constructed by using the canonicalized query string based on the URL encoding rules described in step 1.ii.

## Step 2: Calculate the signature string

1. Calculate the RFC 2104-compliant HMAC value of the string-to-sign.

**Note:**

Use the SHA1 algorithm to calculate the HMAC value of the string-to-sign. Append an ampersand (&) (ASCII code: 38) to your AccessKey secret to obtain the key for the HMAC calculation.

2. Encode the HMAC value in Base64 to obtain the signature string.
3. Add the signature string to the request as the **Signature** parameter.

**Note:**

After the signature string is submitted as the last request parameter value, you must encode the URL according to [RFC 3986](#) in the same way you encode the URL after other parameters are added.

## Example

Use the **DescribeInstanceIds** operation as an example. Assume that AccessKey Id is testid and AccessKey Secret is testsecret. The request URL to be signed is as follows:

```
http://ddoscoo.cn-hangzhou.aliyuncs.com/?Timestamp=2020-01-01T12%3A00%3A00Z&Format=XML&AccessKeyId=testid&Action=DescribeInstanceIds&SignatureMethod=HMAC-SHA1&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&Version=2020-01-01&SignatureVersion=1.0
```

The signature string calculated by using testsecret& is as follows:

```
OLeaidS1JvxuMvnyHOWuJ+uX5qY=
```

Add the **Signature** parameter to the request and set the value to the calculated signature string. The URL of the signed request is as follows:

```
http://ddoscoo.cn-hangzhou.aliyuncs.com/?SignatureVersion=1.0&Action=DescribeInstanceIds&Format=XML&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&
```

```
Version=2020-01-01&AccessKeyId=testid&Signature=OLeaidS1JvxuMvnyH0Wuj+uX5qY=&
SignatureMethod=HMAC-SHA1&Timestamp=2020-01-01T12%3A00%3A00Z
```

## 12.4 Common parameters

This topic describes the request and response parameters that each operation uses.

### Common request parameters

Parameter	Type	Required	Description
<b>RegionId</b>	String	Yes	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li>cn-hangzhou: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>ap-southeast-1: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>Format</b>	String	No	The format in which to return the response. Valid values: <ul style="list-style-type: none"> <li>JSON (default value)</li> <li>XML</li> </ul>
<b>Version</b>	String	Yes	The version number of the API, in the format of YYYY-MM-DD. Set the value to 2020-01-01.
<b>AccessKeyId</b>	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
<b>Signature</b>	String	Yes	The signature string of the current request.
<b>SignatureMethod</b>	String	Yes	The encryption method of the signature string. Set the value to HMAC-SHA1.
<b>Timestamp</b>	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format. The time must be in UTC.  For example, 20:00:00 on January 1, 2020 (UTC+8) is written as 2020-01-01T20:00:00Z.
<b>SignatureVersion</b>	String	Yes	The version of the signature encryption algorithm. Set the value to 1.0.
<b>SignatureNonce</b>	String	Yes	A unique, random number used to prevent replay attacks.  You must use different numbers for different requests.



Parameter	Type	Required	Description
<b>ResourceOwnerAccount</b>	String	No	The owner account (the logon username) of the resource that you want to access by using this API request.

#### Sample requests

```
http://ddoscoo.cn-hangzhou.aliyuncs.com/?Action=DescribeInstanceIds
&RegionId=cn-hangzhou
&TimeStamp=2020-01-01T20%3A00%3A00Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2020-01-01
&SignatureVersion=1.0
&Signature=Signature
```

#### Common response parameters

API responses use the HTTP response format. Responses can be returned in either the JSON or XML format. You can specify the response format in the request. The default response format is JSON. Every response returns a unique **RequestId** regardless of whether the call is successful.

- A 2xx status code indicates a successful call.
- A 4xx or 5xx status code indicates a failed call.

#### Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
  <!--Result Root Node-->
  <Interface Name+Response>
    <!--Return Request Tag-->
    <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
    <!--Return Result Data-->
  </Interface Name+Response>
```

- JSON format

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
  /*Return Result Data*/
}
```

```
}
```

## 12.5 Obtain an AccessKey pair

This topic describes how to create an AccessKey pair for your Alibaba Cloud account or RAM user. When you call the Anti-DDoS Pro or Anti-DDoS Premium API, you must use the AccessKey pair to complete identity verification.

### Context

An AccessKey pair consists of an AccessKey ID and an AccessKey secret.

- The AccessKey ID is used to verify the identity of the user.
- The AccessKey secret is used to encrypt and verify the signature string. You must keep your AccessKey secret strictly confidential.




#### Warning:

If the AccessKey pair of your Alibaba Cloud account is disclosed, the security of your resources will be threatened. We recommend that you use a RAM user to call API operations. This minimizes the possibility of disclosing the AccessKey pair of your Alibaba Cloud account.

### Procedure

1. Log on to [Alibaba Cloud console](#) by using your Alibaba Cloud account.
2. Move the pointer over your account avatar in the upper-right corner and click **AccessKey**.
3. In the **Security Tips** message, click Continue to manage AccessKey or Get Started with Sub Users's AccessKey as required.

#### Security Tips



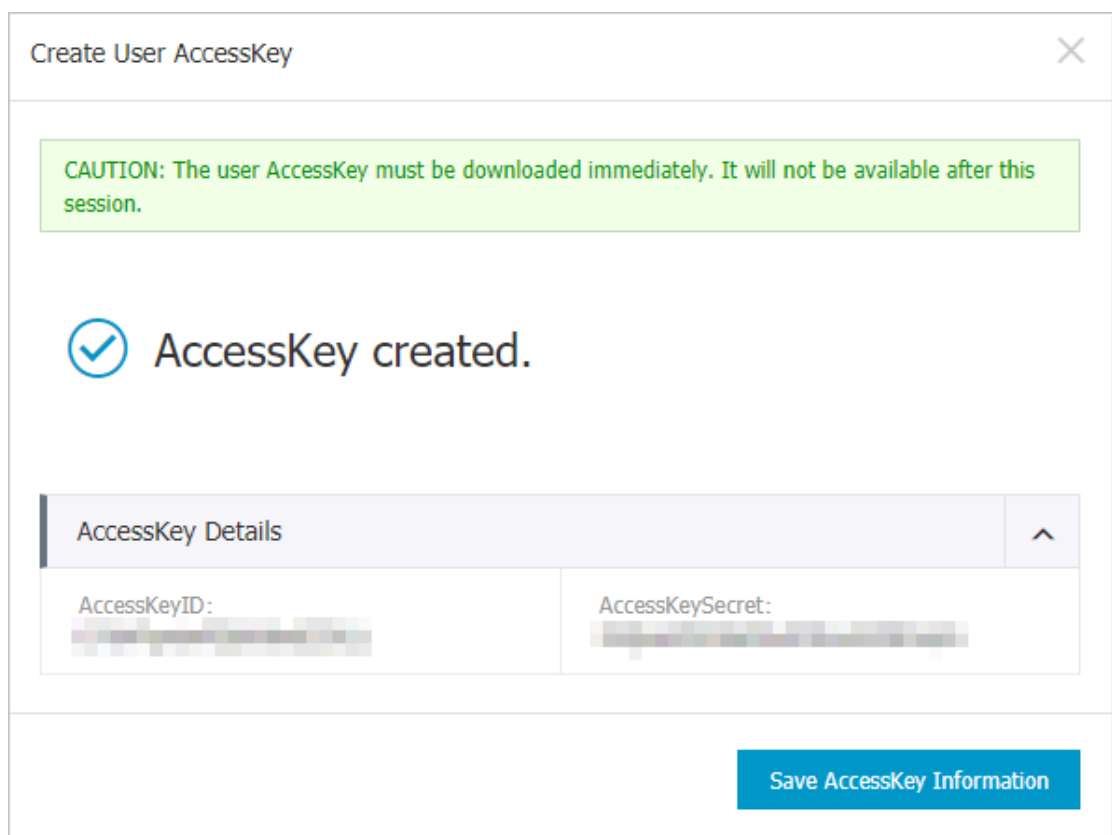
AccessKey of your cloud account is the secret key to access Alibaba Cloud APIs. Since the AccessKey has full permissions of your cloud account, please make sure you keep it well. To avoid the AccessKey being used by others to cause [Sensitive information leakage](#), do not release your AccessKey to any external channels (for example, Github). We strongly recommend you use the AccessKeys of RAM users in API calls, according to [Alibaba Cloud account security best practices](#).

Continue to manage AccessKey

Get Started with Sub Users's AccessKey

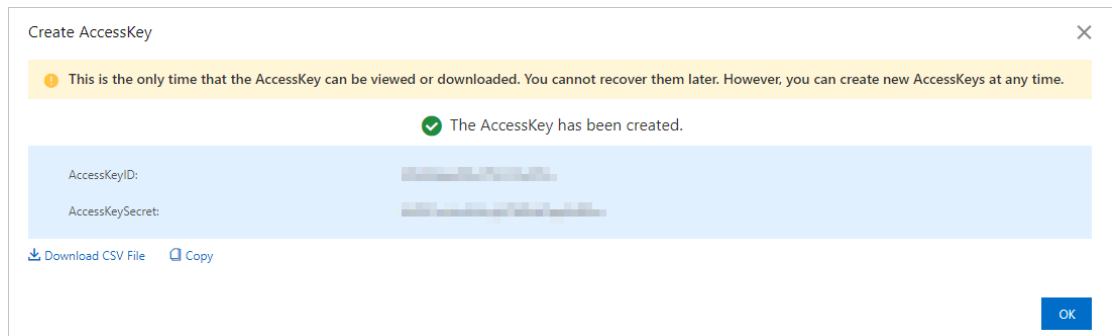
#### 4. Obtain the AccessKey pair of an account.

- Obtain the AccessKey pair of the Alibaba Cloud account
  - a. Click **Continue to manage AccessKey**.
  - b. On the **Security Management** page, click **Create AccessKey**.
  - c. In the **Phone Verification** dialog box, obtain the verification code, complete the verification process, and then click **OK**.
  - d. In the **Create User AccessKey** dialog box, show **AccessKey Details** to view the AccessKey ID and AccessKey secret. You can click **Save AccessKey Information** to download the AccessKey pair.



- Obtain the AccessKey pair of a RAM user
  - a. Click **Get Started with Sub Users's AccessKey**.
  - b. Go to the [RAM console](#) and create a RAM user on the **Create User** page. Skip this step if you want to obtain the AccessKey pair of an existing RAM user.
  - c. In the left-side navigation pane of the [RAM console](#), choose **Identities > Users**.
  - d. Find the target RAM user and click the user logon name. You are navigated to the **Authentication** tab. In the **User AccessKeys** section, click **Create AccessKey**.
  - e. In the **Phone Verification** dialog box, obtain the verification code, complete the verification process, and then click **OK**.

- f. In the **Create AccessKey** dialog box, view the AccessKey ID and AccessKey secret. You can click **Download CSV File** or **Copy** to download or copy the AccessKey pair.



## 12.6 Instances

### 12.6.1 DescribeInstanceIds

Queries the IDs of all Anti-DDoS Pro and Anti-DDoS Premium instances.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

#### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeInstanceIds	The operation that you want to perform. Set the value to <b>DescribeInstanceIds</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>Edition</b>	Integer	No	9	The mitigation plan of the instance that you want to query. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: Anti-DDoS Premium Insurance Plan</li> <li><b>1</b>: Anti-DDoS Premium Unlimited Plan</li> <li><b>2</b>: Anti-DDoS Premium MCA Plan</li> <li><b>9</b>: Anti-DDoS Pro Profession Plan</li> </ul>
<b>InstanceId.N</b>	RepeatList	No	ddoscoo-cn-mp91j1ao****	The ID of instance N.

### Response parameters

Parameter	Type	Example	Description
InstanceId	Array		The ID of an instance.
Edition	Integer	9	The mitigation plan of the instance. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: Anti-DDoS Premium Insurance Plan</li> <li><b>1</b>: Anti-DDoS Premium Unlimited Plan</li> <li><b>2</b>: Anti-DDoS Premium MCA Plan</li> <li><b>9</b>: Anti-DDoS Pro Profession Plan</li> </ul>

Parameter	Type	Example	Description
InstanceId	String	ddoscoo-cn-v0h12g3z****	The ID of the instance.
Remark	String	test	The description of the instance.
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeInstanceIds
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeInstanceIdsResponse>
  <InstanceIds>
    <InstanceId>ddoscoo-cn-v0h12g3z****</InstanceId>
    <Edition>9</Edition>
    <Remark>test</Remark>
  </InstanceIds>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeInstanceIdsResponse>
```

#### JSON format

```
{
  "InstanceIds": [{
    "InstanceId": "ddoscoo-cn-v0h12g3z****",
    "Edition": 9,
    "Remark": "test"
  }],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.6.2 DescribeInstances


Queries the versions and status information of one or more Anti-DDoS Pro or Anti-DDoS Premium instances, such as traffic forwarding status, expiration status, and overdue payment status.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.



### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeInstances	The operation that you want to perform. Set the value to <b>DescribeInstances</b> .
<b>PageNumber</b>	String	Yes	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .
<b>PageSize</b>	String	Yes	10	The number of entries to return on each page. Maximum value: <b>50</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>InstanceId.N</b>	RepeatList	No	ddoscoo-cn-mp91j1ao****	<p>The ID of instance N.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.         </div>
<b>Ip</b>	String	No	203.***.***.117	The IP address of the instance that you want to query. Exact match is supported.
<b>Remark</b>	String	No	test	The description of the instance that you want to query. Fuzzy match is supported.
<b>Edition</b>	Integer	No	9	<p>The mitigation plan of the instance that you want to query.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>0</b>: Anti-DDoS Premium Insurance Plan</li> <li><b>1</b>: Anti-DDoS Premium Unlimited Plan</li> <li><b>2</b>: Anti-DDoS Premium MCA Plan</li> <li><b>9</b>: Anti-DDoS Pro Prefession Plan</li> </ul>



Parameter	Type	Required	Example	Description
<b>Enabled</b>	Integer	No	1	The traffic forwarding status of the instance that you want to query. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: The instance stops traffic forwarding.</li> <li><b>1</b>: The instance forwards traffic properly.</li> </ul>
<b>ExpireStartTime</b>	Long	No	1584460800000	The beginning of the expiration time range that you want to query. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
<b>ExpireEndTime</b>	Long	No	1584560800000	The end of the expiration time range that you want to query. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
<b>Status.N</b>	RepeatList	No	1	The expiration status N of the instance that you want to query. Valid values: <ul style="list-style-type: none"> <li><b>1</b>: The instance works properly.</li> <li><b>2</b>: The instance expires.</li> </ul>

Parameter	Type	Required	Example	Description
<b>Tag.N.Key</b>	String	No	testkey	<p>The key of tag N of the instance that you want to query.</p> <div>  <b>Note:</b>            The tag key (<b>Tag.N.Key</b>) must match the tag value (<b>Tag.N.Value</b>).         </div>
<b>Tag.N.Value</b>	String	No	a	<p>The value of tag N of the instance that you want to query.</p> <div>  <b>Note:</b>            The tag key (<b>Tag.N.Key</b>) must match the tag value (<b>Tag.N.Value</b>).         </div>

### Response parameters

Parameter	Type	Example	Description
Instances	Array		The version and status information of an instance.
CreateTime	Long	1581946582000	The time when the instance was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
DebtStatus	Integer	0	The status of overdue payments under the instance. The value is <b>0</b> . Instances do not have overdue payments because Anti-DDoS Pro and Anti-DDoS Premium only support the subscription billing method.

Parameter	Type	Example	Description
Edition	Integer	9	The mitigation plan of the instance. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: Anti-DDoS Premium Insurance Plan</li> <li><b>1</b>: Anti-DDoS Premium Unlimited Plan</li> <li><b>2</b>: Anti-DDoS Premium MCA Plan</li> <li><b>9</b>: Anti-DDoS Pro Profession Plan</li> </ul>
Enabled	Integer	1	The traffic forwarding status of the instance. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: The instance stops traffic forwarding.</li> <li><b>1</b>: The instance forwards traffic properly.</li> </ul>
ExpireTime	Long	1584460800000	The expiration time of the instance . This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
InstanceId	String	ddoscoo-cn-mp91j1ao****	The ID of the instance.
Remark	String	test	The description of the instance.
Status	Integer	1	The expiration status of the instance. Valid values: <ul style="list-style-type: none"> <li><b>1</b>: The instance works properly.</li> <li><b>2</b>: The instance expires.</li> </ul>
RequestId	String	A09C1F98-4CC1-4A31-B8F3-9E4B7437189F	The ID of the request.
TotalCount	Long	1	The total number of returned instances.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeInstances
&PageNumber=1
&PageSize=10
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeInstancesResponse>
  <Instances>
    <Status>1</Status>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <CreateTime>1581946582000</CreateTime>
    <Enabled>1</Enabled>
    <ExpireTime>1584460800000</ExpireTime>
    <Edition>9</Edition>
    <Remark>test</Remark>
    <DebtStatus>0</DebtStatus>
  </Instances>
  <TotalCount>1</TotalCount>
  <RequestId>A09C1F98-4CC1-4A31-B8F3-9E4B7437189F</RequestId>
</DescribeInstancesResponse>
```

#### JSON format

```
{
  "Instances": [
    {
      "Status": 1,
      "InstanceId": "ddoscoo-cn-mp91j1ao****",
      "CreateTime": 1581946582000,
      "Enabled": 1,
      "ExpireTime": 1584460800000,
      "Edition": 9,
      "Remark": "test",
      "DebtStatus": 0
    }
  ],
  "TotalCount": 1,
  "RequestId": "A09C1F98-4CC1-4A31-B8F3-9E4B7437189F"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.6.3 DescribeInstanceDetails

Queries the IP addresses and Internet service provider (ISP) lines of instances.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeInstanceDetails	The operation that you want to perform. Set the value to <b>DescribeInstanceDetails</b> .
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N.  <b>Note:</b> You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.
<b>RegionId</b>	String	No	cn-hangzhou	The ID of the region where your service is deployed. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
InstanceDetails	Array		The IP address and ISP line information of the instance.

Parameter	Type	Example	Description
EipInfos	Array		Details about the IP address of the instance.
Eip	String	203.***. **.117	The IP address of the instance.
Status	String	normal	The status of the IP address. Valid values: <ul style="list-style-type: none"> <li>• <b>normal</b>: The IP address is normal.</li> <li>• <b>cleaning</b>: The traffic to the IP address is being scrubbed.</li> <li>• <b>blackhole</b>: The traffic to the IP address is routed to a black hole.</li> </ul>
InstanceId	String	ddoscoo-cn-mp91j1ao****	The ID of the instance.
Line	String	coop-line-001	The ISP line of the instance.
RequestId	String	3C814429-21A5-4673-827E-FDD19DC75681	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeInstanceDetails
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeInstanceDetailsResponse>
  <InstanceDetails>
    <Line>coop-line-001</Line>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <EipInfos>
      <Status>normal</Status>
      <Eip>203. ***. **.117</Eip>
    </EipInfos>
  </InstanceDetails>
  <RequestId>3C814429-21A5-4673-827E-FDD19DC75681</RequestId>
```

```
</DescribeInstanceDetailsResponse>
```

JSON format

```
{
  "InstanceDetails": [
    {
      "Line": "coop-line-001",
      "InstanceId": "ddoscoo-cn-mp91j1ao****",
      "EipInfos": [
        {
          "Status": "normal",
          "Eip": "203. ***. **.117"
        }
      ]
    }
  ],
  "RequestId": "3C814429-21A5-4673-827E-FDD19DC75681"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.6.4 DescribeInstanceSpecs

Queries the specifications of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.

### Debugging


OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeInstanceSpecs	The operation that you want to perform. Set the value to <b>DescribeInstanceSpecs</b> .
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N. <div> <b>Note:</b> You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.</div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

### Response parameters

Parameter	Type	Example	Description
InstanceSpecs	Array		The specifications of the instance.
BandwidthMbps	Integer	100	The clean bandwidth of the instance. Unit: Mbit/s.
BaseBandwidth	Integer	30	The basic protection bandwidth of the instance. Unit: Gbit/s.
DefenseCount	Integer	1	<p>The number of available advanced mitigation sessions for this month.- <b>1</b> indicates there is no limit on the number of available advanced mitigation sessions. That is, the instance uses the Unlimited mitigation plan.</p> <div>  <b>Note:</b>            This parameter is returned only if Anti-DDoS Premium instances are queried.         </div>
DomainLimit	Integer	50	The number of domain names that the instance can protect.



Parameter	Type	Example	Description
ElasticBandwidth	Integer	30	The brustable protection bandwidth of the instance. Unit: Gbit/s.
FunctionVersion	String	default	The function plan of the instance. Valid values: <ul style="list-style-type: none"> <li><b>default</b>: standard function plan</li> <li><b>enhance</b>: enhanced function plan</li> </ul>
InstanceId	String	ddoscoo-cn-mp91j1ao****	The ID of the instance.
PortLimit	Integer	50	The number of ports that the instance can protect.
QpsLimit	Integer	3000	The queries per second (QPS) of services.
SiteLimit	Integer	5	The number of websites that the instance can protect.
RequestId	String	23B0245A-0CCC-4637-A8C6-7CA0479395B2	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeInstanceSpecs
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeInstanceSpecsResponse>
  <RequestId>23B0245A-0CCC-4637-A8C6-7CA0479395B2</RequestId>
  <InstanceSpecs>
    <QpsLimit>3000</QpsLimit>
    <BaseBandwidth>30</BaseBandwidth>
    <PortLimit>50</PortLimit>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <DomainLimit>50</DomainLimit>
    <FunctionVersion>default</FunctionVersion>
    <ElasticBandwidth>30</ElasticBandwidth>
```

```
<SiteLimit>5</SiteLimit>
<BandwidthMbps>100</BandwidthMbps>
</InstanceSpecs>
</DescribeInstanceSpecsResponse>
```

JSON format

```
{
  "RequestId": "23B0245A-0CCC-4637-A8C6-7CA0479395B2",
  "InstanceSpecs": [
    {
      "QpsLimit": 3000,
      "BaseBandwidth": 30,
      "PortLimit": 50,
      "InstanceId": "ddoscoo-cn-mp91j1ao****",
      "DomainLimit": 50,
      "FunctionVersion": "default",
      "ElasticBandwidth": 30,
      "SiteLimit": 5,
      "BandwidthMbps": 100
    }
  ]
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.6.5 DescribeInstanceStatistics


Queries the statistics on one or more Anti-DDoS Pro or Anti-DDoS Premium instances, such as the numbers of protected domain names and ports.

### Debugging


OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeInstanceStatistics	The operation that you want to perform. Set the value to <b>DescribeInstanceStatistics</b> .

Parameter	Type	Required	Example	Description
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	<p>The ID of instance N.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

### Response parameters

Parameter	Type	Example	Description
InstanceStatistics	Array		The statistical information of the instance.
DefenseCountUsage	Integer	1	<p>The number of advanced mitigation sessions used in this month.</p> <div>  <b>Note:</b>            This parameter is returned only if Anti-DDoS Premium instances are queried.         </div>
DomainUsage	Integer	1	The number of domain names protected by the instance.
InstanceId	String	ddoscoo-cn-mp91j1ao****	The ID of the instance.
PortUsage	Integer	2	The number of ports protected by the instance.

Parameter	Type	Example	Description
SiteUsage	Integer	1	The number of websites protected by the instance.
RequestId	String	642319A9-D1F2-4459-A447-E57CFC599FDE	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeInstanceStatistics
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeInstanceStatisticsResponse>
  <InstanceStatistics>
    <PortUsage>2</PortUsage>
    <SiteUsage>1</SiteUsage>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <DomainUsage>1</DomainUsage>
  </InstanceStatistics>
  <RequestId>642319A9-D1F2-4459-A447-E57CFC599FDE</RequestId>
</DescribeInstanceStatisticsResponse>
```

#### JSON format

```
{
  "InstanceStatistics": [
    {
      "PortUsage": 2,
      "SiteUsage": 1,
      "InstanceId": "ddoscoo-cn-mp91j1ao****",
      "DomainUsage": 1
    }
  ],
  "RequestId": "642319A9-D1F2-4459-A447-E57CFC599FDE"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.6.6 ModifyInstanceRemark

Modifies the description of an Anti-DDoS Pro or Anti-DDoS Premium instance.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyInstanceRemark	The operation that you want to perform. Set the value to <b>ModifyInstanceRemark</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>InstanceId</b>	String	No	ddoscoo-cn-mp91j1ao****	The ID of the instance.  <b>Note:</b> You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.
<b>Remark</b>	String	No	new-remark	The description that you want to use for the instance.

## Response parameters

Parameter	Type	Example	Description
RequestId	String	7EFA2BA6-9C0A-4410-B735-FC337EB634A1	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyInstanceRemark
&InstanceId=ddoscoo-cn-mp91j1ao****
&Remark=new-remark
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<ModifyInstanceRemarkResponse>
  <RequestId>7EFA2BA6-9C0A-4410-B735-FC337EB634A1</RequestId>
</ModifyInstanceRemarkResponse>
```

#### JSON format

```
{
  "RequestId": "7EFA2BA6-9C0A-4410-B735-FC337EB634A1"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.6.7 DescribeElasticBandwidthSpec

Queries the available burstable protection bandwidth of an Anti-DDoS Pro instance.




### Note:

This API operation is suitable only for Anti-DDoS Pro.

## Debugging

[OpenAPI Explorer](#) automatically calculates the signature value. For your convenience, we recommend that you call this operation in [OpenAPI Explorer](#). [OpenAPI Explorer](#) dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeElasticBandwidthSpec	The operation that you want to perform. Set the value to <b>DescribeElasticBandwidthSpec</b> .
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance.  <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Set the value to <b>cn-hangzhou</b> , which indicates an Anti-DDoS Pro instance.

## Response parameters

Parameter	Type	Example	Description
ElasticBandwidthSpec	List	[5,10,20,30]	The available burstable protection bandwidth. Unit: Gbit/s.
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeElasticBandwidthSpec
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeElasticBandwidthSpecResponse>
  <ElasticBandwidthSpec>5</ElasticBandwidthSpec>
  <ElasticBandwidthSpec>10</ElasticBandwidthSpec>
```

```
<ElasticBandwidthSpec>20</ElasticBandwidthSpec>
<ElasticBandwidthSpec>30</ElasticBandwidthSpec>
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeElasticBandwidthSpecResponse>
```

JSON format

```
{
  "ElasticBandwidthSpec": [
    5,
    10,
    20,
    30
  ],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.6.8 ModifyElasticBandWidth

Modifies the burstable protection bandwidth of an Anti-DDoS Pro instance.



### Note:

This API operation is suitable only for Anti-DDoS Pro.



### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyElasticBandWidth	The operation that you want to perform. Set the value to <b>ModifyElasticBandWidth</b> .



Parameter	Type	Required	Example	Description
<b>ElasticBandwidth</b>	Integer	Yes	50	<p>The burstable protection bandwidth that you want to modify. Unit: Gbit/s.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeElasticBandwidthSpec</a> operation to query the available burstable protection bandwidth of the Anti-DDoS Pro instance.         </div>
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	<p>The ID of the instance.</p> <div>  <b>Note:</b>            The instance must be in the normal status. You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Set the value to <b>cn-hangzhou</b>, which indicates an Anti-DDoS Pro instance.</p>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=ModifyElasticBandWidth
&ElasticBandwidth=50
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<ModifyElasticBandWidthResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyElasticBandWidthResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

#### Error codes

For a list of error codes, visit the [API Error Center](#).

### 12.6.9 DescribeDefenseCountStatistics

Queries the information of mitigation sessions of an Anti-DDoS Premium instance, such as the numbers of available and used advanced mitigation sessions.

**Note:**

This API operation is suitable only for Anti-DDoS Premium.

#### Debugging


[OpenAPI Explorer](#) automatically calculates the signature value. For your convenience, we recommend that you call this operation in [OpenAPI Explorer](#). [OpenAPI Explorer](#) dynamically generates the sample code of the operation for different SDKs.

#### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDefenseCountStatistics	The operation that you want to perform. Set the value to <b>DescribeDefenseCountStatistics</b> .
<b>RegionId</b>	String	No	ap-southeast-1	The region ID of the instance. Set the value to <b>ap-southeast-1</b> , which indicates an Anti-DDoS Premium instance.

Parameter	Type	Required	Example	Description
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
DefenseCountStatistics	Struct		Details about mitigation sessions.
DefenseCountTotalUsageOfCurrentMonth	Integer	1	The number of advanced mitigation sessions used in this month.
FlowPackCountRemain	Integer	1	The number of available mitigation sessions to protect against a DDoS attack.  <div>  <b>Note:</b>            These mitigation sessions are provided for free if you activate Anti-DDoS Premium for the first time, which can protect against a DDoS attack for once.         </div>
MaxUsableDefenseCountCurrentMonth	Integer	2	The number of available advanced mitigation sessions for this month.
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDefenseCountStatistics
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeDefenseCountStatisticsResponse>
  <DefenseCountStatistics>
    <DefenseCountTotalUsageOfCurrentMonth>1</DefenseCountTotalUsageOfCurrentMonth>
    <FlowPackCountRemain>1</FlowPackCountRemain>
    <MaxUsableDefenseCountCurrentMonth>2</MaxUsableDefenseCountCurrentMonth>
  </DefenseCountStatistics>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeDefenseCountStatisticsResponse>
```

#### JSON format

```
{
  "DefenseCountStatistics": {
    "DefenseCountTotalUsageOfCurrentMonth": 1,
    "FlowPackCountRemain": 1,
    "MaxUsableDefenseCountCurrentMonth": 2
  },
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.7 Website configuration


### 12.7.1 DescribeDomains

Queries domain names for which forwarding rules are created.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomains	The operation that you want to perform. Set the value to <b>DescribeDomains</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>InstanceIds.N</b>	RepeatList	No	ddoscoo-cn-mp91j1ao****	The ID of instance N. <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>

## Response parameters

Parameter	Type	Example	Description
Domains	List	["www.aliyun.com"]	The domain names.

Parameter	Type	Example	Description
RequestId	String	F908E959-ADA8-4D7B-8A05-FF2F67F50964	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDomains
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeDomainsResponse>
  <Domains>www.aliyun.com</Domains>
  <RequestId>F908E959-ADA8-4D7B-8A05-FF2F67F50964</RequestId>
</DescribeDomainsResponse>
```

#### JSON format

```
{
  "Domains": [
    "www.aliyun.com"
  ],
  "RequestId": "F908E959-ADA8-4D7B-8A05-FF2F67F50964"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.7.2 DescribeWebRules


Queries the forwarding rules of a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebRules	The operation that you want to perform. Set the value to <b>DescribeWebRules</b> .
<b>PageSize</b>	Integer	Yes	10	The number of entries to return on each page. Maximum value: <b>10</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>Domain</b>	String	No	www.aliyun.com	The domain name of the website. <div>  <b>Note:</b>  A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names. </div>

Parameter	Type	Required	Example	Description
<b>QueryDomainPattern</b>	String	No	fuzzy	The matching mode. Valid values : <ul style="list-style-type: none"> <li>• <b>fuzzy</b>: fuzzy match, which is selected by default</li> <li>• <b>exact</b>: exact match</li> </ul>
<b>PageNumber</b>	Integer	No	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .
<b>InstanceIds.N</b>	RepeatList	No	ddoscoo-cn-mp91j1ao****	The ID of instance N. <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	89E69DD6-C5DD-4636-9AD6-CCF6BEAB59AC	The ID of the request.
TotalCount	Long	1	The total number of returned forwarding rules.
WebRules	Array		Details about a forwarding rule.
BlackList	List	[1. ***. ***.1]	The IP addresses in the blacklist for a domain name.
CcEnabled	Boolean	true	Indicates whether the Frequency Control policy is enabled. Valid values : <ul style="list-style-type: none"> <li>• <b>true</b></li> <li>• <b>false</b></li> </ul>



Parameter	Type	Example	Description
CcRuleEnabled	Boolean	false	Indicates whether the Custom Rule switch of the Frequency Control policy is turned on. Valid values: <ul style="list-style-type: none"> <li><b>true</b></li> <li><b>false</b></li> </ul>
CcTemplate	String	default	The mode of the Frequency Control policy. Valid values: <ul style="list-style-type: none"> <li><b>default</b>: Normal</li> <li><b>gf_under_attack</b>: Emergency</li> <li><b>gf_sos_verify</b>: Strict</li> <li><b>gf_sos_enhance</b>: Super Strict</li> </ul>
CertName	String	testcert	The name of the SSL certificate.
Cname	String	64687s1jf898****.aliyunddos0001.com	The CNAME record of the forwarding rule.
Domain	String	www.aliyun.com	The domain name of the website.
Http2Enable	Boolean	true	Indicates whether HTTP/2 is enabled. Valid values: <ul style="list-style-type: none"> <li><b>true</b></li> <li><b>false</b></li> </ul>
ProxyTypes	Array		Details about the protocol.
ProxyPorts	List	80	The port of the origin server.
ProxyType	String	http	The type of the protocol. Valid values: <ul style="list-style-type: none"> <li><b>http</b></li> <li><b>https</b></li> <li><b>websocket</b></li> <li><b>websockets</b></li> </ul>
RealServers	Array		Details about the address of the origin server.

Parameter	Type	Example	Description
RealServer	String	1.***.***.1	The address of the origin server.
RsType	Integer	0	The address type of the origin server. Valid values: <ul style="list-style-type: none"> <li>• <b>0</b>: IP address</li> <li>• <b>1</b>: domain name</li> </ul>
SslCiphers	String	default	The type of the cipher suite. Valid values: <ul style="list-style-type: none"> <li>• <b>default</b>: default cipher suites, which only include strong cipher suites</li> <li>• <b>all</b>: all cipher suites, which include strong and weak cipher suites</li> <li>• <b>strong</b>: strong cipher suites</li> </ul>
SslProtocols	String	tls1.0	The version of the TLS protocol. Valid values: <ul style="list-style-type: none"> <li>• <b>tls1.0</b>: TLS 1.0 or later</li> <li>• <b>tls1.1</b>: TLS 1.1 or later</li> <li>• <b>tls1.2</b>: TLS 1.2 or later</li> </ul>
WhiteList	List	[1.***.***.1]	The IP addresses in the whitelist for a domain name.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeWebRules
&PageSize=10
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeWebRulesResponse>
  <TotalCount>1</TotalCount>
  <WebRules>
    <CcEnabled>true</CcEnabled>
    <SslProtocols>tls1.0</SslProtocols>
    <ProxyTypes>
```

```

        <ProxyPorts>443</ProxyPorts>
        <ProxyType>https</ProxyType>
    </ProxyTypes>
    <ProxyTypes>
        <ProxyPorts>80</ProxyPorts>
        <ProxyType>http</ProxyType>
    </ProxyTypes>
    <RealServers>
        <RealServer>1. ***. ***.1</RealServer>
        <RsType>0</RsType>
    </RealServers>
    <CcRuleEnabled>>false</CcRuleEnabled>
    <SslCiphers>default</SslCiphers>
    <CertName></CertName>
    <Domain>www.aliyun.com</Domain>
    <Http2Enable>>false</Http2Enable>
    <Cname>64687s1jf898****.aliyunddos0001.com</Cname>
    <CcTemplate>default</CcTemplate>
</WebRules>
<RequestId>89E69DD6-C5DD-4636-9AD6-CCF6BEAB59AC</RequestId>
</DescribeWebRulesResponse>

```

### JSON format

```

{
  "TotalCount": 1,
  "WebRules": [
    {
      "CcEnabled": true,
      "SslProtocols": "tls1.0",
      "ProxyTypes": [
        {
          "ProxyPorts": [
            443
          ],
          "ProxyType": "https"
        },
        {
          "ProxyPorts": [
            80
          ],
          "ProxyType": "http"
        }
      ],
      "RealServers": [
        {
          "RealServer": "1. ***. ***.1",
          "RsType": 0
        }
      ],
      "CcRuleEnabled": false,
      "SslCiphers": "default",
      "CertName": "",
      "Domain": "www.aliyun.com",
      "Http2Enable": false,
      "Cname": "64687s1jf898****.aliyunddos0001.com",
      "CcTemplate": "default"
    }
  ],
  "RequestId": "89E69DD6-C5DD-4636-9AD6-CCF6BEAB59AC"
}

```

```
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.7.3 CreateWebRule

Creates a forwarding rule for a website.


## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	CreateWebRule	The operation that you want to perform. Set the value to <b>CreateWebRule</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.
<b>RsType</b>	Integer	Yes	0	The address type of the origin server. Valid values: <ul style="list-style-type: none"><li><b>0</b>: IP address</li><li><b>1</b>: domain name</li></ul>

Parameter	Type	Required	Example	Description
<b>Rules</b>	String	Yes	<pre>[{"ProxyRules": [{"ProxyPort": 80, "RealServers": ["1.1.1.1"]}], "ProxyType": "http"}, {"ProxyRules": [{"ProxyPort": 443, "RealServers": ["1.1.1.1"]}], "ProxyType": "https"}]</pre>	<p>Details about the forwarding rule. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>ProxyRules</b>: the protocol information. This field is required and must be of the ARRAY type. <ul style="list-style-type: none"> <li>- <b>ProxyPort</b>: the port number. It is required and must be of the INTEGER type.</li> <li>- <b>RealServers</b>: the address of the origin server. It is required and must be of the ARRAY type.</li> </ul> </li> <li>• <b>ProxyType</b>: the protocol type. It is required and must be of the STRING type. Valid values: <ul style="list-style-type: none"> <li>- <b>http</b></li> <li>- <b>https</b></li> <li>- <b>websocket</b></li> <li>- <b>websockets</b></li> </ul> </li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>InstanceIds.N</b>	RepeatList	No	ddoscoo-cn-mp91j1ao****	The ID of instance N. If this parameter is not specified, only a domain name is added but no instance is associated with the website.  <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=CreateWebRule
&Domain=www.aliyun.com
&RsType=0
&Rules=[{"ProxyRules":[{"ProxyPort":80,"RealServers":["1.1.1.1"]},"ProxyType":"http"},{"ProxyRules":[{"ProxyPort":443,"RealServers":["1.1.1.1"]},"ProxyType":"https"}]
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<CreateWebRuleResponse>
```

```
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</CreateWebRuleResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.7.4 ModifyWebRule

Modifies the forwarding rule of a website.

### Debugging


OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebRule	The operation that you want to perform. Set the value to <b>ModifyWebRule</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RealServers.N</b>	RepeatList	Yes	1.1.1.1	The address of origin server N.
<b>RsType</b>	Integer	Yes	0	The address type of the origin server. Valid values: <ul style="list-style-type: none"><li><b>0</b>: IP address</li><li><b>1</b>: domain name</li></ul>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>
<b>ProxyTypes</b>	String	No	<pre>[{"ProxyType": "http", "ProxyPorts": [80]}, {"ProxyType": "https", "ProxyPorts": [443]}</pre>	<p>The protocol of the forwarding rule that you want to modify. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li><b>ProxyType</b>: the protocol type. This field is required and must be of the STRING type. Valid values: <ul style="list-style-type: none"> <li><b>http</b></li> <li><b>https</b></li> <li><b>websocket</b></li> <li><b>websockets</b></li> </ul> </li> <li><b>ProxyPort</b>: the port number. This field is required and must be of the INTEGER type.</li> </ul>



Parameter	Type	Required	Example	Description
<b>InstanceIds.N</b>	RepeatList	No	ddoscoo-cn-mp91j1ao****	<p>The ID of instance N that you want to associate the domain name with. If this parameter is not specified, a domain name is only added but not associated with an instance.</p> <div> <b>Note:</b> You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.</div>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=ModifyWebRule
&Domain=www.aliyun.com
&RealServers.1=1.1.1.1
&RsType=0
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ModifyWebRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyWebRuleResponse>
```

##### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
```

```
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.7.5 DeleteWebRule

Deletes the forwarding rule of a website.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteWebRule	The operation that you want to perform. Set the value to <b>DeleteWebRule</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=DeleteWebRule
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<DeleteWebRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteWebRuleResponse>
```

##### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.7.6 DescribeWebInstanceRelations

Queries the information of the Anti-DDoS Pro or Anti-DDoS Premium instances that are associated with websites.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebInstanceRelations	The operation that you want to perform. Set the value to <b>DescribeWebInstanceRelations</b> .
<b>Domains.N</b>	RepeatList	Yes	www.aliyun.com	The domain name of website N.   <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0222382B-5FE5-4FF7-BC9B-97EE31D58818	The ID of the request.
WebInstanceRelations	Array		Details about the instances that are associated with the website.
Domain	String	www.aliyun.com	The domain name of the website.
InstanceDetails	Array		Details about an instance that is associated with the website.
EipList	List	203.***.***.158	The IP addresses of the instance.
FunctionVersion	String	enhance	The function plan of the instance. Valid values: <ul style="list-style-type: none"><li><b>default</b>: standard function plan</li><li><b>enhance</b>: enhanced function plan</li></ul>
InstanceId	String	ddoscoo-cn-0pp163pd****	The ID of the instance.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeWebInstanceRelations
&Domains.1=www.aliyun.com
```

### &<Common request parameters>

#### Sample success responses

##### XML format

```
<DescribeWebInstanceRelationsResponse>
  <RequestId>0222382B-5FE5-4FF7-BC9B-97EE31D58818</RequestId>
  <WebInstanceRelations>
    <InstanceDetails>
      <EipList>203. ***. ***.158</EipList>
      <InstanceId>ddoscoo-cn-0pp163pd****</InstanceId>
      <FunctionVersion>enhance</FunctionVersion>
    </InstanceDetails>
    <InstanceDetails>
      <EipList>203. ***. ***.38</EipList>
      <InstanceId>ddoscoo-cn-45917cd3****</InstanceId>
      <FunctionVersion>enhance</FunctionVersion>
    </InstanceDetails>
    <Domain>www.aliyun.com</Domain>
  </WebInstanceRelations>
</DescribeWebInstanceRelationsResponse>
```

##### JSON format

```
{
  "RequestId": "0222382B-5FE5-4FF7-BC9B-97EE31D58818",
  "WebInstanceRelations": [
    {
      "InstanceDetails": [
        {
          "EipList": [
            "203. ***. ***.158"
          ],
          "InstanceId": "ddoscoo-cn-0pp163pd****",
          "FunctionVersion": "enhance"
        },
        {
          "EipList": [
            "203. ***. ***.38"
          ],
          "InstanceId": "ddoscoo-cn-45917cd3****",
          "FunctionVersion": "enhance"
        }
      ],
      "Domain": "www.aliyun.com"
    }
  ]
}
```

#### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.7.7 DescribeCerts


Queries the certificate information of a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeCerts	The operation that you want to perform. Set the value to <b>DescribeCerts</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

Parameter	Type	Required	Example	Description
<b>Domain</b>	String	No	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>

### Response parameters

Parameter	Type	Example	Description
Certs	Array		The certificate information of the website.
Common	String	www.aliyun.com	The domain name associated with the certificate.
DomainRelated	Boolean	true	<p>Indicates whether the certificate is associated with the domain name.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>true</b></li> <li><b>false</b></li> </ul>
EndDate	String	2021-09-12	The expiration date of the certificate. This value is of the STRING type.
Id	Integer	81	The ID of the certificate.
Issuer	String	Symantec	The authority that issues the certificate.
Name	String	testcert	The name of the certificate.
StartDate	String	2019-09-12	The issuance date of the certificate. This value is of the STRING type.



Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeCerts
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeCertsResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <Certs>
    <Id>81</Id>
    <Name>testcert</Name>
    <Common>www.aliyun.com</Common>
    <DomainRelated>true</DomainRelated>
    <Issuer>Symantec</Issuer>
    <StartDate>2019-09-12</StartDate>
    <EndDate>2021-09-12</EndDate>
  </Certs>
</DescribeCertsResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "Certs": [
    {
      "Id": 81,
      "Name": "testcert",
      "Common": "www.aliyun.com",
      "DomainRelated": true,
      "Issuer": "Symantec",
      "StartDate": "2019-09-12",
      "EndDate": "2021-09-12"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.7.8 AssociateWebCert



Associates an SSL certificate with the forwarding rule of a website.


### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	AssociateWebCert	The operation that you want to perform. Set the value to <b>AssociateWebCert</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>CertId</b>	Integer	No	2404693	<p>The ID of the SSL certificate that you want to associate. If the SSL certificate that you want to associate has been issued in SSL Certificate Service, you can enter the certificate ID to associate the certificate.</p> <div>  <b>Note:</b>            If you enter the certificate ID, you do not need to specify <b>CertName</b>, <b>Cert</b>, and <b>Key</b>.         </div>
<b>CertName</b>	String	No	example-cert	<p>The name of the certificate that you want to associate. If you set this parameter, you must also specify the <b>Cert</b> and <b>Key</b> parameters.</p> <div>  <b>Note:</b>            If you specify <b>CertName</b>, <b>Cert</b>, and <b>Key</b>, you do not need to specify <b>CertId</b>.         </div>

Parameter	Type	Required	Example	Description
<b>Cert</b>	String	No	<pre> -----BEGIN CERTIFICAT E----- 62EcYPWd2O y1vs6MTXcj SfN9Z7rZ9f mxWr2BFN2X bahgnsSXM4 8ixZJ4krc+1M +j2kcubVpsE 2cgHdj4v8H 6jUz9Ji4mr 7vMNS6dXv8 PUkl/ qoDeNGCNdy TS5NIL5ir+ g92cL8IGOk jgvhlqt9vc 65Cgb4mL+n5 +DV9uOyTZTW /MojmlgfUek C2xiXa54nx Jf17Y1TADG SbyJbsC0Q9 nIrHsPl8YK kvRWvIAqYx XZ7wRwWWmv 4TMxFhWRiN Y7yZlo2ZUh l02SIDNggIEeg == -----END CERTIFICATE ----- </pre>	<p>The public key of the certificate that you want to associate. If you set this parameter, you must also specify the <b>CertName</b> and <b>Key</b> parameters.</p> <div>  <b>Note:</b>            If you specify <b>CertName</b>, <b>Cert</b>, and <b>Key</b>, you do not need to specify <b>CertId</b>.         </div>

Parameter	Type	Required	Example	Description
<b>Key</b>	String	No	<pre> -----BEGIN RSA PRIVATE KEY----- DADTPZoOHd 9WtZ3UKHJT RgNQmioPQn 2bqdKHop+B/ dn/4VZL7Jt8zS DGM9sTMThL yvsmLQKBgQ Cr+ujntC1kN6p GBj2Fw2l/EA /W3rYEce2ty hjgmG7rZ+A /jVE9fld5sQ ra6ZdwBcQJ aiygoIYoam F2EjRwc0qw Haluq0C15f 6ujSoHh2e+ D5zdmkTg/ 3NKNjqNv6x A2gYpinVDz FdZ9Zujxvu h9o4Vqf0YF 8bv5UK5G04 RtKadOw== -----END RSA PRIVATE KEY ----- </pre>	<p>The private key of the certificate that you want to associate. If you set this parameter, you must also specify the <b>CertName</b> and <b>Cert</b> parameters.</p> <div>  <b>Note:</b>            If you specify <b>CertName</b>, <b>Cert</b>, and <b>Key</b>, you do not need to specify <b>CertId</b>.         </div>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	40F11005-A75C-4644-95F2-52A4E7D43E91	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=AssociateWebCert
&Domain=www.aliyun.com
```

```
&CertId=2404693
&<Common request parameters>
```

Sample success responses

XML format

```
<AssociateWebCertResponse>
  <RequestId>40F11005-A75C-4644-95F2-52A4E7D43E91</RequestId>
</AssociateWebCertResponse>
```

JSON format

```
{
  "RequestId": "40F11005-A75C-4644-95F2-52A4E7D43E91"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.7.9 DescribeWebCustomPorts

Queries the supported custom ports of a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebCustomPorts	The operation that you want to perform. Set the value to <b>DescribeWebCustomPorts</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.
WebCustomPorts	Array		Details about supported custom ports of a website.
ProxyPorts	List	[80,8080]	The supported custom ports.
ProxyType	String	http	The protocol of supported ports. Valid values: <ul style="list-style-type: none"><li>• <b>http</b></li><li>• <b>https</b></li></ul>

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeWebCustomPorts
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<DescribeWebCustomPortsResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <WebCustomPorts>
    <ProxyType>https</ProxyType>
    <ProxyPorts>443</ProxyPorts>
    <ProxyPorts>8443</ProxyPorts>
```

```
</WebCustomPorts>
<WebCustomPorts>
  <ProxyType>http</ProxyType>
  <ProxyPorts>80</ProxyPorts>
  <ProxyPorts>8080</ProxyPorts>
</WebCustomPorts>
</DescribeWebCustomPortsResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "WebCustomPorts": [
    {
      "ProxyType": "https",
      "ProxyPorts": [
        443,
        8443
      ]
    },
    {
      "ProxyType": "http",
      "ProxyPorts": [
        80,
        8080
      ]
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.7.10 ModifyTlsConfig

Modifies the Transport Layer Security (TLS) policy configuration for the forwarding rule of a website.


### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyTlsConfig	The operation that you want to perform. Set the value to <b>ModifyTlsConfig</b> .



Parameter	Type	Required	Example	Description
<b>Config</b>	String	Yes	<pre>{"ssl_protocols":"tls1.0", "ssl_ciphers":"all"}</pre>	<p>Details about the TLS policy. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>ssl_protocols</b>: the version of TLS. This field is required and must be of the STRING type. Valid values: <ul style="list-style-type: none"> <li>- <b>tls1.0</b>: TLS 1.0 and later</li> <li>- <b>tls1.1</b>: TLS 1.1 and later</li> <li>- <b>tls1.2</b>: TLS 1.2 and later</li> </ul> </li> <li>• <b>ssl_ciphers</b>: the type of the cipher suite. This field is required and must be of the STRING type. Valid values: <ul style="list-style-type: none"> <li>- <b>all</b>: all cipher suites, which contain strong and weak cipher suites</li> <li>- <b>strong</b>: strong cipher suites</li> <li>- <b>default</b>: default cipher suites, which contains only strong cipher suites</li> </ul> </li> </ul>
<b>Domain</b>	String	Yes	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>  A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names. </div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyTlsConfig
&Config={"ssl_protocols":"tls1.0","ssl_ciphers":"all"}
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<ModifyTlsConfigResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
```

```
</ModifyTlsConfigResponse>
```

JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.7.11 ModifyHttp2Enable

Enables or disables HTTP/2 for the forwarding rule of a website.




### Note:

This API operation is suitable only for Anti-DDoS Pro.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyHttp2Enable	The operation that you want to perform. Set the value to <b>ModifyHttp2Enable</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website. <div><b>Note:</b> A forwarding rule must be configured for the domain name, and the domain name must be protected by an Anti-DDoS Pro instance that uses the enhanced function plan. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.</div>

Parameter	Type	Required	Example	Description
<b>Enable</b>	Integer	Yes	1	Specifies whether to enable HTTP/2. Valid values: <ul style="list-style-type: none"><li>• <b>0</b>: disables HTTP/2.</li><li>• <b>1</b>: enables HTTP/2.</li></ul>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Set the value to <b>cn-hangzhou</b> , which indicates an Anti-DDoS Pro instance.
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyHttp2Enable
&Domain=www.aliyun.com
&Enable=1
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<ModifyHttp2EnableResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
```

```
</ModifyHttp2EnableResponse>
```

JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.7.12 DescribeWebAccessMode

Queries the access mode settings of a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebAccessMode	The operation that you want to perform. Set the value to <b>DescribeWebAccessMode</b> .
<b>Domains.N</b>	RepeatList	Yes	www.aliyun.com	The domain name of website N.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
DomainModes	Array		Details about the access mode used by the website.
AccessMode	Integer	0	The access mode used by the website . Valid values: <ul style="list-style-type: none"><li>• <b>0</b>: A record</li><li>• <b>1</b>: Anti-DDoS</li><li>• <b>2</b>: Back-to-Source</li></ul>
Domain	String	www.aliyun.com	The domain name of the website.
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeWebAccessMode
&Domains.1=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<DescribeWebAccessModeResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
<DomainModes>
  <Domain>www.aliyun.com</Domain>
  <AccessMode>0</AccessMode>
</DomainModes>
</DescribeWebAccessModeResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "DomainModes": [
    {
      "Domain": "www.aliyun.com",
      "AccessMode": 0
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.7.13 ModifyWebAccessMode


Modifies the access mode settings of a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebAccessMode	The operation that you want to perform. Set the value to <b>ModifyWebAccessMode</b> .
<b>AccessMode</b>	Integer	Yes	2	The access mode that you want to set for the website. Valid values: <ul style="list-style-type: none"><li><b>0</b>: A record</li><li><b>1</b>: Anti-DDoS</li><li><b>2</b>: Back-to-Source</li></ul>

Parameter	Type	Required	Example	Description
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.   <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebAccessMode
&AccessMode=2
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<ModifyWebAccessModeResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```



```
</ModifyWebAccessModeResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.7.14 DescribeCnameReuses

Queries the CNAME reuse information of websites.




### Note:

This API operation is suitable only for Anti-DDoS Premium.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeCnameReuses	The operation that you want to perform. Set the value to <b>DescribeCnameReuses</b> .
<b>Domains.N</b>	RepeatList	Yes	www.aliyun.com	The domain name of website N. <div> <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.</div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	ap-southeast-1	The region ID of the instance. Set the value to <b>ap-southeast-1</b> , which indicates an Anti-DDoS Premium instance.
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
CnameReuses	Array		Details about CNAME reuse.
Cname	String	4o6ep6q217k9****.aliyunddos0004.com	The CNAME record reused by the website.
Domain	String	www.aliyun.com	The domain name of the website.
Enable	Integer	1	Indicates whether CNAME reuse is enabled. Valid values: <ul style="list-style-type: none"><li><b>0</b>: disabled</li><li><b>1</b>: enabled</li></ul>
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCnameReuses&Domains.1=www.aliyun.com
```

## &lt;Common request parameters&gt;

## Sample success responses

## XML format

```
<DescribeCnameReusesResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <CnameReuses>
    <Domain>www.aliyun.com</Domain>
    <Cname>4o6ep6q217k9****.aliyunddos0004.com</Cname>
    <Enable>1</Enable>
  </CnameReuses>
</DescribeCnameReusesResponse>
```

## JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "CnameReuses": [{
    "Domain": "www.aliyun.com",
    "Cname": "4o6ep6q217k9****.aliyunddos0004.com",
    "Enable": 1
  }]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.7.15 ModifyCnameReuse

Enables or disables CNAME reuse for a website.

**Note:**


This API operation is suitable only for Anti-DDoS Premium.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyCnameReuse	The operation that you want to perform. Set the value to <b>ModifyCnameReuse</b> .

Parameter	Type	Required	Example	Description
<b>Domain</b>	String	Yes	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>Enable</b>	Integer	Yes	1	<p>Specifies whether to enable CNAME reuse. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>1</b>: enables CNAME reuse.</li> <li>• <b>2</b>: disables CNAME reuse.</li> </ul>
<b>RegionId</b>	String	No	ap-southeast-1	<p>The region ID of the instance.</p> <p>Set the value to <b>ap-southeast-1</b>, which indicates an Anti-DDoS Premium instance.</p>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>
<b>Cname</b>	String	No	4o6ep6q217k9****.aliyunddos0004.com	<p>The CNAME record that you want to reuse for the website.</p>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyCnameReuse
&Domain=www.aliyun.com
&Enable=1
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<ModifyCnameReuseResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyCnameReuseResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.8 Port configuration

### 12.8.1 DescribeNetworkRules


Queries port forwarding rules.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

#### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeNetworkRules	The operation that you want to perform. Set the value to <b>DescribeNetworkRules</b> .

Parameter	Type	Required	Example	Description
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance. <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.         </div>
<b>PageNumber</b>	Integer	Yes	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .
<b>PageSize</b>	Integer	Yes	10	The number of entries to return on each page.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ForwardProtocol</b>	String	No	tcp	The forwarding protocol. Valid values: <ul style="list-style-type: none"> <li><b>tcp</b></li> <li><b>udp</b></li> </ul>
<b>FrontendPort</b>	Integer	No	80	The forwarding port.

### Response parameters

Parameter	Type	Example	Description
NetworkRules	Array		Details about a port forwarding rule.

Parameter	Type	Example	Description
BackendPort	Integer	80	The port of the origin server.
FrontendPort	Integer	80	The forwarding port.
InstanceId	String	ddoscoo-cn-mp91j1ao****	The ID of the instance.
IsAutoCreate	Boolean	true	Indicates whether the port forwarding rule is automatically created. Valid values: <ul style="list-style-type: none"><li>• <b>true</b></li><li>• <b>false</b></li></ul>
Protocol	String	tcp	The forwarding protocol. Valid values: <ul style="list-style-type: none"><li>• <b>tcp</b></li><li>• <b>udp</b></li></ul>
RealServers	List	["112. ***. ***.139"]	The IP addresses of the origin server.
RequestId	String	8597F235-FA5E-4FC7-BAD9-E4C0B01BC771	The ID of the request.
TotalCount	Long	2	The total number of returned port forwarding rules.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeNetworkRules
&InstanceId=ddoscoo-cn-mp91j1ao****
&PageNumber=1
&PageSize=10
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeNetworkRulesResponse>
  <TotalCount>2</TotalCount>
  <NetworkRules>
    <IsAutoCreate>true</IsAutoCreate>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
```

```

    <BackendPort>80</BackendPort>
    <RealServers>112. ***. ***.139</RealServers>
    <FrontendPort>80</FrontendPort>
    <Protocol>tcp</Protocol>
  </NetworkRules>
  <NetworkRules>
    <IsAutoCreate>>false</IsAutoCreate>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <BackendPort>8080</BackendPort>
    <RealServers>1.1.1.1</RealServers>
    <RealServers>2.2.2.2</RealServers>
    <RealServers>3.3.3.3</RealServers>
    <FrontendPort>8080</FrontendPort>
    <Protocol>tcp</Protocol>
  </NetworkRules>
  <RequestId>8597F235-FA5E-4FC7-BAD9-E4C0B01BC771</RequestId>
</DescribeNetworkRulesResponse>

```

### JSON format

```

{
  "TotalCount": 2,
  "NetworkRules": [
    {
      "IsAutoCreate": true,
      "InstanceId": "ddoscoo-cn-mp91j1ao****",
      "BackendPort": 80,
      "RealServers": [
        "112. ***. ***.139"
      ],
      "FrontendPort": 80,
      "Protocol": "tcp"
    },
    {
      "IsAutoCreate": false,
      "InstanceId": "ddoscoo-cn-mp91j1ao****",
      "BackendPort": 8080,
      "RealServers": [
        "1.1.1.1",
        "2.2.2.2",
        "3.3.3.3"
      ],
      "FrontendPort": 8080,
      "Protocol": "tcp"
    }
  ],
  "RequestId": "8597F235-FA5E-4FC7-BAD9-E4C0B01BC771"
}

```

### Error codes

For a list of error codes, visit the [API Error Center](#).



## 12.8.2 CreateNetworkRules

Creates a port forwarding rule.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	CreateNetworkRules	The operation that you want to perform. Set the value to <b>CreateNetworkRules</b> .
<b>NetworkRules</b>	String	Yes	[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080,"BackendPort":8080,"RealServers":["1.1.1.1","2.2.2.2"]}]	Details about the port forwarding rule. This parameter is a JSON string. The fields in the value are described as follows: <ul style="list-style-type: none"><li>• <b>InstanceId</b>: the ID of the instance. This field is required and must be of the STRING type.</li><li>• <b>Protocol</b>: the forwarding protocol. This field is required and must be of the STRING type. Valid values: <b>tcp</b> and <b>udp</b>.</li><li>• <b>FrontendPort</b>: the forwarding port. This field is required and must be of the INTEGER type.</li><li>• <b>BackendPort</b>: the port of the origin server. This field is required and must be of the INTEGER type.</li><li>• <b>RealServers</b>: the IP addresses of the origin server. This field is required and must be a JSON array. It can contain up to 20 IP addresses.</li></ul>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	ADCA45A5-D15C-4B7D-9F81-138B0B36D0BD	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=CreateNetworkRules
&NetworkRules=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080,"BackendPort":8080,"RealServers":["1.1.1.1","2.2.2.2"]}]]
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<CreateNetworkRulesResponse>
  <RequestId>ADCA45A5-D15C-4B7D-9F81-138B0B36D0BD</RequestId>
</CreateNetworkRulesResponse>
```

##### JSON format

```
{
  "RequestId": "ADCA45A5-D15C-4B7D-9F81-138B0B36D0BD"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.8.3 ConfigNetworkRules


Modifies a port forwarding rule, namely, the IP addresses of the origin server.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ConfigNetworkRules	The operation that you want to perform. Set the value to <b>ConfigNetworkRules</b> .

Parameter	Type	Required	Example	Description
<b>NetworkRules</b>	String	Yes	<pre>[{"InstanceId": "ddoscoo-cn-mp91j1ao****", "Protocol": "tcp", "FrontendPort": 8080, "BackendPort": 8080, "RealServers": ["1.1.1.1", "2.2.2.2", "3.3.3.3"]}]</pre>	<p>Details about the port forwarding rule. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>InstanceId</b>: the ID of the instance. This field is required and must be of the STRING type.</li> <li>• <b>Protocol</b>: the forwarding protocol. This field is required and must be of the STRING type. Valid values: <b>tcp</b> and <b>udp</b>.</li> <li>• <b>FrontendPort</b>: the forwarding port. This field is required and must be of the INTEGER type.</li> <li>• <b>BackendPort</b>: the port of the origin server. This field is required and must be of the INTEGER type.</li> <li>• <b>RealServers</b>: the IP addresses of the origin server. This field is required and must be a JSON array. It can contain up to 20 IP addresses.</li> </ul> <div>  <b>Note:</b>            You can only modify the value of <b>RealServers</b> when you modify a port forwarding rule.         </div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	CC042262-15A3-4A49-ADF0-130968EA47BC	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ConfigNetworkRules
&NetworkRules=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080,"BackendPort":8080,"RealServers":["1.1.1.1","2.2.2.2","3.3.3.3"]}]]
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ConfigNetworkRulesResponse>
  <RequestId>CC042262-15A3-4A49-ADF0-130968EA47BC</RequestId>
</ConfigNetworkRulesResponse>
```

##### JSON format

```
{
  "RequestId": "CC042262-15A3-4A49-ADF0-130968EA47BC"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.8.4 DeleteNetworkRule

Deletes a port forwarding rule. You can only delete one port forwarding rule at a time.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteNetworkRule	The operation that you want to perform. Set the value to <b>DeleteNetworkRule</b> .
<b>NetworkRule</b>	String	Yes	[{"InstanceId": "ddoscoo-cn-mp91j1ao****", "Protocol": "tcp", "FrontendPort": 8080}]	Details about the port forwarding rule. This parameter is a JSON string. The fields in the value are described as follows: <ul style="list-style-type: none"><li>• <b>InstanceId</b>: the ID of the instance. This field is required and must be of the STRING type.</li><li>• <b>Protocol</b>: the forwarding protocol. This field is required and must be of the STRING type. Valid values: <b>tcp</b> and <b>udp</b>.</li><li>• <b>FrontendPort</b>: the forwarding port. This field is required and must be of the INTEGER type.</li></ul>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	49AD2F34-694A-4024-9B0E-DDCFC59CCC13	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=DeleteNetworkRule
&NetworkRule=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080}]
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<DeleteNetworkRuleResponse>
  <RequestId>49AD2F34-694A-4024-9B0E-DDCFC59CCC13</RequestId>
</DeleteNetworkRuleResponse>
```

##### JSON format

```
{
  "RequestId": "49AD2F34-694A-4024-9B0E-DDCFC59CCC13"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.8.5 DescribeHealthCheckList

Queries the Layer 4 or Layer 7 health check configuration of a port forwarding rule.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.


### Request parameters


Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeHealthCheckList	The operation that you want to perform. Set the value to <b>DescribeHealthCheckList</b> .
<b>NetworkRules</b>	String	Yes	[{"InstanceId": "ddoscoo-cn-mp91j1ao****", "Protocol": "tcp", "FrontendPort": 8080}]	Details about the port forwarding rule. This parameter is a JSON string. The fields in the value are described as follows: <ul style="list-style-type: none"><li>• <b>InstanceId</b>: the ID of the instance. This field is required and must be of the STRING type.</li><li>• <b>Protocol</b>: the forwarding protocol. This field is required and must be of the STRING type. Valid values: <b>tcp</b> and <b>udp</b>.</li><li>• <b>FrontendPort</b>: the forwarding port. This field is required and must be of the INTEGER type.</li></ul>



Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

### Response parameters

Parameter	Type	Example	Description
HealthCheckList	Array		Details about the health check configuration.
FrontendPort	Integer	8080	The forwarding port.
HealthCheck	Struct		The health check configuration.
Domain	String	www.aliyun.com	<p>The domain name that corresponds to the port forwarding rule.</p> <div>  <b>Note:</b>            This parameter is returned only when the Layer 7 health check configuration is queried.         </div>
Down	Integer	3	The number of consecutive failed health checks that must occur before declaring a port unhealthy. Valid values: <b>1</b> to <b>10</b> .
Interval	Integer	15	The health check intervals. Valid values: <b>1</b> to <b>30</b> . Unit: seconds.
Port	Integer	8080	The port that was checked.

Parameter	Type	Example	Description
Timeout	Integer	5	The response timeout period. Valid values: <b>1</b> to <b>30</b> . Unit: seconds.
Type	String	tcp	The protocol type. Valid values: <ul style="list-style-type: none"> <li><b>tcp</b>: The Layer 4 health check configuration was queried.</li> <li><b>http</b>: The Layer 7 health check configuration was queried.</li> </ul>
Up	Integer	3	The number of consecutive successful health checks that must occur before declaring a port healthy. Valid values: <b>1</b> to <b>10</b> .
Uri	String	/abc	The check path. <div>  <b>Note:</b>  This parameter is returned only when the Layer 7 health check configuration is queried. </div>
InstanceId	String	ddoscoo-cn-mp91j1ao****	The ID of the instance.
Protocol	String	tcp	The forwarding protocol. Valid values: <ul style="list-style-type: none"> <li><b>tcp</b></li> <li><b>udp</b></li> </ul>
RequestId	String	83B4AF42-E8EE-4DC9-BD73-87B7733A36F9	The ID of the request.
TotalCount	String	1	The total number of returned health check configurations.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeHealthCheckList
&NetworkRules=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080}]
```

### &<Common request parameters>

#### Sample success responses

##### XML format

```
<DescribeHealthCheckListResponse>
  <RequestId>83B4AF42-E8EE-4DC9-BD73-87B7733A36F9</RequestId>
  <HealthCheckList>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <FrontendPort>8080</FrontendPort>
    <HealthCheck>
      <Type>tcp</Type>
      <Down>3</Down>
      <Timeout>5</Timeout>
      <Port>8080</Port>
      <Up>3</Up>
      <Interval>15</Interval>
    </HealthCheck>
    <Protocol>tcp</Protocol>
  </HealthCheckList>
  <TotalCount>1</TotalCount>
</DescribeHealthCheckListResponse>
```

##### JSON format

```
{
  "RequestId": "83B4AF42-E8EE-4DC9-BD73-87B7733A36F9",
  "HealthCheckList": [
    {
      "InstanceId": "ddoscoo-cn-mp91j1ao****",
      "FrontendPort": 8080,
      "HealthCheck": {
        "Type": "tcp",
        "Down": 3,
        "Timeout": 5,
        "Port": 8080,
        "Up": 3,
        "Interval": 15
      },
      "Protocol": "tcp"
    }
  ],
  "TotalCount": 1
}
```

#### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.8.6 ModifyHealthCheckConfig



Modifies the Layer 4 or Layer 7 health check configuration of a port forwarding rule.


### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyHealthCheckConfig	The operation that you want to perform. Set the value to <b>ModifyHealthCheckConfig</b> .
<b>ForwardProtocol</b>	String	Yes	tcp	The forwarding protocol of the port forwarding rule. Valid values : <ul style="list-style-type: none"><li>• <b>tcp</b></li><li>• <b>udp</b></li></ul>
<b>FrontendPort</b>	Integer	Yes	8080	The forwarding port of the port forwarding rule.

Parameter	Type	Required	Example	Description
<b>HealthCheck</b>	String	Yes	<pre>{"Type":"tcp","Timeout":10,"Port":8080,"Interval":10,"Up":10,"Down":40}</pre>	<p>Details about the health check configuration. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>Type</b>: the protocol type. This field is required and must be of the STRING type. Valid values: <b>tcp</b> (Layer 4) and <b>http</b> (Layer 7).</li> <li>• <b>Domain</b>: the domain name. This field is optional and must be of the STRING type.</li> </ul> <div>  <b>Note:</b>  This field must be specified only when you want to modify Layer 7 health check configurations. </div> <ul style="list-style-type: none"> <li>• <b>Uri</b>: the check path. This field is optional and must be of the STRING type.</li> </ul> <div>  <b>Note:</b>  This field must be specified only when you want to modify Layer 7 health check configurations. </div> <ul style="list-style-type: none"> <li>• <b>Timeout</b>: the response timeout period. This field is optional and must be of the INTEGER type. Valid values: <b>1</b> to <b>30</b>. Unit: seconds.</li> <li>• <b>Port</b>: the port on which you want to perform the health check. This field is optional and must be of the INTEGER type.</li> </ul>
Issue: 20200529				<ul style="list-style-type: none"> <li>• <b>Interval</b>: the health check intervals. This field is optional and must be of the INTEGER type. Valid values: <b>1</b> to <b>30</b>.</li> </ul>

Parameter	Type	Required	Example	Description
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance.   <b>Note:</b> You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyHealthCheckConfig
&ForwardProtocol=tcp
&FrontendPort=8080
&HealthCheck={"Type":"tcp","Timeout":10,"Port":8080,"Interval":10,"Up":10,"Down":40}
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ModifyHealthCheckConfigResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</ModifyHealthCheckConfigResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.8.7 DescribeHealthCheckStatus

Queries the health status of an origin server.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeHealthCheckStatus	The operation that you want to perform. Set the value to <b>DescribeHealthCheckStatus</b> .

Parameter	Type	Required	Example	Description
<b>NetworkRules</b>	String	Yes	[[{"InstanceId": "ddoscoo-cn-mp91j1ao****", "Protocol": "tcp", "FrontendPort": 8080}]]	<p>Details about the port forwarding rule. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>InstanceId</b>: the ID of the instance. This field is required and must be of the STRING type.</li> <li>• <b>Protocol</b>: the forwarding protocol. This field is required and must be of the STRING type. Valid values: <b>tcp</b> and <b>udp</b>.</li> <li>• <b>FrontendPort</b>: the forwarding port. This field is required and must be of the INTEGER type.</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

### Response parameters

Parameter	Type	Example	Description
HealthCheckStatus	Array		Details about the health status of the origin server.
FrontendPort	Integer	8080	The forwarding port.
InstanceId	String	ddoscoo-cn-mp91j1ao****	The ID of the instance.



Parameter	Type	Example	Description
Protocol	String	tcp	The forwarding protocol. Valid values: <ul style="list-style-type: none"> <li><b>tcp</b></li> <li><b>udp</b></li> </ul>
RealServerStatusList	Array		The health status of the IP addresses of the origin server.
Address	String	1.1.1.1	The IP address of the origin server.
Status	String	abnormal	The health state of the IP address. Valid values: <ul style="list-style-type: none"> <li><b>normal</b>: healthy</li> <li><b>abnormal</b>: unhealthy</li> </ul>
Status	String	normal	The health status of the origin server. Valid values: <ul style="list-style-type: none"> <li><b>normal</b>: healthy</li> <li><b>abnormal</b>: unhealthy</li> </ul>
RequestId	String	DE9FF9E1-569C-4B6C-AB6A-0F6D927BB27C	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeHealthCheckStatus
&NetworkRules=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080}]
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeHealthCheckStatusResponse>
  <RequestId>DE9FF9E1-569C-4B6C-AB6A-0F6D927BB27C</RequestId>
  <HealthCheckStatus>
    <Status>abnormal</Status>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <FrontendPort>8080</FrontendPort>
    <RealServerStatusList>
      <Status>abnormal</Status>
      <Address>1.1.1.1</Address>
```

```
</RealServerStatusList>
<RealServerStatusList>
  <Status>abnormal</Status>
  <Address>2.2.2.2</Address>
</RealServerStatusList>
<RealServerStatusList>
  <Status>abnormal</Status>
  <Address>3.3.3.3</Address>
</RealServerStatusList>
<Protocol>tcp</Protocol>
</HealthCheckStatus>
</DescribeHealthCheckStatusResponse>
```

JSON format

```
{
  "RequestId": "DE9FF9E1-569C-4B6C-AB6A-0F6D927BB27C",
  "HealthCheckStatus": [
    {
      "Status": "abnormal",
      "InstanceId": "ddoscoo-cn-mp91j1ao****",
      "FrontendPort": 8080,
      "RealServerStatusList": [
        {
          "Status": "abnormal",
          "Address": "1.1.1.1"
        },
        {
          "Status": "abnormal",
          "Address": "2.2.2.2"
        },
        {
          "Status": "abnormal",
          "Address": "3.3.3.3"
        }
      ]
    },
    {
      "Protocol": "tcp"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.9 Sec-Traffic manager

### 12.9.1 DescribeSchedulerRules

Queries the scheduling rules that are created for Sec-Traffic Manager.


#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

**Request parameters**

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeSchedulerRules	The operation that you want to perform. Set the value to <b>DescribeSchedulerRules</b> .
<b>PageSize</b>	Integer	Yes	10	The number of entries to return on each page.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>RuleName</b>	String	No	testrule	The name of the scheduling rule.
<b>PageNumber</b>	Integer	No	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .

## Response parameters

Parameter	Type	Example	Description
RequestId	String	11C55595-1757-4B17-9ACE-4ACB68C2D989	The ID of the request.
SchedulerRules	Array		Details about scheduling rules.
Cname	String	4eru5229a843****.aliyunddos0001.com	The CNAME record assigned by Sec-Traffic Manager for the scheduling rule.
RuleName	String	doctest	The name of the scheduling rule.
RuleType	String	6	The type of the scheduling rule. Valid values: <ul style="list-style-type: none"> <li><b>2</b>: tiered protection</li> <li><b>3</b>: network acceleration</li> <li><b>5</b>: CDN interaction</li> <li><b>6</b>: cloud service interaction</li> </ul>
Rules	Array		Details about the scheduling rule.
Priority	Integer	100	The priority of the rule.
RegionId	Integer	1	The region where the interaction resource that is used in the scheduling rule is deployed. <div>  <b>Note:</b>  This parameter is returned only if <b>RuleType</b> is set to <b>2</b>. </div>
Status	Integer	0	The status of the scheduling rule. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: disabled</li> <li><b>1</b>: enabled</li> </ul>

Parameter	Type	Example	Description
Type	String	A	The address type of the interaction resource. Valid values: <ul style="list-style-type: none"><li>• <b>IP</b>: IP address</li><li>• <b>CNAME</b>: CNAME record</li></ul>
Value	String	203.***.***.39	The address of the interaction resource.
ValueType	Integer	1	The address type of the interaction resource. Valid values: <ul style="list-style-type: none"><li>• <b>1</b>: the IP address of Anti-DDoS Pro or Anti-DDoS Premium</li><li>• <b>2</b>: the IP address of the interaction resource (in the tiered protection scenario)</li><li>• <b>3</b>: the IP address used to accelerate access (in the network acceleration scenario)</li><li>• <b>5</b>: the domain name configured in CDN (in the CDN interaction scenario)</li><li>• <b>6</b> the IP address of the interaction resource (in the cloud service interaction scenario)</li></ul>
TotalCount	String	1	The total number of returned scheduling rules.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSchedulerRules
&PageSize=10
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeSchedulerRulesResponse>
  <TotalCount>1</TotalCount>
```

```

<RequestId>11C55595-1757-4B17-9ACE-4ACB68C2D989</RequestId>
<SchedulerRules>
  <RuleType>6</RuleType>
  <Cname>4eru5229a843****.aliyunddos0001.com</Cname>
  <Rules>
    <Status>0</Status>
    <Type>A</Type>
    <ValueType>1</ValueType>
    <Priority>100</Priority>
    <Value>203. ***. ***.39</Value>
    <RegionId></RegionId>
  </Rules>
  <Rules>
    <Status>1</Status>
    <Type>A</Type>
    <ValueType>6</ValueType>
    <Priority>50</Priority>
    <Value>47. ***. ***.47</Value>
    <RegionId>cn-hangzhou</RegionId>
  </Rules>
  <RuleName>doctest</RuleName>
</SchedulerRules>
</DescribeSchedulerRulesResponse>

```

#### JSON format

```

{
  "TotalCount": 1,
  "RequestId": "11C55595-1757-4B17-9ACE-4ACB68C2D989",
  "SchedulerRules": [
    {
      "RuleType": 6,
      "Cname": "4eru5229a843****.aliyunddos0001.com",
      "Rules": [
        {
          "Status": 0,
          "Type": "A",
          "ValueType": 1,
          "Priority": 100,
          "Value": "203. ***. ***.39",
          "RegionId": ""
        },
        {
          "Status": 1,
          "Type": "A",
          "ValueType": 6,
          "Priority": 50,
          "Value": "47. ***. ***.47",
          "RegionId": "cn-hangzhou"
        }
      ],
      "RuleName": "doctest"
    }
  ]
}

```

#### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.9.2 CreateSchedulerRule

Creates a scheduling rule for Sec-Traffic Manager.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	CreateSchedulerRule	The operation that you want to perform. Set the value to <b>CreateSchedulerRule</b> .
<b>RuleName</b>	String	Yes	testrule	The name of the scheduling rule.


Parameter	Type	Required	Example	Description
<b>Rules</b>	String	Yes	<pre>[{"Type": "A", "Value": "1.1.1.1", "Priority": 80, "ValueType": 2, "RegionId": "cn-hangzhou"}, {"Type": "A", "Value": "203.***.***.199", "Priority": 80, "ValueType": 1}]</pre>	<p>Details about the scheduling rule. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>Type</b>: the address type of the interaction resource that you want to use in the scheduling rule. This field is required and must be of the STRING type. Valid values: <ul style="list-style-type: none"> <li>- <b>A</b>: IP address</li> <li>- <b>CNAME</b>: domain name</li> </ul> </li> <li>• <b>Value</b>: the address of the interaction resource that you want to use in the scheduling rule. This field is required and must be of the STRING type.</li> <li>• <b>Priority</b>: the priority of the scheduling rule. This field is required and must be of the INTEGER type. Valid values: <b>0</b> to <b>100</b>. A larger value indicates a higher priority.</li> <li>• <b>ValueType</b>: The type of the interaction resource that you want to use in the scheduling rule. This field is required and must be of the INTEGER type. Valid values: <ul style="list-style-type: none"> <li>- <b>1</b>: the IP address of Anti-DDoS Pro or Anti-DDoS Premium</li> <li>- <b>2</b>: the IP address of the interaction resource (in the tiered protection scenario)</li> <li>- <b>3</b>: the IP address used to accelerate access (in the network acceleration scenario)</li> <li>- <b>5</b>: the domain name configured in CDN (in the CDN interaction scenario)</li> <li>- <b>6</b>: the IP address of the interaction resource (in the</li> </ul> </li> </ul>



Parameter	Type	Required	Example	Description
<b>RuleType</b>	Integer	Yes	2	The type of the scheduling rule. Valid values: <ul style="list-style-type: none"><li>• <b>2</b>: tiered protection</li><li>• <b>3</b>: network acceleration</li><li>• <b>5</b>: CDN interaction</li><li>• <b>6</b>: cloud service interaction</li></ul>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

Parameter	Type	Required	Example	Description
<b>Param</b>	String	No	<pre>{   "ParamType": "cdn",   "ParamData": {     "Domain": "cdn.test.com",     "Cname": "cdnname.test.com",     "AccessQps": 100,     "UpstreamQps": 100   } }</pre>	<p>Details about the CDN interaction rule. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>ParamType</b>: the type of the scheduling rule that you want to create. This field is required and must be of the STRING type. Set the value to <b>cdn</b>. This indicates that you want to create a CDN interaction rule.</li> <li>• <b>ParamData</b>: the parameters that you want to configure for the CDN interaction rule. The field is required and must be of the MAP type. <ul style="list-style-type: none"> <li>- <b>Domain</b>: the domain name configured in CDN. It is required and must be of the STRING type.</li> <li>- <b>Cname</b>: the CNAME record of the domain name configured in CDN. It is required and must be of the STRING type.</li> <li>- <b>AccessQps</b>: the queries per second (QPS) threshold used to switch service traffic to Anti-DDoS Pro or Anti-DDoS Premium. It is required and must be of the INTEGER type.</li> <li>- <b>UpstreamQps</b>: the QPS threshold used to switch service traffic to CDN. It must be of the INTEGER type.</li> </ul> </li> </ul>

## Response parameters

Parameter	Type	Example	Description
Cname	String	48k7b372gpl4****.aliyunddos0001.com	The CNAME record assigned by Sec-Traffic Manager for the rule. <div> <b>Note:</b> To enable the rule, you must map the domain name of your service to the CNAME record.</div>
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.
RuleName	String	testrule	The name of the rule.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=CreateSchedulerRule
&RuleName=testrule
&Rules=[{"Type":"A", "Value":"1.1.1.1", "Priority":80,"ValueType":2, "RegionId":"cn-
hangzhou"}, {"Type":"A", "Value":"203. ***. ***.199", "Priority":80,"ValueType":1}]
&RuleType=2
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<CreateSchedulerRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <Cname>48k7b372gpl4****.aliyunddos0001.com</Cname>
  <RuleName>testrule</RuleName>
</CreateSchedulerRuleResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "Cname": "48k7b372gpl4****.aliyunddos0001.com",
  "RuleName": "testrule"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.9.3 ModifySchedulerRule

Modifies the scheduling rule of Sec-Traffic Manager.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters


Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifySchedulerRule	The operation that you want to perform. Set the value to <b>ModifySchedulerRule</b> .
<b>RuleName</b>	String	Yes	testrule	The name of the scheduling rule that you want to modify.

Parameter	Type	Required	Example	Description
<b>Rules</b>	String	Yes	<pre>[{"Type": "A", "Value": "1.1.1.1", "Priority": 80, "ValueType": 2, "RegionId": "cn-hangzhou"}, {"Type": "A", "Value": "203.***.***.199", "Priority": 80, "ValueType": 1}]</pre>	<p>Details about the scheduling rule. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>Type</b>: the address type of the interaction resource that you want to use in the scheduling rule. This field is required and must be of the STRING type. Valid values: <ul style="list-style-type: none"> <li>- <b>A</b>: IP address</li> <li>- <b>CNAME</b>: domain name</li> </ul> </li> <li>• <b>Value</b>: the address of the interaction resource that you want to use in the scheduling rule. This field is required and must be of the STRING type.</li> <li>• <b>Priority</b>: the priority of the scheduling rule. This field is required and must be of the INTEGER type. Valid values: <b>0</b> to <b>100</b>. A larger value indicates a higher priority.</li> <li>• <b>ValueType</b>: the type of the interaction resource that you want to use in the scheduling rule. This field is required and must be of the INTEGER type. Valid values: <ul style="list-style-type: none"> <li>- <b>1</b>: the IP address of Anti-DDoS Pro or Anti-DDoS Premium</li> <li>- <b>2</b>: the IP address of the interaction resource (in the tiered protection scenario)</li> <li>- <b>3</b>: the IP address used to accelerate access (in the network acceleration scenario)</li> <li>- <b>5</b>: the domain name configured in CDN (in the CDN interaction scenario)</li> <li>- <b>6</b>: the IP address of the interaction resource (in the</li> </ul> </li> </ul>

Parameter	Type	Required	Example	Description
<b>RuleType</b>	Integer	Yes	2	The type of the scheduling rule. Valid values: <ul style="list-style-type: none"><li>• <b>2</b>: tiered protection</li><li>• <b>3</b>: network acceleration</li><li>• <b>5</b>: CDN interaction</li><li>• <b>6</b>: cloud service interaction</li></ul>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

Parameter	Type	Required	Example	Description
<b>Param</b>	String	No	<pre>{   "ParamType": "cdn",   "ParamData": {     "Domain": "cdn.test.com",     "Cname": "cdnname.test.com",     "AccessQps": 100,     "UpstreamQps": 100   } }</pre>	<p>Details about the CDN interaction rule. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>ParamType</b>: the type of the scheduling rule. This field is required and must be of the STRING type. Set the value to <b>cdn</b>. This indicates that you want to modify a CDN interaction rule.</li> <li>• <b>ParamData</b>: the values of parameters that you want to modify for the CDN interaction rule. This field is required and must be of the MAP type. <ul style="list-style-type: none"> <li>- <b>Domain</b>: the domain name configured in CDN. It is required and must be of the STRING type.</li> <li>- <b>Cname</b>: the CNAME record of the domain name configured in CDN. It is required and must be of the STRING type.</li> <li>- <b>AccessQps</b>: the queries per second (QPS) threshold used to switch service traffic to Anti-DDoS Pro or Anti-DDoS Premium. It is required and must be of the INTEGER type.</li> <li>- <b>UpstreamQps</b>: the QPS threshold used to switch service traffic to CDN. It must be of the INTEGER type.</li> </ul> </li> </ul>

## Response parameters

Parameter	Type	Example	Description
Cname	String	48k7b372gpl4****.aliyunddos0001.com	The CNAME record assigned by Sec-Traffic Manager for the scheduling rule.   <b>Note:</b> To enable the rule, you must map the domain name of the service to the CNAME record.
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.
RuleName	String	testrule	The name of the rule.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=ModifySchedulerRule
&RuleName=testrule
&Rules=[{"Type":"A", "Value":"1.1.1.1", "Priority":80,"ValueType":2, "RegionId":"cn-hangzhou"}, {"Type":"A", "Value":"203. ***. ***.199", "Priority":80,"ValueType":1}]
&RuleType=2
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<ModifySchedulerRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <Cname>48k7b372gpl4****.aliyunddos0001.com</Cname>
  <RuleName>testrule</RuleName>
</ModifySchedulerRuleResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "Cname": "48k7b372gpl4****.aliyunddos0001.com",
  "RuleName": "testrule"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).



## 12.9.4 DeleteSchedulerRule

Deletes a scheduling rule of Sec-Traffic Manager.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteSchedulerRule	The operation that you want to perform. Set the value to <b>DeleteSchedulerRule</b> .
<b>RuleName</b>	String	Yes	testrule	The name of the scheduling rule that you want to delete.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

## Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DeleteSchedulerRule
&RuleName=testrule
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DeleteSchedulerRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteSchedulerRuleResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.10 Protection for infrastructure

### 12.10.1 DescribeAutoCcListCount

Queries the numbers of IP addresses in the whitelist and blacklist of an Anti-DDoS Pro or Anti-DDoS Premium instance.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeAutoCcListCount	The operation that you want to perform. Set the value to <b>DescribeAutoCcListCount</b> .
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance.  <div>  <b>Note:</b>            You can call the <b>DescribeInstances</b> operation to query the IDs of all instances.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>QueryType</b>	String	No	manual	The mode of how an IP address is added to the whitelist or blacklist. Valid values: <ul style="list-style-type: none"> <li><b>manual</b>: manually added</li> <li><b>auto</b>: automatically added</li> </ul>

## Response parameters

Parameter	Type	Example	Description
BlackCount	Integer	0	The total number of IP addresses in the blacklist.
RequestId	String	5AC3785F-C789-4622-87A4-F58BE7F6B184	The ID of the request.

Parameter	Type	Example	Description
WhiteCount	Integer	2	The total number of IP addresses in the whitelist.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAutoCcListCount
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeAutoCcListCountResponse>
  <BlackCount>0</BlackCount>
  <RequestId>5AC3785F-C789-4622-87A4-F58BE7F6B184</RequestId>
  <WhiteCount>2</WhiteCount>
</DescribeAutoCcListCountResponse>
```

#### JSON format

```
{
  "BlackCount": 0,
  "RequestId": "5AC3785F-C789-4622-87A4-F58BE7F6B184",
  "WhiteCount": 2
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.10.2 DescribeAutoCcBlacklist


Queries IP addresses in the blacklist of an Anti-DDoS Pro or Anti-DDoS Premium instance.

### Debugging

[OpenAPI Explorer](#) automatically calculates the signature value. For your convenience, we recommend that you call this operation in [OpenAPI Explorer](#). [OpenAPI Explorer](#) dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeAutoCcBlacklist	The operation that you want to perform. Set the value to <b>DescribeAutoCcBlacklist</b> .
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance.  <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.         </div>
<b>PageNumber</b>	Integer	Yes	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .
<b>PageSize</b>	Integer	Yes	10	The number of entries to return on each page.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

Parameter	Type	Required	Example	Description
<b>Keyword</b>	String	No	138	<p>The keyword for the query. This keyword is used to specify the prefix of the source IP address that you want to query.</p> <div>  <b>Note:</b>            It must be greater than three characters in length.         </div>

### Response parameters

Parameter	Type	Example	Description
AutoCcBlacklist	Array		Details about the IP address in the blacklist of the instance.
DestIp	String	203.***.***.132	The IP address of the instance.
EndTime	Long	1584093569	The validity period of the IP address in the blacklist. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
SourceIp	String	1.1.1.1	The IP address in the blacklist.
Type	String	manual	<p>The mode of how an IP address is added to the blacklist. Valid values:</p> <ul style="list-style-type: none"> <li><b>manual:</b> manually added</li> <li><b>auto:</b> automatically added</li> </ul>
RequestId	String	E78C8472-0B15-42D5-AF22-A32A78818AB2	The ID of the request.
TotalCount	Long	2	The total number of returned IP addresses in the blacklist.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAutoCcBlacklist
&InstanceId=ddoscoo-cn-mp91j1ao****
&PageNumber=1
&PageSize=10
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeAutoCcBlacklistResponse>
  <TotalCount>2</TotalCount>
  <RequestId>E78C8472-0B15-42D5-AF22-A32A78818AB2</RequestId>
  <AutoCcBlacklist>
    <Type>manual</Type>
    <SourceIp>1.1.1.1</SourceIp>
    <EndTime>1584093569</EndTime>
    <DestIp>203. ***. ***.132</DestIp>
  </AutoCcBlacklist>
  <AutoCcBlacklist>
    <Type>manual</Type>
    <SourceIp>2.2.2.2</SourceIp>
    <EndTime>1584093569</EndTime>
    <DestIp>203. ***. ***.132</DestIp>
  </AutoCcBlacklist>
</DescribeAutoCcBlacklistResponse>
```

#### JSON format

```
{
  "TotalCount": 2,
  "RequestId": "E78C8472-0B15-42D5-AF22-A32A78818AB2",
  "AutoCcBlacklist": [
    {
      "Type": "manual",
      "SourceIp": "1.1.1.1",
      "EndTime": "1584093569",
      "DestIp": "203. ***. ***.132"
    },
    {
      "Type": "manual",
      "SourceIp": "2.2.2.2",
      "EndTime": "1584093569",
      "DestIp": "203. ***. ***.132"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.10.3 AddAutoCcBlacklist

Adds IP addresses to the blacklist of an Anti-DDoS Pro or Anti-DDoS Premium instance.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	AddAutoCcBlacklist	The operation that you want to perform. Set the value to <b>AddAutoCcBlacklist</b> .
<b>Blacklist</b>	String	Yes	[{"src":"1.1.1.1"}, {"src":"2.2.2.2"}]	The IP addresses that you want to manage. This parameter is a JSON string. The field in the value is described as follows: <ul style="list-style-type: none"><li><b>src</b>: the IP address. This field is required and must be of the STRING type.</li></ul>
<b>ExpireTime</b>	Integer	Yes	300	The validity period of the IP address in the blacklist. Valid values: <b>300</b> to <b>7200</b> . Unit: seconds.
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance. <div> <b>Note:</b> You can call the <b>DescribeInstances</b> operation to query the IDs of all instances.</div>



Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=AddAutoCcBlacklist
&Blacklist=[{"src":"1.1.1.1"}, {"src":"2.2.2.2"}]
&ExpireTime=300
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<AddAutoCcBlacklistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</AddAutoCcBlacklistResponse>
```

##### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.10.4 DeleteAutoCcBlacklist

Removes IP addresses from the blacklist of an Anti-DDoS Pro or Anti-DDoS Premium instance.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteAutoCcBlacklist	The operation that you want to perform. Set the value to <b>DeleteAutoCcBlacklist</b> .
<b>Blacklist</b>	String	Yes	[{"src":"1.1.1.1"}, {"src":"2.2.2.2"}]	The IP addresses that you want to manage. This parameter is a JSON string. The field in the value is described as follows: <ul style="list-style-type: none"><li><b>src</b>: the IP address. This field is required and must be of the STRING type.</li></ul>
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance. <div> <b>Note:</b> You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.</div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DeleteAutoCcBlacklist
&Blacklist=[{"src":"1.1.1.1"}, {"src":"2.2.2.2"}]
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<DeleteAutoCcBlacklistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DeleteAutoCcBlacklistResponse>
```

##### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.10.5 EmptyAutoCcBlacklist

Clears IP addresses from the blacklist of an Anti-DDoS Pro or Anti-DDoS Premium instance.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	EmptyAutoCcBlacklist	The operation that you want to perform. Set the value to <b>EmptyAutoCcBlacklist</b> .
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance.  <b>Note:</b> You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=EmptyAutoCcBlacklist
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<EmptyAutoCcBlacklistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</EmptyAutoCcBlacklistResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.10.6 DescribeAutoCcWhitelist



Queries IP addresses in the whitelist of an Anti-DDoS Pro or Anti-DDoS Premium instance.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeAutoCcWhitelist	The operation that you want to perform. Set the value to <b>DescribeAutoCcWhitelist</b> .

Parameter	Type	Required	Example	Description
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	<p>The ID of the instance.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.         </div>
<b>PageNumber</b>	Integer	Yes	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .
<b>PageSize</b>	Integer	Yes	10	The number of entries to return on each page.
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>Keyword</b>	String	No	138	<p>The keyword for the query. This keyword is used to specify the prefix of the source IP address that you want to query.</p> <div>  <b>Note:</b>            It must be greater than three characters in length.         </div>

## Response parameters

Parameter	Type	Example	Description
AutoCcWhitelist	Array		Details about the IP address in the whitelist of the instance.
DestIp	String	203.***.***.117	The IP address of the instance.
EndTime	Long	0	The validity period of the IP address in the whitelist. Unit: seconds. <b>0</b> indicates that the whitelist takes effect all the time.
SourceIp	String	2.2.2.2	The IP address in the whitelist.
Type	String	manual	The mode of how an IP address is added to the whitelist. Valid values: <ul style="list-style-type: none"><li>• <b>manual</b>: manually added</li><li>• <b>auto</b>: automatically added</li></ul>
RequestId	String	F09D085E-5E0F-4FF2-B32E-F4A644049162	The ID of the request.
TotalCount	Long	2	The total number of returned IP addresses in the whitelist.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAutoCcWhitelist
&InstanceId=ddoscoo-cn-mp91j1ao****
&PageNumber=1
&PageSize=10
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeAutoCcWhitelistResponse>
  <AutoCcWhitelist>
    <Type>manual</Type>
    <SourceIp>4.4.4.4</SourceIp>
```

```
<EndTime>0</EndTime>
<DestIp>203. ***. ***.117</DestIp>
</AutoCcWhitelist>
<AutoCcWhitelist>
  <Type>manual</Type>
  <SourceIp>2.2.2.2</SourceIp>
  <EndTime>0</EndTime>
  <DestIp>203. ***. ***.117</DestIp>
</AutoCcWhitelist>
<TotalCount>2</TotalCount>
<RequestId>F09D085E-5E0F-4FF2-B32E-F4A644049162</RequestId>
</DescribeAutoCcWhitelistResponse>
```

JSON format

```
{
  "AutoCcWhitelist": [
    {
      "Type": "manual",
      "SourceIp": "4.4.4.4",
      "EndTime": "0",
      "DestIp": "203. ***. ***.117"
    },
    {
      "Type": "manual",
      "SourceIp": "2.2.2.2",
      "EndTime": "0",
      "DestIp": "203. ***. ***.117"
    }
  ],
  "TotalCount": 2,
  "RequestId": "F09D085E-5E0F-4FF2-B32E-F4A644049162"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.10.7 AddAutoCcWhitelist

Adds IP addresses to the whitelist of an Anti-DDoS Pro or Anti-DDoS Premium instance.


### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AddAutoCcWhitelist	The operation that you want to perform. Set the value to <b>AddAutoCcWhitelist</b> .



Parameter	Type	Required	Example	Description
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	<p>The ID of the instance.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.         </div>
<b>Whitelist</b>	String	Yes	[{"src": "1.1.1.1"}, {"src": "2.2.2.2"}]	<p>The IP addresses that you want to manage. This parameter is a JSON string. The field in the value is described as follows:</p> <ul style="list-style-type: none"> <li><b>src</b>: the IP address. This field is required and must be of the STRING type.</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ExpireTime</b>	Integer	No	3600	<p>The validity period of the IP address in the whitelist. Unit: seconds. <b>0</b> indicates that the whitelist takes effect all the time.</p>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=AddAutoCcWhitelist
&InstanceId=ddoscoo-cn-mp91j1ao****
&Whitelist=[{"src":"1.1.1.1"}, {"src":"2.2.2.2"}]
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<AddAutoCcWhitelistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</AddAutoCcWhitelistResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.10.8 DeleteAutoCcWhitelist


Removes IP addresses from the whitelist of an Anti-DDoS Pro or Anti-DDoS Premium instance.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteAutoCcWhitelist	The operation that you want to perform. Set the value to <b>DeleteAutoCcWhitelist</b> .

Parameter	Type	Required	Example	Description
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	<p>The ID of the instance.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.         </div>
<b>Whitelist</b>	String	Yes	[{"src":"1.1.1.1"}, {"src":"2.2.2.2"}]	<p>The IP addresses that you want to manage. This parameter is a JSON string. The field in the value is described as follows:</p> <ul style="list-style-type: none"> <li><b>src</b>: the IP address. This field is required and must be of the STRING type.</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DeleteAutoCcWhitelist
&InstanceId=ddoscoo-cn-mp91j1ao****
&Whitelist=[{"src":"1.1.1.1"}, {"src":"2.2.2.2"}]
```

&<Common request parameters>

Sample success responses

XML format

```
<DeleteAutoCcWhitelistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DeleteAutoCcWhitelistResponse>
```

JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.10.9 EmptyAutoCcWhitelist

Clears IP addresses from the whitelist of an Anti-DDoS Pro or Anti-DDoS Premium instance.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	EmptyAutoCcWhitelist	The operation that you want to perform. Set the value to <b>EmptyAutoCcWhitelist</b> .
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance. <div> <b>Note:</b> You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.</div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=EmptyAutoCcWhitelist
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<EmptyAutoCcWhitelistResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</EmptyAutoCcWhitelistResponse>
```

##### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.10.10 DescribeUnBlackholeCount

Queries the total and remaining quotas that you can deactivate the black hole.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeUnBlackholeCount	The operation that you want to perform. Set the value to <b>DescribeUnBlackholeCount</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RemainCount	Integer	5	The remaining quota that you can deactivate the black hole.

Parameter	Type	Example	Description
RequestId	String	232929FA-40B6-4C53-9476-EE335ABA44CD	The ID of the request.
TotalCount	Integer	5	The total quota that you can deactivate the black hole.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeUnBlackholeCount
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeUnBlackholeCountResponse>
  <TotalCount>5</TotalCount>
  <RequestId>232929FA-40B6-4C53-9476-EE335ABA44CD</RequestId>
  <RemainCount>5</RemainCount>
</DescribeUnBlackholeCountResponse>
```

#### JSON format

```
{
  "TotalCount": 5,
  "RequestId": "232929FA-40B6-4C53-9476-EE335ABA44CD",
  "RemainCount": 5
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.10.11 DescribeBlackholeStatus

Queries the black hole status of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeBlackholeStatus	The operation that you want to perform. Set the value to <b>DescribeBlackholeStatus</b> .
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N.  <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

## Response parameters

Parameter	Type	Example	Description
BlackholeStatus	Array		Details about the black hole status of the instance.
BlackStatus	String	blackhole	Indicates whether the instance is in the Blackhole state. Valid values: <ul style="list-style-type: none"> <li><b>blackhole</b>: The instance is in the Blackhole state.</li> <li><b>normal</b>: The instance is in the Normal state.</li> </ul>



Parameter	Type	Example	Description
EndTime	Long	1540196323	The end time of the black hole. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Ip	String	203.***.***.132	The IP address of the instance.
StartTime	Long	1540195323	The start time of the black hole. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeBlackholeStatus
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeBlackholeStatusResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <BlackholeStatus>
    <Ip>203.***.***.132</Ip>
    <BlackStatus>blackhole</BlackStatus>
    <StartTime>1540195323</StartTime>
    <EndTime>1540196323</EndTime>
  </BlackholeStatus>
</DescribeBlackholeStatusResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "BlackholeStatus": [{
    "Ip": "203.***.***.132",
    "BlackStatus": "blackhole",
```

```
"StartTime": 1540195323,  
"EndTime": 1540196323  
  }  
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.10.12 ModifyBlackholeStatus

Deactivates the black hole.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyBlackholeStatus	The operation that you want to perform. Set the value to <b>ModifyBlackholeStatus</b> .
<b>BlackholeStatus</b>	String	Yes	undo	The action that you want to perform on the black hole. Set the value to <b>undo</b> , which indicates that you want to deactivate the black hole.
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance. <div> <b>Note:</b> You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.</div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyBlackholeStatus
&BlackholeStatus=undo
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ModifyPortAutoCcStatusResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</ModifyPortAutoCcStatusResponse>
```

##### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.10.13 DescribeNetworkRegionBlock

Queries the blocked regions that are configured for an Anti-DDoS Pro or Anti-DDoS Premium instance.

### Debugging



OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeNetworkRegionBlock	The operation that you want to perform. Set the value to <b>DescribeNetworkRegionBlock</b> .
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance.  <b>Note:</b> You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
Config	Struct		The configuration of blocked regions.

Parameter	Type	Example	Description
Countries	List	[1,2]	<p>The codes of blocked regions outside China.</p> <div>  <b>Note:</b>            For more information about country codes, see the Codes of regions outside China table in this topic.         </div>
Provinces	List	[11,12]	<p>The codes of blocked regions inside China.</p> <div>  <b>Note:</b>            For more information about codes of regions inside China, see the Codes of regions inside China table in this topic.         </div>
RegionBlockSwitch	String	on	<p>The status of the Blocked Regions policy. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>on</b></li> <li>• <b>off</b></li> </ul>
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Codes of regions inside China

Code	Region
11	Beijing
12	Tianjin
13	Hebei
14	Shanxi
15	Nei Mongol

Code	Region
21	Liaoning
22	Jilin
23	Heilongjiang
31	Shanghai
32	Jiangsu
33	Zhejiang
34	Anhui
35	Fujian
36	Jiangxi
37	Shandong
41	Henan
42	Hubei
43	Hunan
44	Guangdong
45	Guangxi
46	Hainan
50	Chongqing
51	Sichuan
52	Guizhou
53	Yunnan

Code	Region
54	Xizang
61	Shaanxi
62	Gansu
63	Qinghai
64	Ningxia
65	Xinjiang
81	Hong Kong S.A.R
71	Taiwan
82	Macao S.A.R

**Codes of regions outside China**

Code	Country	Abbreviation
1	China	CN
2	Australia	AU
3	Japan	JP
4	Thailand	TH
5	India	IN
7	United States	US
8	Germany	DE
9	Netherlands	NL
10	Malaysia	MY

Code	Country	Abbreviation
11	Angola	AO
12	South Korea	KR
13	Singapore	SG
14	Kampuchea	KH
16	Philippines	PH
17	Vietnam	VN
18	France	FR
19	Poland	PL
20	Spain	ES
21	Russia	RU
22	Switzerland	CH
23	United Kingdom	GB
24	Italy	IT
25	Czech Republic	CZ
26	Ireland	IE
27	Denmark	DK
28	Portugal	PT
29	Sweden	SE
30	Ghana	GH
31	Turkey	TR



Code	Country	Abbreviation
32	Cameroon	CM
33	South Africa	ZA
34	Finland	FI
35	Hungary	HU
36	United Arab Emirates	AE
37	Greece	GR
38	Brazil	BR
39	Austria	AT
40	Jordan	JO
41	Belgium	BE
42	Romania	RO
43	Luxembourg	LU
44	Argentina	AR
45	Uganda	UG
46	Armenia	AM
47	Tanzania	TZ
48	Burundi	BI
49	Uruguay	UY
50	Bulgaria	BG
51	Ukraine	UA

Code	Country	Abbreviation
52	Israel	IL
53	Qatar	QA
54	Iraq	IQ
55	Lithuania	LT
56	Moldova	MD
57	Uzbekistan	UZ
58	Slovakia	SK
59	Kazakhstan	KZ
60	Croatia	HR
61	Georgia	GE
62	Estonia	EE
63	Gibraltar	GI
64	Latvia	LV
65	Norway	NO
66	Palestine	PS
67	Cyprus	CY
68	Saudi Arabia	SA
69	Iran	IR
70	Canada	CA
71	American Samoa	AS

Code	Country	Abbreviation
72	Syria	SY
73	Kuwait	KW
74	Bahrain	BH
75	Lebanon	LB
76	Oman	OM
77	Azerbaijan	AZ
78	Zambia	ZM
79	Zimbabwe	ZW
80	Democratic Republic of the Congo	CD
81	Serbia	RS
82	Iceland	IS
83	Slovenia	SI
84	Macedonia	MK
85	Liechtenstein	LI
86	Jersey	JE
87	Bosnia and Herzegovina	BA
88	Chile	CL
89	Peru	PE
90	Kyrgyzstan	KG

Code	Country	Abbreviation
91	Reunion	RE
92	Tajikistan	TJ
93	Isle of Man	IM
94	Guernsey	GG
95	Malta	MT
96	Libya	LY
97	Yemen	YE
98	Belarus	BY
99	Mayotte	YT
100	Guadeloupe	GP
101	Saint Martin	MF
102	Martinique	MQ
103	Guyana	GY
104	Kosovo	XK
105	Indonesia	ID
106	Northern Mariana Islands	MP
107	Dominican Republic	DO
108	Mexico	MX
109	Guam	GU
110	Nigeria	NG

Code	Country	Abbreviation
111	Venezuela	VE
112	Puerto Rico	PR
113	Mongolia	MN
114	New Zealand	NZ
115	Bangladesh	BD
116	Pakistan	PK
117	Papua New Guinea	PG
118	Trinidad and Tobago	TT
119	Lesotho	LS
120	Colombia	CO
121	Costa Rica	CR
123	Ecuador	EC
124	Sri Lanka	LK
125	Egypt	EG
126	British Virgin Islands	VG
127	Jamaica	JM
128	Saint Lucia	LC
129	Cayman Islands	KY
130	Grenada	GD
131	Curacao	CW

Code	Country	Abbreviation
132	Panama	PA
133	Barbados	BB
134	The Bahamas	BS
135	Nepal	NP
136	Tokelau	TK
137	Maldives	MV
138	Afghanistan	AF
139	New Caledonia	NC
140	Fiji	FJ
141	Wallis and Futuna Islands	WF
142	Albania	AL
143	San Marino	SM
144	Montenegro	ME
145	East Timor	TL
146	Monaco	MC
147	Guinea	GN
148	Myanmar	MM
149	Greenland	GL
150	Bermuda	BM

Code	Country	Abbreviation
151	Saint Vincent and the Grenadines	VC
152	United States Virgin Islands	VI
153	Suriname	SR
154	Saint Barthelemy	BL
155	Haiti	HT
156	Antigua and Barbuda	AG
157	Liberia	LR
158	Kenya	KE
159	Botswana	BW
160	Mozambique	MZ
161	Senegal	SN
162	Madagascar	MG
163	Namibia	NA
164	Côte d'Ivoire	CI
165	Sudan	SD
166	Malawi	MW
167	Gabon	GA
168	Mali	ML
169	Benin	BJ

Code	Country	Abbreviation
170	Chad	TD
171	Cabo Verde	CV
172	Rwanda	RW
173	Republic of the Congo	CG
174	The Gambia	GM
175	Mauritius	MU
176	Algeria	DZ
177	Eswatini	SZ
178	Burkina Faso	BF
179	Sierra Leone	SL
180	Somalia	SO
181	Niger	NE
182	Central African Republic	CF
183	Togo	TG
184	South Sudan	SS
185	Equatorial Guinea	GQ
186	Seychelles	SC
187	Djibouti	DJ
188	Morocco	MA
189	Mauritania	MR



Code	Country	Abbreviation
190	Comoros	KM
191	British Indian Ocean Territory	IO
192	Tunisia	TN
193	Laos	LA
194	Brunei	BN
195	Bhutan	BT
196	Nauru	NR
197	Vanuatu	VU
198	Federated States of Micronesia	FM
199	French Polynesia	PF
200	Tonga	TO
201	Honduras	HN
202	Bolivia	BO
203	El Salvador	SV
204	Guatemala	GT
205	Nicaragua	NI
206	Belize	BZ
207	Paraguay	PY
208	French Guiana	GF

Code	Country	Abbreviation
209	Andorra	AD
210	Faroe Islands	FO
211	Niue	NU
212	Kiribati	KI
213	Marshall Islands	MH
214	Palau	PW
215	Samoa	WS
216	Solomon Islands	SB
217	Tuvalu	TV
218	North Korea	KP
219	Vatican City	VA
220	Eritrea	ER
221	Ethiopia	ET
222	Guinea-Bissau	GW
223	Sao Tome and Principe	ST
224	Turkmenistan	TM
225	Cuba	CU
226	Dominica	DM
227	Saint Kitts and Nevis	KN
228	Aruba	AW

Code	Country	Abbreviation
229	Falkland Islands	FK
230	Turks and Caicos Islands	TC
231	Caribbean Netherlands	BQ
232	Sint Maarten	SX
233	Montserrat	MS
234	Anguilla	AI
235	Saint Pierre and Miquelon	PM
236	Åland Islands	AX
237	Norfolk Island	NF
238	Antarctica	AQ
239	Cook Islands	CK
240	Christmas Island	CX
241	Other countries in Europe	EU

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeNetworkRegionBlock
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeNetworkRegionBlockResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Config>
    <RegionBlockSwitch>off</RegionBlockSwitch>
    <Countries>1</Countries>
    <Countries>2</Countries>
```

```
<Provinces>11</Provinces>
<Provinces>12</Provinces>
</Config>
</DescribeNetworkRegionBlockResponse>
```

JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "Config": {
    "RegionBlockSwitch": "off",
    "Countries": [
      1,
      2
    ],
    "Provinces": [
      11,
      12
    ]
  }
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.10.14 ConfigNetworkRegionBlock



Configures blocked regions for an Anti-DDoS Pro or Anti-DDoS Premium instance.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ConfigNetworkRegionBlock	The operation that you want to perform. Set the value to <b>ConfigNetworkRegionBlock</b> .

Parameter	Type	Required	Example	Description
<b>Config</b>	String	Yes	<pre>{"RegionBlockSwitch":"off", "Countries":[], "Provinces":[11,12,13,14,15,21,22,23,31,32,33,34,35,36,37,41,42,43,44,45,46,50,51,52,53,54,61,62,63,64,65,71,81,82]}</pre>	<p>Details about the configurations of blocked regions. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>RegionBlockSwitch:</b> the status of the Blocked Regions policy. This field is required and must be of the STRING type. Valid values: <ul style="list-style-type: none"> <li>- <b>on</b></li> <li>- <b>off</b></li> </ul> </li> <li>• <b>Countries:</b> the codes of the regions outside China from which you want to block requests, which must be of the ARRAY type.</li> <li>• <b>Provinces:</b> the codes of the regions inside China from which you want to block requests, which must be of the ARRAY type.</li> </ul> <div>  <b>Note:</b>  For more information about codes of regions inside China, see the Codes of regions inside China table in this topic. </div>
<b>InstanceId</b>	String	Yes	<code>ddoscoo-cn-mp91j1ao****</code>	<p>The ID of the instance.</p> <div>  <b>Note:</b>  You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances. </div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

#### Codes of regions inside China

Code	Region
11	Beijing
12	Tianjin
13	Hebei
14	Shanxi
15	Nei Mongol
21	Liaoning
22	Jilin
23	Heilongjiang
31	Shanghai
32	Jiangsu
33	Zhejiang
34	Anhui
35	Fujian

Code	Region
36	Jiangxi
37	Shandong
41	Henan
42	Hubei
43	Hunan
44	Guangdong
45	Guangxi
46	Hainan
50	Chongqing
51	Sichuan
52	Guizhou
53	Yunnan
54	Xizang
61	Shaanxi
62	Gansu
63	Qinghai
64	Ningxia
65	Xinjiang
81	Hong Kong S.A.R
71	Taiwan

Code	Region
82	Macao S.A.R

**Codes of regions outside China**

Code	Region	Abbreviation
1	China	CN
2	Australia	AU
3	Japan	JP
4	Thailand	TH
5	India	IN
7	United States	US
8	Germany	DE
9	Netherlands	NL
10	Malaysia	MY
11	Angola	AO
12	South Korea	KR
13	Singapore	SG
14	Kampuchea	KH
16	Philippines	PH
17	Vietnam	VN
18	France	FR
19	Poland	PL



Code	Region	Abbreviation
20	Spain	ES
21	Russia	RU
22	Switzerland	CH
23	United Kingdom	GB
24	Italy	IT
25	Czech Republic	CZ
26	Ireland	IE
27	Denmark	DK
28	Portugal	PT
29	Sweden	SE
30	Ghana	GH
31	Turkey	TR
32	Cameroon	CM
33	South Africa	ZA
34	Finland	FI
35	Hungary	HU
36	United Arab Emirates	AE
37	Greece	GR
38	Brazil	BR
39	Austria	AT

Code	Region	Abbreviation
40	Jordan	JO
41	Belgium	BE
42	Romania	RO
43	Luxembourg	LU
44	Argentina	AR
45	Uganda	UG
46	Armenia	AM
47	Tanzania	TZ
48	Burundi	BI
49	Uruguay	UY
50	Bulgaria	BG
51	Ukraine	UA
52	Israel	IL
53	Qatar	QA
54	Iraq	IQ
55	Lithuania	LT
56	Moldova	MD
57	Uzbekistan	UZ
58	Slovakia	SK
59	Kazakhstan	KZ

Code	Region	Abbreviation
60	Croatia	HR
61	Georgia	GE
62	Estonia	EE
63	Gibraltar	GI
64	Latvia	LV
65	Norway	NO
66	Palestine	PS
67	Cyprus	CY
68	Saudi Arabia	SA
69	Iran	IR
70	Canada	CA
71	American Samoa	AS
72	Syria	SY
73	Kuwait	KW
74	Bahrain	BH
75	Lebanon	LB
76	Oman	OM
77	Azerbaijan	AZ
78	Zambia	ZM
79	Zimbabwe	ZW

Code	Region	Abbreviation
80	Democratic Republic of the Congo	CD
81	Serbia	RS
82	Iceland	IS
83	Slovenia	SI
84	Macedonia	MK
85	Liechtenstein	LI
86	Jersey	JE
87	Bosnia and Herzegovina	BA
88	Chile	CL
89	Peru	PE
90	Kyrgyzstan	KG
91	Reunion	RE
92	Tajikistan	TJ
93	Isle of Man	IM
94	Guernsey	GG
95	Malta	MT
96	Libya	LY
97	Yemen	YE
98	Belarus	BY

Code	Region	Abbreviation
99	Mayotte	YT
100	Guadeloupe	GP
101	Saint Martin	MF
102	Martinique	MQ
103	Guyana	GY
104	Kosovo	XK
105	Indonesia	ID
106	Northern Mariana Islands	MP
107	Dominican Republic	DO
108	Mexico	MX
109	Guam	GU
110	Nigeria	NG
111	Venezuela	VE
112	Puerto Rico	PR
113	Mongolia	MN
114	New Zealand	NZ
115	Bangladesh	BD
116	Pakistan	PK
117	Papua New Guinea	PG
118	Trinidad and Tobago	TT

Code	Region	Abbreviation
119	Lesotho	LS
120	Colombia	CO
121	Costa Rica	CR
123	Ecuador	EC
124	Sri Lanka	LK
125	Egypt	EG
126	British Virgin Islands	VG
127	Jamaica	JM
128	Saint Lucia	LC
129	Cayman Islands	KY
130	Grenada	GD
131	Curacao	CW
132	Panama	PA
133	Barbados	BB
134	The Bahamas	BS
135	Nepal	NP
136	Tokelau	TK
137	Maldives	MV
138	Afghanistan	AF
139	New Caledonia	NC

Code	Region	Abbreviation
140	Fiji	FJ
141	Wallis and Futuna Islands	WF
142	Albania	AL
143	San Marino	SM
144	Montenegro	ME
145	East Timor	TL
146	Monaco	MC
147	Guinea	GN
148	Myanmar	MM
149	Greenland	GL
150	Bermuda	BM
151	Saint Vincent and the Grenadines	VC
152	United States Virgin Islands	VI
153	Suriname	SR
154	Saint Barthelemy	BL
155	Haiti	HT
156	Antigua and Barbuda	AG
157	Liberia	LR
158	Kenya	KE

Code	Region	Abbreviation
159	Botswana	BW
160	Mozambique	MZ
161	Senegal	SN
162	Madagascar	MG
163	Namibia	NA
164	Côte d'Ivoire	CI
165	Sudan	SD
166	Malawi	MW
167	Gabon	GA
168	Mali	ML
169	Benin	BJ
170	Chad	TD
171	Cabo Verde	CV
172	Rwanda	RW
173	Republic of the Congo	CG
174	The Gambia	GM
175	Mauritius	MU
176	Algeria	DZ
177	Eswatini	SZ
178	Burkina Faso	BF



Code	Region	Abbreviation
179	Sierra Leone	SL
180	Somalia	SO
181	Niger	NE
182	Central African Republic	CF
183	Togo	TG
184	South Sudan	SS
185	Equatorial Guinea	GQ
186	Seychelles	SC
187	Djibouti	DJ
188	Morocco	MA
189	Mauritania	MR
190	Comoros	KM
191	British Indian Ocean Territory	IO
192	Tunisia	TN
193	Laos	LA
194	Brunei	BN
195	Bhutan	BT
196	Nauru	NR
197	Vanuatu	VU

Code	Region	Abbreviation
198	Federated States of Micronesia	FM
199	French Polynesia	PF
200	Tonga	TO
201	Honduras	HN
202	Bolivia	BO
203	El Salvador	SV
204	Guatemala	GT
205	Nicaragua	NI
206	Belize	BZ
207	Paraguay	PY
208	French Guiana	GF
209	Andorra	AD
210	Faroe Islands	FO
211	Niue	NU
212	Kiribati	KI
213	Marshall Islands	MH
214	Palau	PW
215	Samoa	WS
216	Solomon Islands	SB

Code	Region	Abbreviation
217	Tuvalu	TV
218	North Korea	KP
219	Vatican City	VA
220	Eritrea	ER
221	Ethiopia	ET
222	Guinea-Bissau	GW
223	Sao Tome and Principe	ST
224	Turkmenistan	TM
225	Cuba	CU
226	Dominica	DM
227	Saint Kitts and Nevis	KN
228	Aruba	AW
229	Falkland Islands	FK
230	Turks and Caicos Islands	TC
231	Caribbean Netherlands	BQ
232	Sint Maarten	SX
233	Montserrat	MS
234	Anguilla	AI
235	Saint Pierre and Miquelon	PM
236	Åland Islands	AX

Code	Region	Abbreviation
237	Norfolk Island	NF
238	Antarctica	AQ
239	Cook Islands	CK
240	Christmas Island	CX
241	Other regions in Europe	EU

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ConfigNetworkRegionBlock
&Config={"RegionBlockSwitch":"off","Countries":[],"Provinces":[11,12,13,14,15,21,22,23,31,32,33,34,35,36,37,41,42,43,44,45,46,50,51,52,53,54,61,62,63,64,65,71,81,82]}
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameter>
```

#### Sample success responses

##### XML format

```
<ConfigNetworkRegionBlockResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</ConfigNetworkRegionBlockResponse>
```

##### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.10.15 DescribeBlockStatus

Queries the Diversion from Origin Server configurations of one or more Anti-DDoS Pro instances.



### Note:

This operation is suitable only for Anti-DDoS Pro.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeBlockStatus	The operation that you want to perform. Set the value to <b>DescribeBlockStatus</b> .
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N.  <div> <b>Note:</b>            You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Set the value to <b>cn-hangzhou</b> , which indicates an Anti-DDoS Pro instance.

## Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.
StatusList	Array		Details about the Diversion from Origin Server configurations of the instance.
BlockStatusList	Array		Details about the Diversion from Origin Server configuration.
BlockStatus	String	areablock	The status of the network traffic from a specific region. Valid values: <ul style="list-style-type: none"> <li><b>areablock</b>: The network traffic is blocked.</li> <li><b>normal</b>: The network traffic is not blocked.</li> </ul>
EndTime	Long	1540196323	The end time of the blocking. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Line	String	cut	The blocked line. Valid values: <ul style="list-style-type: none"> <li><b>ct</b>: China Telecom (International)</li> <li><b>cut</b>: China Unicom (International)</li> </ul>
StartTime	Long	1540195323	The start time of the blocking. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Ip	String	203.***.***.88	The IP address of the instance.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeBlockStatus
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeBlockStatusResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <StatusList>
    <Ip>203. ***. ***.88</Ip>
    <BlockStatusList>
      <BlockStatus>areablock</BlockStatus>
      <Line>cut</Line>
      <StartTime>1540195323</StartTime>
      <EndTime>1540196323</EndTime>
    </BlockStatusList>
  </StatusList>
</DescribeBlockStatusResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "StatusList": [
    {
      "Ip": "203. ***. ***.88",
      "BlockStatusList": [
        {
          "BlockStatus": "areablock",
          "Line": "cut",
          "StartTime": 1540195323,
          "EndTime": 1540196323
        }
      ]
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.10.16 ModifyBlockStatus

Modifies the Diversion from Origin Server configuration of an Anti-DDoS Pro instance.




### Note:

This operation is suitable only for Anti-DDoS Pro.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyBlockStatus	The operation that you want to perform. Set the value to <b>ModifyBlockStatus</b> .
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance.  <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.         </div>
<b>Status</b>	String	Yes	do	The status of the Diversion from Origin Server policy. Valid values: <ul style="list-style-type: none"> <li><b>do</b>: enables the policy.</li> <li><b>undo</b>: disables the policy.</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Set the value to <b>cn-hangzhou</b> , which indicates an Anti-DDoS Pro instance.
<b>Duration</b>	Integer	No	10	The blocking time. Valid values: <b>5</b> to <b>43200</b> . Unit: minutes.  <div>  <b>Note:</b>            If you set <b>Status</b> to <b>do</b>, you must also specify this parameter.         </div>



Parameter	Type	Required	Example	Description
Lines.N	RepeatListNo	No	ct	Line N to block. Valid values: <ul style="list-style-type: none"><li>• <b>ct</b>: China Telecom (International)</li><li>• <b>cut</b>: China Unicom (International)</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyBlockStatus
&InstanceId=ddoscoo-cn-mp91j1ao****
&Status=do
&Duration=10
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ModifyBlockStatusResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</ModifyBlockStatusResponse>
```

##### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.10.17 DescribeUnBlockCount

Queries the remaining quota that you can use the Diversion from Origin Server policy.



#### Note:

This operation is suitable only for Anti-DDoS Pro.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeUnBlockCount	The operation that you want to perform. Set the value to <b>DescribeUnBlockCount</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Set the value to <b>cn-hangzhou</b> , which indicates an Anti-DDoS Pro instance.
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

## Response parameters

Parameter	Type	Example	Description
RemainCount	Integer	7	The remaining quota that you can use the Diversion from Origin Server policy.
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

Parameter	Type	Example	Description
TotalCount	Integer	10	The total quota that you can use the Diversion from Origin Server policy.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeUnBlockCount
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeUnBlockCountResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <TotalCount>10</TotalCount>
  <RemainCount>7</RemainCount>
</DescribeUnBlockCountResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "TotalCount": 10,
  "RemainCount": 7
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.11 Protection for website services


### 12.11.1 DescribeWebCcProtectSwitch

Queries the status of each protection policy for websites.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebCcProtectSwitch	The operation that you want to perform. Set the value to <b>DescribeWebCcProtectSwitch</b> .
<b>Domains.N</b>	RepeatList	Yes	www.aliyun.com	The domain name of website N.  <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

## Response parameters

Parameter	Type	Example	Description
ProtectSwitchList	Array		The status of each protection policy for a website.

Parameter	Type	Example	Description
AiMode	String	defense	The mode of the Intelligent Protection policy. Valid values: <ul style="list-style-type: none"> <li>• <b>watch</b>: the Warning mode</li> <li>• <b>defense</b>: the Defense mode</li> </ul>
AiRuleEnable	Integer	1	The status of the Intelligent Protection policy. Valid values: <ul style="list-style-type: none"> <li>• <b>0</b>: The policy is disabled.</li> <li>• <b>1</b>: The policy is enabled.</li> </ul>
AiTemplate	String	level60	The level of the Intelligent Protection policy. Valid values: <ul style="list-style-type: none"> <li>• <b>level30</b>: the Low level</li> <li>• <b>level60</b>: the Normal level</li> <li>• <b>level90</b>: the Strict level</li> </ul>
BlackWhiteListEnable	Integer	1	The status of the Black Lists and White Lists (Domain Names) policy. Valid values: <ul style="list-style-type: none"> <li>• <b>0</b>: The policy is disabled.</li> <li>• <b>1</b>: The policy is enabled.</li> </ul>
CcCustomRuleEnable	Integer	0	The status of the Custom Rule switch for the Frequency Control policy. Valid values: <ul style="list-style-type: none"> <li>• <b>0</b>: The switch is turned off.</li> <li>• <b>1</b>: The switch is turned on.</li> </ul>
CcEnable	Integer	1	The status of the Frequency Control policy. Valid values: <ul style="list-style-type: none"> <li>• <b>0</b>: The policy is disabled.</li> <li>• <b>1</b>: The policy is enabled.</li> </ul>

Parameter	Type	Example	Description
CcTemplate	String	default	The mode of the Frequency Control policy. Valid values: <ul style="list-style-type: none"> <li><b>default</b>: the Normal mode</li> <li><b>gf_under_attack</b>: the Emergency mode</li> <li><b>gf_sos_verify</b>: the Strict mode</li> <li><b>gf_sos_enhance</b>: the Super Strict mode</li> </ul>
Domain	String	www.aliyun.com	The domain name of the website.
PreciseRuleEnable	Integer	0	The status of the Accurate Access Control policy. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: The policy is disabled.</li> <li><b>1</b>: The policy is enabled.</li> </ul>
RegionBlockEnable	Integer	0	The status of the Blocked Regions (Domain Names) policy. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: The policy is disabled.</li> <li><b>1</b>: The policy is enabled.</li> </ul>
RequestId	String	3ADD9EED-CA4B-488C-BC82-01B0B899363D	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeWebCcProtectSwitch
&Domains.1=www.aliyun.com
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeWebCcProtectSwitchResponse>
  <RequestId>3ADD9EED-CA4B-488C-BC82-01B0B899363D</RequestId>
  <ProtectSwitchList>
    <CcEnable>1</CcEnable>
    <BlackWhiteListEnable>1</BlackWhiteListEnable>
    <AiRuleEnable>1</AiRuleEnable>
    <CcCustomRuleEnable>0</CcCustomRuleEnable>
```

```
<PreciseRuleEnable>0</PreciseRuleEnable>
<Domain>www.aliyun.com</Domain>
<AiMode>defense</AiMode>
<RegionBlockEnable>0</RegionBlockEnable>
<CcTemplate>default</CcTemplate>
<AiTemplate>level60</AiTemplate>
</ProtectSwitchList>
</DescribeWebCcProtectSwitchResponse>
```

JSON format

```
{
  "RequestId": "3ADD9EED-CA4B-488C-BC82-01B0B899363D",
  "ProtectSwitchList": [
    {
      "CcEnable": 1,
      "BlackWhiteListEnable": 1,
      "AiRuleEnable": 1,
      "CcCustomRuleEnable": 0,
      "PreciseRuleEnable": 0,
      "Domain": "www.aliyun.com",
      "AiMode": "defense",
      "RegionBlockEnable": 0,
      "CcTemplate": "default",
      "AiTemplate": "level60"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.11.2 ModifyWebAIProtectSwitch


Enables or disables the Intelligent Protection policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebAIProtectSwitch	The operation that you want to perform. Set the value to <b>ModifyWebAIProtectSwitch</b> .

Parameter	Type	Required	Example	Description
<b>Config</b>	String	Yes	<code>{"AiRuleEnable": 1}</code>	<p>Details about the Intelligent Protection policy. This parameter is a JSON string. The field in the value is described as follows:</p> <ul style="list-style-type: none"> <li>• <b>AiRuleEnable</b>: the status of the Intelligent Protection policy. This field is required and must be of the INTEGER type. Valid values: <ul style="list-style-type: none"> <li>- <b>0</b>: disables the policy.</li> <li>- <b>1</b>: enables the policy.</li> </ul> </li> </ul>
<b>Domain</b>	String	Yes	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>  A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names. </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>



Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebAIProtectSwitch
&Config={"AiRuleEnable": 1},
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ModifyWebAIProtectSwitchResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyWebAIProtectSwitchResponse>
```

##### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.11.3 ModifyWebAIProtectMode


Modifies the mode settings of the Intelligent Protection policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebAIProtectMode	The operation that you want to perform. Set the value to <b>ModifyWebAIProtectMode</b> .
<b>Config</b>	String	Yes	{"AiTemplate": "level60", "AiMode": "defense"}	Details about the Intelligent Protection policy. This parameter is a JSON string. The fields in the value are described as follows: <ul style="list-style-type: none"><li>• <b>AiTemplate</b>: the level of the Intelligent Protection policy. This field is required and must be of the STRING type. Valid values:<ul style="list-style-type: none"><li>- <b>level30</b>: the Low level</li><li>- <b>level60</b>: the Normal level</li><li>- <b>level90</b>: the Strict level</li></ul></li><li>• <b>AiMode</b>: the mode of the Intelligent Protection policy. This field is required and must be of the STRING type. Valid values:<ul style="list-style-type: none"><li>- <b>watch</b>: the Warning mode</li><li>- <b>defense</b>: the Defense mode</li></ul></li></ul>

Parameter	Type	Required	Example	Description
<b>Domain</b>	String	Yes	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou:</b> mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1:</b> outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebAIProtectMode
&Config={"AiTemplate":"level60","AiMode":"defense"}
```

```
&Domain=www.aliyun.com  
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifyWebAIProtectModeResponse>  
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>  
</ModifyWebAIProtectModeResponse>
```

JSON format

```
{  
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"  
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.11.4 ModifyWebIpSetSwitch


Enables or disables the Black Lists and White Lists (Domain Names) policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebIpSetSwitch	The operation that you want to perform. Set the value to <b>ModifyWebIpSetSwitch</b> .

Parameter	Type	Required	Example	Description
<b>Config</b>	String	Yes	<code>{"BwlistEnable": 1}</code>	<p>Details about the Black Lists and White Lists (Domain Names) policy. This parameter is a JSON string. The field in the value is described as follows:</p> <ul style="list-style-type: none"> <li>• <b>Bwlist_Enable</b>: the status of the Black Lists and White Lists (Domain Names) policy. This field is required and must be of the INTEGER type. Valid values: <ul style="list-style-type: none"> <li>- <b>0</b>: disables the policy.</li> <li>- <b>1</b>: enables the policy.</li> </ul> </li> </ul>
<b>Domain</b>	String	Yes	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>  A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names. </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebIpSetSwitch
&Config={"BwlistEnable":1}
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ModifyWebIpSetSwitchResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyWebIpSetSwitchResponse>
```

##### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.5 ConfigWebIpSet

Configures the IP address whitelist and blacklist for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ConfigWebIpSet	The operation that you want to perform. Set the value to <b>ConfigWebIpSet</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.   <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>BlackList.N</b>	RepeatList	No	1.1.1.1	IP address N or CIDR block N that you want to add to the blacklist. The maximum value of N is 200. You can add a maximum of 200 IP addresses or CIDR blocks to the blacklist.
<b>WhiteList.N</b>	RepeatList	No	2.2.2.2/24	IP address N or CIDR block N that you want to add to the whitelist. The maximum value of N is 200. You can add a maximum of 200 IP addresses or CIDR blocks to the whitelist.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ConfigWebIpSet
&Domain=www.aliyun.com
&BlackList.1=1.1.1.1
&WhiteList.1=2.2.2.2/24
```



&<Common request parameters>

Sample success responses

XML format

```
<ConfigWebIpSetResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigWebIpSetResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.6 EnableWebCC

Enables the Frequency Control policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	EnableWebCC	The operation that you want to perform. Set the value to <b>EnableWebCC</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=EnableWebCC
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<EnableWebCCResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</EnableWebCCResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.7 DisableWebCC

Disables the Frequency Control policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DisableWebCC	The operation that you want to perform. Set the value to <b>DisableWebCC</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DisableWebCC
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<DisableWebCCResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</DisableWebCCResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.8 ConfigWebCCTemplate

Configures the mode of the Frequency Control policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ConfigWebCCTemplate	The operation that you want to perform. Set the value to <b>ConfigWebCCTemplate</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.

Parameter	Type	Required	Example	Description
<b>Template</b>	String	Yes	default	The mode of the Frequency Control policy. Valid values: <ul style="list-style-type: none"> <li>• <b>default</b>: the Normal mode</li> <li>• <b>gf_under_attack</b>: the Emergency mode</li> <li>• <b>gf_sos_verify</b>: the Strict mode</li> <li>• <b>gf_sos_enhance</b>: the Super Strict mode</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ConfigWebCCTemplate
```

```
&Domain=www.aliyun.com
&Template=default
&<Common request parameters>
```

Sample success responses

XML format

```
<ConfigWebCCTemplateResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ConfigWebCCTemplateResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.9 EnableWebCCRule

Turns on the Custom Rule switch of the Frequency Control policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	EnableWebCCRule	The operation that you want to perform. Set the value to <b>EnableWebCCRule</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website. <div> <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.</div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=EnableWebCCRule
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<EnableWebCCRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```



```
</EnableWebCCRuleResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.10 DisableWebCCRule

Turns off the Custom Rule switch of the Frequency Control policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Name	Type	Required	Example	Description
<b>Action</b>	String	Yes	DisableWebCCRule	The operation that you want to perform. Set the value to <b>DisableWebCCRule</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.

Name	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DisableWebCCRule
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<DisableWebCCRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</DisableWebCCRuleResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.11 DescribeWebCCRules

Queries the custom frequency control rules that are created for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebCCRules	The operation that you want to perform. Set the value to <b>DescribeWebCCRules</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>PageSize</b>	String	Yes	10	The number of entries to return on each page.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>PageNumber</b>	Integer	No	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .

### Response parameters

Parameter	Type	Example	Description
RequestId	String	EAED912D-909E-45F0-AF74-AC0CCDCAE314	The ID of the request.
TotalCount	Long	1	The total number of returned custom frequency control rules.
WebCCRules	Array		Details about the custom frequency control rule.

Parameter	Type	Example	Description
Act	String	close	The blocking type. Valid values: <ul style="list-style-type: none"><li>• <b>close</b>: Block</li><li>• <b>captcha</b>: Captcha Verification</li></ul>
Count	Integer	3	The number of requests that is allowed from an individual IP address. Valid values: <b>2</b> to <b>2000</b> .
Interval	Integer	5	The check intervals. Valid values: <b>5</b> to <b>10800</b> . Unit: seconds.
Mode	String	prefix	The matching mode. Valid values: <ul style="list-style-type: none"><li>• <b>prefix</b>: Prefix Match</li><li>• <b>match</b>: Exact Match</li></ul>
Name	String	wq	The name of the custom frequency control rule.
Ttl	Integer	60	The blocking duration. Valid values: <b>1</b> to <b>1440</b> . Unit: minutes.
Uri	String	/hello	The check path.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeWebCCRules
&Domain=www.aliyun.com
&PageSize=10
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeWebCCRulesResponse>
  <TotalCount>1</TotalCount>
  <RequestId>EAED912D-909E-45F0-AF74-AC0CCDCAE314</RequestId>
  <WebCCRules>
    <Act>close</Act>
    <Mode>prefix</Mode>
    <Count>3</Count>
    <Ttl>60</Ttl>
```

```
<Uri>/hello</Uri>
<Name>wq</Name>
<Interval>5</Interval>
</WebCCRules>
</DescribeWebCCRulesResponse>
```

JSON format

```
{
  "TotalCount": 1,
  "RequestId": "EAED912D-909E-45F0-AF74-AC0CCDCAE314",
  "WebCCRules": [
    {
      "Act": "close",
      "Mode": "prefix",
      "Count": 3,
      "Ttl": 60,
      "Uri": "/hello",
      "Name": "wq",
      "Interval": 5
    }
  ]
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.11.12 CreateWebCCRule



Creates a custom frequency control rule for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	CreateWebC CRule	The operation that you want to perform. Set the value to <b>CreateWebCCRule</b> .
<b>Act</b>	String	Yes	close	The blocking type. Valid values: <ul style="list-style-type: none"><li><b>close</b>: Block</li><li><b>captcha</b>: Captcha Verification</li></ul>

Parameter	Type	Required	Example	Description
<b>Count</b>	Integer	Yes	60	The number of requests that is allowed from an individual IP address. Valid values: <b>2</b> to <b>2000</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>Interval</b>	Integer	Yes	20	The check intervals. Valid values: <b>5</b> to <b>10800</b> . Unit: seconds.
<b>Mode</b>	String	Yes	prefix	The matching mode. Valid values : <ul style="list-style-type: none"> <li><b>prefix</b>: Prefix Match</li> <li><b>match</b>: Exact Match</li> </ul> <div>  <b>Note:</b>            If the <b>Uri</b> of the check path contains parameters, you must set the value to Prefix Match.         </div>
<b>Name</b>	String	Yes	testrule	The name of the custom frequency control rule. The name can be up to 128 characters in length and contain letters, digits, and underscores (_).
<b>Ttl</b>	Integer	Yes	10	The blocking duration. Valid values: <b>1</b> to <b>1440</b> . Unit: minutes.
<b>Uri</b>	String	Yes	/abc/a.php	The check path.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=CreateWebCCRule
&Act=close
&Count=60
&Domain=www.aliyun.com
&Interval=20
&Mode=prefix
&Name=testrule
&Ttl=10
&Uri=/abc/a.php
&<Common request parameters>
```

#### Sample success responses



#### XML format

```
<CreateWebCCRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</CreateWebCCRuleResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

#### Error codes

For a list of error codes, visit the [API Error Center](#).

### 12.11.13 ModifyWebCCRule


Modifies the custom frequency control rule of a website.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

#### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebCCRule	The operation that you want to perform. Set the value to <b>ModifyWebCCRule</b> .
<b>Act</b>	String	Yes	close	The blocking type. Valid values: <ul style="list-style-type: none"><li><b>close</b>: Block</li><li><b>captcha</b>: Captcha Verification</li></ul>
<b>Count</b>	Integer	Yes	3	The number of requests that is allowed from an individual IP address. Valid values: <b>2</b> to <b>2000</b> .

Parameter	Type	Required	Example	Description
<b>Domain</b>	String	Yes	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>Interval</b>	Integer	Yes	30	The check intervals. Valid values: <b>5</b> to <b>10800</b> . Unit: seconds.
<b>Mode</b>	String	Yes	prefix	<p>The matching mode. Valid values :</p> <ul style="list-style-type: none"> <li>• <b>prefix</b>: Prefix Match</li> <li>• <b>match</b>: Exact Match</li> </ul>
<b>Name</b>	String	Yes	testrule	The name of the custom frequency control rule.
<b>Ttl</b>	Integer	Yes	10	The blocking duration. Valid values: <b>1</b> to <b>1440</b> . Unit: minutes.
<b>Uri</b>	String	Yes	/abc	The check path.
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebCCRule
&Act=close
&Count=3
&Domain=www.aliyun.com
&Interval=30
&Mode=prefix
&Name=testrule
&Ttl=10
&Uri=/abc
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ModifyWebCCRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyWebCCRuleResponse>
```

##### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
```

```
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.14 DeleteWebCCRule

Deletes the custom frequency control rule of a website.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteWebCCRule	The operation that you want to perform. Set the value to <b>DeleteWebCCRule</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website. <div> <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.</div>
<b>Name</b>	String	Yes	wq	The name of the custom frequency control rule that you want to delete.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DeleteWebCCRule
&Domain=www.aliyun.com
&Name=wq
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<DeleteWebCCRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</DeleteWebCCRuleResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.11.15 ModifyWebPreciseAccessSwitch


Enables or disables the Accurate Access Control policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebPreciseAccessSwitch	The operation that you want to perform. Set the value to <b>ModifyWebPreciseAccessSwitch</b> .
<b>Config</b>	String	Yes	{"PreciseRuleEnable":0}	The configuration of the Accurate Access Control policy. This parameter is a JSON string. The field in the value is described as follows: <ul style="list-style-type: none"><li>• <b>PreciseRuleEnable</b>: the status of the Accurate Access Control policy. This field is required and must be of the INTEGER type. Valid values:<ul style="list-style-type: none"><li>- <b>0</b>: disables the policy.</li><li>- <b>1</b>: enables the policy.</li></ul></li></ul>

Parameter	Type	Required	Example	Description
<b>Domain</b>	String	Yes	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou:</b> mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1:</b> outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebPreciseAccessSwitch
&Config={"PreciseRuleEnable":0}
```

```
&Domain=www.aliyun.com  
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifyWebPreciseAccessSwitchResponse>  
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>  
</ModifyWebPreciseAccessSwitchResponse>
```

JSON format

```
{  
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"  
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.16 DescribeWebPreciseAccessRule

Queries the accurate access control rules that are created for websites.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters


Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebPreciseAccessRule	The operation that you want to perform. Set the value to <b>DescribeWebPreciseAccessRule</b> .
<b>Domains.N</b>	RepeatList	Yes	www.aliyun.com	The domain name of website N. <div> <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.</div>



Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
PreciseAccessConfigList	Array		The configuration of the accurate access control rule that is created for the website.
Domain	String	www.aliyun.com	The domain name of the website.
RuleList	Array		Details about the accurate access control rule.
Action	String	accept	The action performed if the rule is matched. Valid values: <ul style="list-style-type: none"><li>• <b>accept</b></li><li>• <b>block</b></li><li>• <b>challenge</b></li></ul>

Parameter	Type	Example	Description
ConditionList	Array		The match conditions.
Content	String	1.1.1.1	The match content.
Field	String	ip	The match field.
HeaderName	String	null	<p>The custom HTTP header.</p> <div>  <b>Note:</b>            This parameter is returned only when the <b>Field</b> parameter is <b>header</b>.         </div>
MatchMethod	String	belong	The logical relation.
Expires	Long	0	<p>The validity period of the rule. Unit: seconds. This parameter only takes effect when the <b>Action</b> parameter of a rule is <b>block</b>. Access requests that hit the rule are blocked within the specified validity period of the rule. <b>0</b> indicates that the rule takes effect all the time.</p>
Name	String	testrule	The name of the rule.
Owner	String	manual	<p>The mode of how the rule was created . Valid values:</p> <ul style="list-style-type: none"> <li>• <b>manual</b>: manually created</li> <li>• <b>auto</b>: automatically generated</li> </ul>
RequestId	String	209EEFBF-B0C7-441E-8C28-D0945A57A638	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeWebPreciseAccessRule
&Domains.1=www.aliyun.com
```

## &<Common request parameters>

### Sample success responses

#### XML format

```
<DescribeWebPreciseAccessRuleResponse>
  <PreciseAccessConfigList>
    <RuleList>
      <Owner>manual</Owner>
      <Action>accept</Action>
      <ConditionList>
        <MatchMethod>belong</MatchMethod>
        <Field>ip</Field>
        <HeaderName></HeaderName>
        <Content>1. ***. ***.2</Content>
      </ConditionList>
      <Expires>0</Expires>
      <Name>testrule</Name>
    </RuleList>
    <Domain>www.aliyun.com</Domain>
  </PreciseAccessConfigList>
  <RequestId>209EEFBF-B0C7-441E-8C28-D0945A57A638</RequestId>
</DescribeWebPreciseAccessRuleResponse>
```

#### JSON format

```
{
  "PreciseAccessConfigList": [
    {
      "RuleList": [
        {
          "Owner": "manual",
          "Action": "accept",
          "ConditionList": [
            {
              "MatchMethod": "belong",
              "Field": "ip",
              "HeaderName": "",
              "Content": "1. ***. ***.2"
            }
          ],
          "Expires": 0,
          "Name": "testrule"
        }
      ],
      "Domain": "www.aliyun.com"
    }
  ],
  "RequestId": "209EEFBF-B0C7-441E-8C28-D0945A57A638"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.17 ModifyWebPreciseAccessRule



Modifies the accurate access control rule of a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebPreciseAccessRule	The operation that you want to perform. Set the value to <b>ModifyWebPreciseAccessRule</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.

Parameter	Type	Required	Example	Description
<b>Rules</b>	String	Yes	<pre>[{"action":"block","name":"testrule","condition":{"field":"uri","match_method":"contain","content":"/test/123"}}]</pre>	<p>Details about the accurate access control rule. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>action:</b> the action performed if the rule is matched. This field is required and must be of the STRING type. Valid values: <ul style="list-style-type: none"> <li>- <b>accept</b></li> <li>- <b>block</b></li> <li>- <b>challenge</b></li> </ul> </li> <li>• <b>name:</b> the name of the rule. This field is required and must be of the STRING type.</li> <li>• <b>condition:</b> the match conditions. This field is required and must be of the MAP type.</li> </ul> <div data-bbox="1018 1182 1436 1482">  <b>Note:</b> The AND operator is used to define the relationship among multiple match conditions. </div> <ul style="list-style-type: none"> <li>- <b>field:</b> the match field. It is required and must be of the STRING type.</li> <li>- <b>match_method:</b> the logical relation. It is required and must be of the STRING type.</li> </ul> <div data-bbox="1053 1803 1436 2240">  <b>Note:</b> For information about the mappings between the <b>field</b> and <b>match_method</b> parameters, see the Mappings between the field and match_method parameters table in this </div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>Expires</b>	Integer	No	600	The validity period of the rule. Unit: seconds. This parameter only takes effect when <b>action</b> is <b>block</b> . Access requests that hit the rule are blocked within the specified validity period of the rule. If you do not specify this parameter, this rule takes effect all the time.

#### Mappings between the field and match\_method parameters

field	Description	match_method
<b>ip</b>	The source IP address of the request.	<b>belong</b> : the Is Part Of relation  <b>nbelong</b> : the Is Not Part Of relation

field	Description	match_method
uri	The URI of the request.	<b>contain:</b> the Contains relation <b>ncontain:</b> the Does Not Contain relation <b>equal:</b> the Equals relation <b>nequal:</b> the Does Not Equal relation <b>lless:</b> the Is Shorter Than relation <b>lequal:</b> the Has a Length Of relation <b>lgreat:</b> the Is Longer Than relation <b>regular:</b> The match content is the regular expression of the URI.

field	Description	match_method
referer	The source URI of the request , namely, the page from which the access request is redirected.	<b>contain</b> : the Contains relation <b>ncontain</b> : the Does Not Contain relation <b>equal</b> : the Equals relation <b>nequal</b> : the Does Not Equal relation <b>lless</b> : the Is Shorter Than relation <b>lequal</b> : the Has a Length Of relation <b>lgreat</b> : the Is Longer Than relation <b>nexist</b> : the Does Not Exist relation <b>regular</b> : The match content is the regular expression of the URI.



field	Description	match_method
<b>user-agent</b>	The browser ID, rendering engine ID, version information, and other browser-related information of the client that initiates the request.	<b>contain:</b> the Contains relation <b>ncontain:</b> the Does Not Contain relation <b>equal:</b> the Equals relation <b>nequal:</b> the Does Not Equal relation <b>lless:</b> the Is Shorter Than relation <b>lequal:</b> the Has a Length Of relation <b>lgreat:</b> the Is Longer Than relation <b>regular:</b> The match content is the regular expression of the information.

field	Description	match_method
<b>params</b>	The parameter part in the request URL, usually the part that follows the question mark (?) in the URL. For example, in <code>www.abc.com/index.html? action=login</code> , <code>action=login</code> is the parameter part.	<b>contain:</b> the Contains relation <b>ncontain:</b> the Does Not Contain relation <b>equal:</b> the Equals relation <b>nequal:</b> the Does Not Equal relation <b>lless:</b> the Is Shorter Than relation <b>lequal:</b> the Has a Length Of relation <b>lgreat:</b> the Is Longer Than relation
<b>cookie</b>	The cookie information in the request.	<b>contain:</b> the Contains relation <b>ncontain:</b> the Does Not Contain relation <b>equal:</b> the Equals relation <b>nequal:</b> the Does Not Equal relation <b>lless:</b> the Is Shorter Than relation <b>lequal:</b> the Has a Length Of relation <b>lgreat:</b> the Is Longer Than relation <b>nexist:</b> the Does Not Exist relation

field	Description	match_method
<b>content-type</b>	The HTTP content type of the response specified by the request, namely, MIME type information.	<b>contain</b> : the Contains relation <b>ncontain</b> : the Does Not Contain relation <b>equal</b> : the Equals relation <b>nequal</b> : the Does Not Equal relation <b>lless</b> : the Is Shorter Than relation <b>lequal</b> : the Has a Length Of relation <b>lgreat</b> : the Is Longer Than relation

field	Description	match_method
<b>x-forwarded-for</b>	The actual IP address of the client that initiates an access request. X-Forwarded-For (XFF) is used to identify the HTTP request header field of the initial IP address of the client that initiates the access request that is forwarded through an HTTP proxy server or a Server Load Balancer (SLB) instance. XFF is only included in the access requests that are forwarded by the HTTP proxy or SLB instances.	<b>contain:</b> the Contains relation <b>ncontain:</b> the Does Not Contain relation <b>equal:</b> the Equals relation <b>nequal:</b> the Does Not Equal relation <b>lless:</b> the Is Shorter Than relation <b>lequal:</b> the Has a Length Of relation <b>lgreat:</b> the Is Longer Than relation <b>nexist:</b> the Does Not Exist relation <b>Regular:</b> The match content is the regular expression of the IP address.
<b>content-length</b>	The amount of bytes in the HTTP body of the request.	<b>vless:</b> the Is Smaller Than relation <b>vequal:</b> the Has a Value Of relation <b>vgreat:</b> the Is Larger Than relation

field	Description	match_method
<b>post-body</b>	The content of the request.	<b>contain:</b> the Contains relation <b>ncontain:</b> the Does Not Contain relation <b>equal:</b> the Equals relation <b>nequal:</b> the Does Not Equal relation <b>regular:</b> The match content is the regular expression of the HTTP request header.
<b>http-method</b>	The request method, such as GET and POST.	<b>equal:</b> the Equals relation <b>nequal:</b> the Does Not Equal relation
<b>header</b>	The header of the request, which is used to customize the HTTP header.	<b>contain:</b> the Contains relation <b>ncontain:</b> the Does Not Contain relation <b>equal:</b> the Equals relation <b>nequal:</b> the Does Not Equal relation <b>lless:</b> the Is Shorter Than relation <b>lequal:</b> the Has a Length Of relation <b>lgreat:</b> the Is Longer Than relation <b>nexist:</b> the Does Not Exist relation

## Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=ModifyWebPreciseAccessRule
&Domain=www.aliyun.com
&Rules=[{"action":"block","name":"testrule","condition":{"field":"uri","match_method":"
contain","content":"/test/123"}}]
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<ModifyWebPreciseAccessRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyWebPreciseAccessRuleResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.18 DeleteWebPreciseAccessRule

Deletes one or more accurate access control rules that are created for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteWebPreciseAccessRule	The operation that you want to perform. Set the value to <b>DeleteWebPreciseAccessRule</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>RuleNames.N</b>	RepeatList	Yes	testrule	The name of rule N that you want to delete.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

## Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DeleteWebPreciseAccessRule
&Domain=www.aliyun.com
&RuleNames.1=testrule
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DeleteWebPreciseAccessRule>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteWebPreciseAccessRule>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.11.19 ModifyWebAreaBlockSwitch


Enables or disables the Blocked Regions (Domain Names) policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.



## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebAreaBlockSwitch	The operation that you want to perform. Set the value to <b>ModifyWebAreaBlockSwitch</b> .
<b>Config</b>	String	Yes	{"RegionblockEnable": 1}	<p>The status of the Blocked Regions (Domain Names) policy. This parameter is a JSON string. The field in the value is described as follows:</p> <ul style="list-style-type: none"> <li>• <b>RegionblockEnable</b>: the status of the Blocked Regions (Domain Names) policy. This field is required and must be of the INTEGER type. Valid values: <ul style="list-style-type: none"> <li>- <b>1</b>: enables the policy.</li> <li>- <b>0</b>: disables the policy.</li> </ul> </li> </ul>
<b>Domain</b>	String	Yes	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>  A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names. </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebAreaBlockSwitch
&Config={"RegionblockEnable": 1}
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ModifyWebAreaBlockSwitchResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyWebAreaBlockSwitchResponse>
```

##### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.11.20 DescribeWebAreaBlockConfigs

Queries the Blocked Regions (Domain Names) configurations for websites.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebAreaBlockConfigs	The operation that you want to perform. Set the value to <b>DescribeWebAreaBlockConfigs</b> .
<b>Domains.N</b>	RepeatList	Yes	www.aliyun.com	The domain name of website N.   <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
AreaBlockConfigs	Array		The configuration of the Blocked Regions (Domain Names) policy.
Domain	String	www.aliyun.com	The domain name of the website.
RegionList	Array		The configuration of the blocked region.
Block	Integer	0	Indicates whether the region is blocked. Valid values: <ul style="list-style-type: none"><li><b>0</b>: The region is not blocked.</li><li><b>1</b>: The region is blocked.</li></ul>
Region	String	CN-SHANGHAI	The region.
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeWebAreaBlockConfigs
&Domains.1=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

## XML format

```
<DescribeWebAreaBlockConfigsResponse>
  <AreaBlockConfigs>
    <RegionList>
      <Block>1</Block>
      <Region>CN-YUNNAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HEILONGJIANG</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>OVERSEAS-ANTARCTICA</Region>
    </RegionList>
    <RegionList>
      <Block>1</Block>
      <Region>OVERSEAS-EUROPE</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-BEIJING</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HENAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HUNAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-FUJIAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-JIANGSU</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-ZHEJIANG</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-HAINAN</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-TIBET</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-INNERMONGOLIA</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-NINGXIA</Region>
    </RegionList>
    <RegionList>
      <Block>0</Block>
      <Region>CN-SHAANXI</Region>
    </RegionList>
  </AreaBlockConfigs>
</DescribeWebAreaBlockConfigsResponse>
```

```
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-GUANGDONG</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-QINGHAI</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>OVERSEAS-NAMERICA</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>OVERSEAS-SAMERICA</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-SHANGHAI</Region>
</RegionList>
<RegionList>
  <Block>1</Block>
  <Region>CN-GUANGXI</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>OVERSEAS-ASIA</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>OVERSEAS-OCEANIA</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-MACAU</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-GUIZHOU</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-JILIN</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-ANHUI</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-JIANGXI</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-HEBEI</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-CHONGQING</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>OVERSEAS-AFRICA</Region>
```

```

</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-SICHUAN</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-TIANJIN</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-XINJIANG</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-LIAONING</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-GANSU</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-HONGKONG</Region>
</RegionList>
<RegionList>
  <Block>1</Block>
  <Region>CN-TAIWAN</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-SHANDONG</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-SHANXI</Region>
</RegionList>
<RegionList>
  <Block>0</Block>
  <Region>CN-HUBEI</Region>
</RegionList>
<Domain>www.aliyun.com</Domain>
</AreaBlockConfigs>
<RequestId>044D33A9-80B9-4F07-BA63-9207CAD53263</RequestId>
</DescribeWebAreaBlockConfigsResponse>

```

### JSON format

```

{
  "AreaBlockConfigs": [
    {
      "RegionList": [
        {
          "Block": 1,
          "Region": "CN-YUNNAN"
        },
        {
          "Block": 0,
          "Region": "CN-HEILONGJIANG"
        },
        {
          "Block": 0,
          "Region": "OVERSEAS-ANTARCTICA"
        }
      ]
    }
  ]
}

```

```
    },
    {
      "Block": 1,
      "Region": "OVERSEAS-EUROPE"
    },
    {
      "Block": 0,
      "Region": "CN-BEIJING"
    },
    {
      "Block": 0,
      "Region": "CN-HENAN"
    },
    {
      "Block": 0,
      "Region": "CN-HUNAN"
    },
    {
      "Block": 0,
      "Region": "CN-FUJIAN"
    },
    {
      "Block": 0,
      "Region": "CN-JIANGSU"
    },
    {
      "Block": 0,
      "Region": "CN-ZHEJIANG"
    },
    {
      "Block": 0,
      "Region": "CN-HAINAN"
    },
    {
      "Block": 0,
      "Region": "CN-TIBET"
    },
    {
      "Block": 0,
      "Region": "CN-INNERMONGOLIA"
    },
    {
      "Block": 0,
      "Region": "CN-NINGXIA"
    },
    {
      "Block": 0,
      "Region": "CN-SHAANXI"
    },
    {
      "Block": 0,
      "Region": "CN-GUANGDONG"
    },
    {
      "Block": 0,
      "Region": "CN-QINGHAI"
    },
    {
      "Block": 0,
      "Region": "OVERSEAS-NAMERICA"
    },
    {
      "Block": 0,
      "Region": "OVERSEAS-SAMERICA"
    }
  ],
  "Total": 15
}
```



```
    },
    {
      "Block": 0,
      "Region": "CN-SHANGHAI"
    },
    {
      "Block": 1,
      "Region": "CN-GUANGXI"
    },
    {
      "Block": 0,
      "Region": "OVERSEAS-ASIA"
    },
    {
      "Block": 0,
      "Region": "OVERSEAS-OCEANIA"
    },
    {
      "Block": 0,
      "Region": "CN-MACAU"
    },
    {
      "Block": 0,
      "Region": "CN-GUIZHOU"
    },
    {
      "Block": 0,
      "Region": "CN-JILIN"
    },
    {
      "Block": 0,
      "Region": "CN-ANHUI"
    },
    {
      "Block": 0,
      "Region": "CN-JIANGXI"
    },
    {
      "Block": 0,
      "Region": "CN-HEBEI"
    },
    {
      "Block": 0,
      "Region": "CN-CHONGQING"
    },
    {
      "Block": 0,
      "Region": "OVERSEAS-AFRICA"
    },
    {
      "Block": 0,
      "Region": "CN-SICHUAN"
    },
    {
      "Block": 0,
      "Region": "CN-TIANJIN"
    },
    {
      "Block": 0,
      "Region": "CN-XINJIANG"
    },
    {
      "Block": 0,
      "Region": "CN-LIAONING"
```

```
{
  {
    "Block": 0,
    "Region": "CN-GANSU"
  },
  {
    "Block": 0,
    "Region": "CN-HONGKONG"
  },
  {
    "Block": 1,
    "Region": "CN-TAIWAN"
  },
  {
    "Block": 0,
    "Region": "CN-SHANDONG"
  },
  {
    "Block": 0,
    "Region": "CN-SHANXI"
  },
  {
    "Block": 0,
    "Region": "CN-HUBEI"
  }
],
"Domain": "www.aliyun.com"
},
"RequestId": "044D33A9-80B9-4F07-BA63-9207CAD53263"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.11.21 ModifyWebAreaBlock


Modifies the blocked regions that are configured in the Blocked Regions (Domain Names) policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebAreaBlock	The operation that you want to perform. Set the value to <b>ModifyWebAreaBlock</b> .

Parameter	Type	Required	Example	Description
<b>Domain</b>	String	Yes	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou:</b> mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1:</b> outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

Parameter	Type	Required	Example	Description
<b>Regions.N</b>	RepeatList	No	CN-SHANGHAI	<p>The name of region N to block. If you do not specify this parameter , the Blocked Regions (Domain Names) policy is disabled. Valid values:</p> <p>Regions inside China:</p> <ul style="list-style-type: none"> <li>• <b>CN-SHANGHAI</b>: Shanghai</li> <li>• <b>CN-YUNNAN</b>: Yunnan</li> <li>• <b>CN-INNERMONGOLIA</b>: Nei Mongol</li> <li>• <b>CN-BEIJING</b>: Beijing</li> <li>• <b>CN-TAIWAN</b>: Taiwan</li> <li>• <b>CN-JILIN</b>: Jilin</li> <li>• <b>CN-SICHUAN</b>: Sichuan</li> <li>• <b>CN-TIANJIN</b>: Tianjin</li> <li>• <b>CN-NINGXIA</b>: Ningxia</li> <li>• <b>CN-ANHUI</b>: Anhui</li> <li>• <b>CN-SHANDONG</b>: Shandong</li> <li>• <b>CN-SHAANXI</b>: Shaanxi</li> <li>• <b>CN-SHANXI</b>: Shanxi</li> <li>• <b>CN-GUANGDONG</b>: Guangdong</li> <li>• <b>CN-GUANGXI</b>: Guangxi</li> <li>• <b>CN-XINJIANG</b>: Xinjiang</li> <li>• <b>CN-JIANGSU</b>: Jiangsu</li> <li>• <b>CN-JIANGXI</b>: Jiangxi</li> <li>• <b>CN-HEBEI</b>: Hebei</li> <li>• <b>CN-HENAN</b>: Henan</li> <li>• <b>CN-ZHEJIANG</b>: Zhejiang</li> <li>• <b>CN-HAINAN</b>: Hainan</li> <li>• <b>CN-HUBEI</b>: Hubei</li> <li>• <b>CN-HUNAN</b>: Hunan</li> <li>• <b>CN-MACAU</b>: Macao S.A.R</li> <li>• <b>CN-GANSU</b>: Gansu</li> <li>• <b>CN-FUJIAN</b>: Fujian</li> <li>• <b>CN-TIBET</b>: Xizang</li> <li>• <b>CN-GUIZHOU</b>: Guizhou</li> <li>• <b>CN-LIAONING</b>: Liaoning</li> <li>• <b>CN-CHONGQING</b>: Chongqing</li> </ul>
				<ul style="list-style-type: none"> <li>• <b>CN-QINGHAI</b>: Qinghai</li> <li>• <b>CN-HONGKONG</b>: Hong Kong S.A.R</li> <li>• <b>CN-MACAU</b>: Macao S.A.R</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc" }	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebAreaBlock
&Domain=www.aliyun.com
&Regions.1=CN-SHANGHAI
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<ModifyWebAreaBlockResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyWebAreaBlockResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.12 Protection for non-website services


### 12.12.1 DescribePortAutoCcStatus

Queries the Intelligent Protection configurations of non-website services.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribePortAutoCcStatus	The operation that you want to perform. Set the value to <b>DescribePortAutoCcStatus</b> .
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N.  <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

## Response parameters

Parameter	Type	Example	Description
PortAutoCcStatus	Array		The configuration of the Intelligent Protection policy.
Mode	String	normal	The mode of the Intelligent Protection policy. Valid values: <ul style="list-style-type: none"> <li><b>normal</b></li> <li><b>loose</b></li> <li><b>strict</b></li> </ul>

Parameter	Type	Example	Description
Switch	String	on	The status of the Intelligent Protection policy. Valid values: <ul style="list-style-type: none"> <li>• <b>on</b></li> <li>• <b>off</b></li> </ul>
WebMode	String	normal	The protection mode for ports 80 and 443. Valid values: <ul style="list-style-type: none"> <li>• <b>normal</b></li> <li>• <b>loose</b></li> <li>• <b>strict</b></li> </ul>
WebSwitch	String	off	The status of the Intelligent Protection policy for ports 80 and 443. Valid values: <ul style="list-style-type: none"> <li>• <b>on</b></li> <li>• <b>off</b></li> </ul>
RequestId	String	BC3C6403-F248-4125-B2C9-8733ED94EA85	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribePortAutoCcStatus
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribePortAutoCcStatusResponse>
  <RequestId>BC3C6403-F248-4125-B2C9-8733ED94EA85</RequestId>
  <PortAutoCcStatus>
    <WebSwitch>off</WebSwitch>
    <Switch>on</Switch>
    <WebMode>normal</WebMode>
    <Mode>normal</Mode>
  </PortAutoCcStatus>
```

```
</DescribePortAutoCcStatusResponse>
```

JSON format

```
{
  "RequestId": "BC3C6403-F248-4125-B2C9-8733ED94EA85",
  "PortAutoCcStatus": [
    {
      "WebSwitch": "off",
      "Switch": "on",
      "WebMode": "normal",
      "Mode": "normal"
    }
  ]
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.12.2 ModifyPortAutoCcStatus

Modifies the Intelligent Protection configuration of a non-website service.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyPortAutoCcStatus	The operation that you want to perform. Set the value to <b>ModifyPortAutoCcStatus</b> .
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	The ID of the instance. <div> <b>Note:</b> You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.</div>



Parameter	Type	Required	Example	Description
<b>Mode</b>	String	Yes	normal	The mode of the Intelligent Protection policy. Valid values: <ul style="list-style-type: none"><li>• <b>normal</b></li><li>• <b>loose</b></li><li>• <b>strict</b></li></ul>
<b>Switch</b>	String	Yes	on	The status of the Intelligent Protection policy. Valid values: <ul style="list-style-type: none"><li>• <b>on</b></li><li>• <b>off</b></li></ul>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyPortAutoCcStatus
&InstanceId=ddoscoo-cn-mp91j1ao****
&Switch=on
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<ModifyPortAutoCcStatusResponse>
```

```
<RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyPortAutoCcStatusResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.12.3 DescribeNetworkRuleAttributes

Queries the mitigation settings of the port forwarding rule for a non-website service, which include session persistence and anti-DDoS protection policies.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeNetworkRuleAttributes	The operation that you want to perform. Set the value to <b>DescribeNetworkRuleAttributes</b> .

Parameter	Type	Required	Example	Description
<b>NetworkRules</b>	String	Yes	<pre>[{"InstanceId": "ddoscoo-cn-mp91j1ao****", "Protocol": "tcp", "FrontendPort": 8080}]</pre>	<p>Details about the port forwarding rule. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>InstanceId</b>: the ID of the instance. This field is required and must be of the STRING type.</li> <li>• <b>Protocol</b>: the forwarding protocol. This field is required and must be of the STRING type. Valid values: <b>tcp</b> and <b>udp</b>.</li> <li>• <b>FrontendPort</b>: the forwarding port. This field is required and must be of the INTEGER type.</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

### Response parameters

Parameter	Type	Example	Description
NetworkRuleAttributes	Array		Details about the mitigation settings of the port forwarding rule, which include session persistence and anti-DDoS protection policies.
Config	Struct		The mitigation settings of the port forwarding rule.

Parameter	Type	Example	Description
Cc	Struct		The protection policy applied when the number of connections initiated from a source IP address frequently exceeds the limit.
Sblack	Array		The protection policy that a source IP address is added to the blacklist when the number of connections initiated from the IP address frequently exceeds the limit.
Cnt	Integer	5	The threshold that the number of connections initiated from a source IP address can exceed the limit. Set the value to <b>5</b> . If the number of connections initiated from a source IP address exceeds the limit five times during the check, the source IP address is added to the blacklist.
During	Integer	60	The check intervals. Set the value to <b>60</b> . Unit: seconds.
Expires	Integer	600	The validity period of the IP address in the blacklist. Valid values: <b>60</b> to <b>604800</b> . Unit: seconds.
Type	Integer	1	The type of the limit that causes a source IP address to be added to the blacklist. Valid values: <ul style="list-style-type: none"> <li><b>1</b>: Source New Connection Rate Limit</li> <li><b>2</b>: Source Concurrent Connection Rate Limit</li> <li><b>3</b>: PPS Limit for Source</li> <li><b>4</b>: Bandwidth Limit for Source</li> </ul>

Parameter	Type	Example	Description
NodataConn	String	off	The status of the Empty Connection switch. Valid values: <ul style="list-style-type: none"> <li><b>on</b></li> <li><b>off</b></li> </ul>
PayloadLen	Struct		The settings of the Packet Length Limit policy.
Max	Integer	6000	The maximum length of a packet. Valid values: <b>0</b> to <b>6000</b> . Unit: bytes.
Min	Integer	0	The minimum length of a packet. Valid values: <b>0</b> to <b>6000</b> . Unit: bytes.
PersistenceTimeout	Integer	0	The timeout period of session persistence. Valid values: <b>30</b> to <b>3600</b> . Unit: seconds. Default value: <b>0</b> , which indicates that session persistence is disabled.
Sla	Struct		The settings of the Speed Limit for Destination policy.
Cps	Integer	100000	The maximum number of new connections per second that can be established over the port of the destination instance. Valid values: <b>100</b> to <b>100000</b> .
CpsEnable	Integer	1	The status of the Destination New Connection Rate Limit switch. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: The switch is turned off.</li> <li><b>1</b>: The switch is turned on.</li> </ul>

Parameter	Type	Example	Description
Maxconn	Integer	1000000	The maximum number of concurrent connections that can be established over the port of the destination instance. Valid values: <b>1000</b> to <b>1000000</b> .
MaxconnEnable	Integer	0	The status of the Destination Concurrent Connection Rate Limit switch. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: The switch is turned off.</li> <li><b>1</b>: The switch is turned on.</li> </ul>
Slimit	Struct		The settings of the Speed Limit for Source policy.
Bps	Long	0	The bandwidth limit for a source IP address. Valid values: <b>1024</b> to <b>268435456</b> . Unit: bytes/s. Default value: <b>0</b> , which indicates that the bandwidth for a source IP address is unlimited.
Cps	Integer	0	The maximum number of new connections per second that can be initiated from a source IP address. Valid values: <b>1</b> to <b>500000</b> .
CpsEnable	Integer	0	The status of the Source New Connection Rate Limit switch. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: The switch is turned off.</li> <li><b>1</b>: The switch is turned on.</li> </ul>

Parameter	Type	Example	Description
CpsMode	Integer	1	The mode of the Source New Connection Rate Limit switch. Valid values: <ul style="list-style-type: none"> <li><b>1</b>: the Manual mode</li> <li><b>2</b>: the Automatic mode</li> </ul>
Maxconn	Integer	0	The maximum number of concurrent connections initiated from a source IP address. Valid values: <b>1</b> to <b>500000</b> .
MaxconnEnable	Integer	0	The status of the Source Concurrent Connection Rate Limit switch. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: The switch is turned off.</li> <li><b>1</b>: The switch is turned on.</li> </ul>
Pps	Long	0	The packets per second (pps) limit for a source IP address. Valid values: <b>1</b> to <b>100000</b> . Unit: packets/s. Default value: <b>0</b> , which indicates that the pps for a source IP address is unlimited.
Synproxy	String	off	The status of the False Source switch. Valid values: <ul style="list-style-type: none"> <li><b>on</b></li> <li><b>off</b></li> </ul>
FrontendPort	Integer	8080	The forwarding port.
InstanceId	String	ddoscoo-cn-mp91j1ao****	The ID of the instance.
Protocol	String	tcp	The forwarding protocol. Valid values: <ul style="list-style-type: none"> <li><b>tcp</b></li> <li><b>udp</b></li> </ul>

Parameter	Type	Example	Description
RequestId	String	F9F2F77D-307C-4F15-8D02-AB5957EEBF97	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeNetworkRuleAttributes
&NetworkRules=[{"InstanceId":"ddoscoo-cn-mp91j1ao****","Protocol":"tcp","FrontendPort":8080}]
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeNetworkRuleAttributesResponse>
  <NetworkRuleAttributes>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <Config>
      <NodataConn>off</NodataConn>
      <Cc></Cc>
      <PersistenceTimeout>0</PersistenceTimeout>
      <PayloadLen>
        <Min>0</Min>
        <Max>6000</Max>
      </PayloadLen>
      <Sla>
        <Cps>100000</Cps>
        <CpsEnable>1</CpsEnable>
        <MaxconnEnable>0</MaxconnEnable>
        <Maxconn>1000000</Maxconn>
      </Sla>
      <Slimit>
        <CpsMode>1</CpsMode>
        <Pps>0</Pps>
        <Bps>0</Bps>
        <Cps>0</Cps>
        <CpsEnable>0</CpsEnable>
        <MaxconnEnable>0</MaxconnEnable>
        <Maxconn>0</Maxconn>
      </Slimit>
      <Synproxy>on</Synproxy>
    </Config>
    <FrontendPort>8080</FrontendPort>
    <Protocol>tcp</Protocol>
  </NetworkRuleAttributes>
  <RequestId>F9F2F77D-307C-4F15-8D02-AB5957EEBF97</RequestId>
</DescribeNetworkRuleAttributesResponse>
```

#### JSON format

```
{
  "NetworkRuleAttributes": [
    {
```



```
"InstanceId": "ddoscoo-cn-mp91j1ao****",
"Config": {
  "NodataConn": "off",
  "Cc": {
    "Sblack": []
  },
  "PersistenceTimeout": 0,
  "PayloadLen": {
    "Min": 0,
    "Max": 6000
  },
  "Sla": {
    "Cps": 100000,
    "CpsEnable": 1,
    "MaxconnEnable": 0,
    "Maxconn": 100000
  },
  "Slimit": {
    "CpsMode": 1,
    "Pps": 0,
    "Bps": 0,
    "Cps": 0,
    "CpsEnable": 0,
    "MaxconnEnable": 0,
    "Maxconn": 0
  },
  "Synproxy": "on"
},
"FrontendPort": 8080,
"Protocol": "tcp"
},
"RequestId": "F9F2F77D-307C-4F15-8D02-AB5957EEBF97"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.12.4 ModifyNetworkRuleAttribute


Modifies the session persistence settings of a port forwarding rule.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyNetworkRuleAttribute	The operation that you want to perform. Set the value to <b>ModifyNetworkRuleAttribute</b> .

Parameter	Type	Required	Example	Description
<b>Config</b>	String	Yes	{"PersistenceTimeout":900}	<p>The session persistence settings of the port forwarding rule. This parameter is a JSON string. The field in the value is described as follows:</p> <ul style="list-style-type: none"> <li>• <b>PersistenceTimeout:</b> The timeout period of session persistence. This field is required and must be of the INTEGER type. Valid values: <b>30</b> to <b>3600</b>. Unit: seconds. Default value: <b>0</b>, which indicates that session persistence is disabled.</li> </ul>
<b>ForwardProtocol</b>	String	Yes	tcp	<p>The forwarding protocol. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>tcp</b></li> <li>• <b>udp</b></li> </ul>
<b>FrontendPort</b>	Integer	Yes	8080	The forwarding port.
<b>InstanceId</b>	String	Yes	ddoscoo-cn-mp91j1ao****	<p>The ID of the instance.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou:</b> mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1:</b> outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyNetworkRuleAttribute
&Config={"PersistenceTimeout":900}
&ForwardProtocol=tcp
&FrontendPort=8080
&InstanceId=ddoscoo-cn-mp91j1ao****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<ModifyNetworkRuleAttributeResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyNetworkRuleAttributeResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.13 Custom scenario policy

### 12.13.1 DescribeSceneDefensePolicies

Queries details about a scenario-specific custom policy.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeSceneDefensePolicies	The operation that you want to perform. Set the value to <b>DescribeSceneDefensePolicies</b> .
<b>Template</b>	String	No	promotion	The template of the policy. Valid values: <ul style="list-style-type: none"> <li><b>promotion</b>: important activity</li> <li><b>bypass</b>: all traffic forwarded</li> </ul>
<b>Status</b>	String	No	1	The status of the policy. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: the Disabled state</li> <li><b>1</b>: the Pending Enabled state</li> <li><b>2</b>: the Running state</li> <li><b>3</b>: the Expired state</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

## Response parameters

Parameter	Type	Example	Description
Policies	Array		Details about the policy.
Done	Integer	1	<p>The execution status of the policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>1</b>: not executed or execution completed</li> <li><b>0</b>: being executed</li> <li><b>-1</b>: failed</li> </ul>
EndTime	Long	1586016000000	The end time of the policy. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Name	String	testpolicy	The name of the policy.
ObjectCount	Integer	1	The number of protected targets.
PolicyId	String	321a-fd31-df51-****	The ID of the policy.
RuntimePolicies	Array		The running rules of the policy.
NewValue	String	{"cc_rule_enable": false}	<p>The protection rule applied when the policy takes effect.</p> <p>The value is <b>{"cc_rule_enable": false}</b> when <b>PolicyType</b> is set to <b>1</b>. This indicates that the Frequency Control policy is disabled.</p> <p>The value is <b>{"ai_rule_enable": 0}</b> when <b>PolicyType</b> is set to <b>2</b>. This indicates that the Intelligent Protection policy is disabled.</p>

Parameter	Type	Example	Description
PolicyType	Integer	1	<p>The protection policy whose status is changed when the policy takes effect.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>1</b>: the Frequency Control policy</li> <li><b>2</b>: the Intelligent Protection policy</li> </ul>
Status	Integer	3	<p>The running status of the policy. Valid values:</p> <ul style="list-style-type: none"> <li><b>0</b>: The policy has not been issued or is restored.</li> <li><b>1</b>: The policy is pending.</li> <li><b>2</b>: The policy is being restored.</li> <li><b>3</b>: The policy takes effect.</li> <li><b>4</b>: The policy fails to take effect.</li> <li><b>5</b>: The policy fails to be restored.</li> <li><b>6</b>: The protection target specified in the policy does not exist, which may have been deleted.</li> </ul>
oldValue	String	<code>{"cc_rule_enable": true}</code>	<p>The protection rule applied before the policy takes effect.</p> <p>The value is <b><code>{"cc_rule_enable": true}</code></b> when <b>PolicyType</b> is set to <b>1</b>. This indicates that the Frequency Control policy is enabled.</p> <p>The value is <b><code>{"ai_rule_enable": 1}</code></b> when <b>PolicyType</b> is set to <b>2</b>. This indicates that the Intelligent Protection policy is enabled.</p>
StartTime	Long	1585670400000	<p>The start time of the policy. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p>

Parameter	Type	Example	Description
Status	Integer	1	The status of the policy. Valid values: <ul style="list-style-type: none"> <li><b>0</b>: the Disabled state</li> <li><b>1</b>: the Pending Enabled state</li> <li><b>2</b>: the Running state</li> <li><b>3</b>: the Expired state</li> </ul>
Template	String	promotion	The template of the policy. Valid values: <ul style="list-style-type: none"> <li><b>promotion</b>: important activity</li> <li><b>bypass</b>: all traffic forwarded</li> </ul>
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. Valid values: <ul style="list-style-type: none"> <li><b>true</b>: The request is successful.</li> <li><b>false</b>: The request failed.</li> </ul>

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSceneDefensePolicies
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeSceneDefensePoliciesResponse>
  <Policies>
    <PolicyId>321a-fd31-df51-****</PolicyId>
    <Name>testpolicy</Name>
    <Template>promotion</Template>
    <StartTime>1585670400000</StartTime>
    <EndTime>1586016000000</EndTime>
    <Status>1</Status>
    <ObjectCount>1</ObjectCount>
    <Done>1</Done>
    <RuntimePolicies>
      <Status>4</Status>
      <PolicyType>1</PolicyType>
      <NewValue>
        <cc_rule_enable>>false</cc_rule_enable>
      </NewValue>
```

```

        <oldValue>
            <cc_rule_enable>true</cc_rule_enable>
        </oldValue>
    </RuntimePolicies>
    <RuntimePolicies>
        <Status>3</Status>
        <PolicyType>2</PolicyType>
        <NewValue>
            <ai_rule_enable>0</ai_rule_enable>
        </NewValue>
        <oldValue>
            <ai_rule_enable>1</ai_rule_enable>
        </oldValue>
    </RuntimePolicies>
</Policies>
<Success>true</Success>
<RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
</DescribeSceneDefensePoliciesResponse>

```

#### JSON format

```

{
  "Policies": [
    {
      "PolicyId": "321a-fd31-df51-****",
      "Name": "testpolicy",
      "Template": "promotion",
      "StartTime": 1585670400000,
      "EndTime": 1586016000000,
      "Status": 1,
      "ObjectCount": 1,
      "Done": 1,
      "RuntimePolicies": [
        {
          "Status": 4,
          "PolicyType": 1,
          "NewValue": {
            "cc_rule_enable": false
          },
          "oldValue": {
            "cc_rule_enable": true
          }
        },
        {
          "Status": 3,
          "PolicyType": 2,
          "NewValue": {
            "ai_rule_enable": 0
          },
          "oldValue": {
            "ai_rule_enable": 1
          }
        }
      ]
    }
  ],
  "Success": true,
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D"
}

```



```
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.13.2 CreateSceneDefensePolicy

Creates a scenario-specific custom policy.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	CreateSceneDefensePolicy	The operation that you want to perform. Set the value to <b>CreateSceneDefensePolicy</b> .
<b>EndTime</b>	Long	Yes	1586016000000	The time when the policy expires . This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
<b>Name</b>	String	Yes	testpolicy	The name of the policy.
<b>StartTime</b>	Long	Yes	1585670400000	The time when the policy starts to take effect. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Required	Example	Description
<b>Template</b>	String	Yes	promotion	The template of the policy. Valid values: <ul style="list-style-type: none"><li>• <b>promotion</b>: important activity</li><li>• <b>bypass</b>: all traffic forwarded</li></ul>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. Valid values: <ul style="list-style-type: none"><li>• <b>true</b>: The request is successful.</li><li>• <b>false</b>: The request failed.</li></ul>

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=CreateSceneDefensePolicy
&EndTime=1586016000000
&Name=testpolicy
&StartTime=1585670400000
&Template=promotion
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<CreateSceneDefensePolicyResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</CreateSceneDefensePolicyResponse>
```

#### JSON format

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success": true
}
```

#### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.13.3 ModifySceneDefensePolicy


Modifies a scenario-specific custom policy.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

#### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifySceneDefensePolicy	The operation that you want to perform. Set the value to <b>ModifySceneDefensePolicy</b> .
<b>EndTime</b>	Long	Yes	1586016000000	The time when the policy expires. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
<b>Name</b>	String	Yes	testpolicy	The name of the policy.

Parameter	Type	Required	Example	Description
<b>PolicyId</b>	String	Yes	321a-fd31-df51_****	<p>The ID of the policy that you want to modify.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeSceneDefensePolicies</a> operation to query the IDs of all policies.         </div>
<b>StartTime</b>	Long	Yes	1585670400000	The time when the policy starts to take effect. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
<b>Template</b>	String	Yes	promotion	<p>The template of the policy. Valid values:</p> <ul style="list-style-type: none"> <li><b>promotion</b>: important activity</li> <li><b>bypass</b>: all traffic forwarded</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	The ID of the request.

Parameter	Type	Example	Description
Success	Boolean	True	Indicates whether the request is successful. Valid values: <ul style="list-style-type: none"><li><b>true</b>: The request is successful.</li><li><b>false</b>: The request failed.</li></ul>

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=ModifySceneDefensePolicy
&EndTime=1586016000000
&Name=testpolicy
&PolicyId=321a-fd31-df51-****
&StartTime=1585670400000
&Template=promotion
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<ModifySceneDefensePolicyResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</ModifySceneDefensePolicyResponse>
```

#### JSON format

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success": true
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.13.4 DeleteSceneDefensePolicy

Deletes a scenario-specific custom policy.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteSceneDefensePolicy	The operation that you want to perform. Set the value to <b>DeleteSceneDefensePolicy</b> .
<b>PolicyId</b>	String	Yes	321a-fd31-df51-****	The ID of the policy that you want to delete.  <div>  <b>Note:</b>            You can call the <a href="#">DescribeSceneDefensePolicies</a> operation query the IDs of all policies.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. Valid values: <ul style="list-style-type: none"> <li><b>true</b>: The request is successful.</li> <li><b>false</b>: The request failed.</li> </ul>

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DeleteSceneDefensePolicy
&PolicyId=321a-fd31-df51-****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DeleteSceneDefensePolicyResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</DeleteSceneDefensePolicyResponse>
```

#### JSON format

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success": true
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.13.5 DescribeSceneDefenseObjects


Queries the protection target of a scenario-specific custom policy.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeSceneDefenseObjects	The operation that you want to perform. Set the value to <b>DescribeSceneDefenseObjects</b> .

Parameter	Type	Required	Example	Description
<b>PolicyId</b>	String	Yes	321a-fd31-df51-****	<p>The ID of the policy that you want to query.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeSceneDefensePolicies</a> operation to query the IDs of all policies.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou:</b> mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1:</b> outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

### Response parameters

Parameter	Type	Example	Description
Objects	Array		Details about the protection target.
Domain	String	www.aliyun.com	The domain name.
PolicyId	String	321a-fd31-df51-****	The ID of the policy.
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	The ID of the request.



Parameter	Type	Example	Description
Success	Boolean	true	Indicates whether the request is successful. Valid values: <ul style="list-style-type: none"><li><b>true</b>: The request is successful.</li><li><b>false</b>: The request failed.</li></ul>

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeSceneDefenseObjects
&PolicyId=321a-fd31-df51-****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeSceneDefenseObjectsResponse>
  <Objects>
    <PolicyId>321a-fd31-df51-****</PolicyId>
    <Domain>www.aliyun.com</Domain>
  </Objects>
  <Success>true</Success>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
</DescribeSceneDefenseObjectsResponse>
```

#### JSON format

```
{
  "Objects": [
    {
      "PolicyId": "321a-fd31-df51-****",
      "Domain": "www.aliyun.com"
    }
  ],
  "Success": true,
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.13.6 AttachSceneDefenseObject

Attaches a protection target to a scenario-specific custom policy.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	AttachSceneDefenseObject	The operation that you want to perform. Set the value to <b>AttachSceneDefenseObject</b> .
<b>Objects</b>	String	Yes	www.aliyun.com	The protection target that you want to attach to a policy. Separate multiple protection targets with commas (,).
<b>ObjectType</b>	String	Yes	Domain	The type of the protection target. Set the value to <b>Domain</b> , which indicates a domain name.
<b>PolicyId</b>	String	Yes	321a-fd31-df51_****	The ID of the policy. <div> <b>Note:</b> You can call the <a href="#">DescribeSceneDefensePolicies</a> operation query the IDs of all policies.</div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. Valid values: <ul style="list-style-type: none"><li>• <b>true</b>: The request is successful.</li><li>• <b>false</b>: The request failed.</li></ul>

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=AttachSceneDefenseObject
&Objects=www.aliyun.com
&ObjectType=Domain
&PolicyId=321a-fd31-df51-****
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<AttachSceneDefenseObjectResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</AttachSceneDefenseObjectResponse>
```

##### JSON format

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
```

```
"Success":true
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.13.7 DetachSceneDefenseObject

Deletes the protection target of a scenario-specific custom policy.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DetachSceneDefenseObject	The operation that you want to perform. Set the value to <b>DetachSceneDefenseObject</b> .
<b>Objects</b>	String	Yes	www.aliyun.com	The protection target that you want to delete from a policy. Separate multiple protection targets with commas (,).
<b>PolicyId</b>	String	Yes	321a-fd31-df51_****	The ID of the policy. <div> <b>Note:</b> You can call the <a href="#">DescribeSceneDefensePolicies</a> operation to query the IDs of all policies.</div>
<b>ObjectType</b>	String	No	Domain	The type of the protection target. Set the value to <b>Domain</b> , which indicates a domain name.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. Value <ul style="list-style-type: none"><li>• <b>true</b>: The request is successful.</li><li>• <b>false</b>: The request failed.</li></ul>

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DetachSceneDefenseObject
&Objects=www.aliyun.com
&PolicyId=321a-fd31-df51-****
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<DetachSceneDefenseObjectResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</DetachSceneDefenseObjectResponse>
```

##### JSON format

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success": true
}
```

```
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.13.8 EnableSceneDefensePolicy

Enables a scenario-specific custom policy.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	EnableSceneDefensePolicy	The operation that you want to perform. Set the value to <b>EnableSceneDefensePolicy</b> .
<b>PolicyId</b>	String	Yes	321a-fd31-df51_****	The ID of the policy that you want to enable.   <b>Note:</b> You can call the <a href="#">DescribeSceneDefensePolicies</a> operation query the IDs of all policies.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. Valid values: <ul style="list-style-type: none"><li><b>true</b>: The request is successful.</li><li><b>false</b>: The request failed.</li></ul>

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=EnableSceneDefensePolicy
&PolicyId=321a-fd31-df51-****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<EnableSceneDefensePolicyResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</EnableSceneDefensePolicyResponse>
```

#### JSON format

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success": true
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.13.9 DisableSceneDefensePolicy

Disables a scenario-specific custom policy.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DisableSceneDefensePolicy	The operation that you want to perform. Set the value to <b>DisableSceneDefensePolicy</b> .
<b>PolicyId</b>	String	Yes	321a-fd31-df51-****	The ID of the policy that you want to disable.  <div>  <b>Note:</b>            You can call the <a href="#">DescribeSceneDefensePolicies</a> operation to query the IDs of all policies.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	F65DF043-E0EB-4796-9467-23DDCDF92C1D	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. Valid values: <ul style="list-style-type: none"> <li><b>true</b>: The request is successful.</li> <li><b>false</b>: The request failed.</li> </ul>



## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DisableSceneDefensePolicy
&PolicyId=321a-fd31-df51-****
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DisableSceneDefensePolicyResponse>
  <RequestId>F65DF043-E0EB-4796-9467-23DDCDF92C1D</RequestId>
  <Success>true</Success>
</DisableSceneDefensePolicyResponse>
```

#### JSON format

```
{
  "RequestId": "F65DF043-E0EB-4796-9467-23DDCDF92C1D",
  "Success": true
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.14 Static page caching

### 12.14.1 ModifyWebCacheSwitch


Enables or disables the Static Page Caching policy for a website.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

#### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebCacheSwitch	The operation that you want to perform. Set the value to <b>ModifyWebCacheSwitch</b> .

Parameter	Type	Required	Example	Description
<b>Domain</b>	String	Yes	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name, and the domain name must be associated with an instance that uses the enhanced function plan. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>Enable</b>	Integer	Yes	1	<p>The status of the Static Page Caching policy. Valid values:</p> <ul style="list-style-type: none"> <li><b>1</b>: enables the policy.</li> <li><b>0</b>: disables the policy.</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupID</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebCacheSwitch
&Domain=www.aliyun.com
&Enable=1
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<ModifyWebCacheSwitchResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyWebCacheSwitchResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.14.2 ModifyWebCacheMode

Modifies the cache mode settings of the Static Page Caching policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebCacheMode	The operation that you want to perform. Set the value to <b>ModifyWebCacheMode</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name, and the domain name must be associated with an instance that uses the enhanced function plan. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>Mode</b>	String	Yes	standard	The cache mode of the Static Page Caching policy. Valid values :  <ul style="list-style-type: none"> <li>• <b>standard</b>: the Standard mode</li> <li>• <b>aggressive</b>: the Enhanced mode</li> <li>• <b>bypass</b>: the No Cache mode</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values:  <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=ModifyWebCacheMode
&Domain=www.aliyun.com
&Mode=standard
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ModifyWebCacheModeResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyWebCacheModeResponse>
```

##### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.14.3 ModifyWebCacheCustomRule

Modifies the custom rule of the Static Page Caching policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyWebCacheCustomRule	The operation that you want to perform. Set the value to <b>ModifyWebCacheCustomRule</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website. <div> <b>Note:</b> A forwarding rule must be configured for the domain name, and the domain name must be associated with an instance that uses the enhanced function plan. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.</div>

Parameter	Type	Required	Example	Description
<b>Rules</b>	String	Yes	<pre>[{"Name": "test","Uri": "/a","Mode": "standard","CacheTtl": 3600}]</pre>	<p>Details about the custom rule. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>: the name of the rule. This field is required and must be of the STRING type.</li> <li>• <b>Uri</b>: the path to the cached page. This field is required and must be of the STRING type.</li> <li>• <b>Mode</b>: the cache mode. This field is required and must be of the STRING type. Valid values: <ul style="list-style-type: none"> <li>- <b>standard</b>: the Standard mode</li> <li>- <b>aggressive</b>: the Enhanced mode</li> <li>- <b>bypass</b>: the No Cache mode</li> </ul> </li> <li>• <b>CacheTtl</b>: the expiration time of the page cache. This field is required and must be of the INTEGER type. Unit: seconds.</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=ModifyWebCacheCustomRule
&Domain=www.aliyun.com
&Rules=[{"Name": "test", "Uri": "/a", "Mode": "standard", "CacheTtl": 3600}]
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<ModifyWebCacheCustomRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</ModifyWebCacheCustomRuleResponse>
```

##### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).




## 12.14.4 DeleteWebCacheCustomRule

Deletes custom rules of the Static Page Caching policy for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteWebCacheCustomRule	The operation that you want to perform. Set the value to <b>DeleteWebCacheCustomRule</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.   <b>Note:</b> A forwarding rule must be configured for the domain name, and the domain name must be associated with an instance that uses the enhanced function plan. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RuleNames.N</b>	RepeatList	Yes	test	The name of rule N.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DeleteWebCacheCustomRule
&Domain=www.aliyun.com
&RuleNames.1=test
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<DeleteWebCacheCustomRuleResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteWebCacheCustomRuleResponse>
```

##### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.14.5 DescribeWebCacheConfigs

Queries the Static Page Caching configurations of websites.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebCacheConfigs	The operation that you want to perform. Set the value to <b>DescribeWebCacheConfigs</b> .
<b>Domains.N</b>	RepeatList	Yes	www.aliyun.com	The domain name of website N.   <b>Note:</b> A forwarding rule must be configured for the domain name, and the domain name must be associated with an instance that uses the enhanced function plan. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
DomainCacheConfigs	Array		The configuration of the Static Page Caching policy.
CustomRules	Array		Details about the custom static page caching rule.
CacheTtl	Long	86400	The expiration time of the page cache . Unit: seconds.
Mode	String	standard	The cache mode of the rule. Valid values: <ul style="list-style-type: none"> <li><b>standard</b>: the Standard mode</li> <li><b>aggressive</b>: the Enhanced mode</li> <li><b>bypass</b>: the No Cache mode</li> </ul>
Name	String	c1	The name of the rule.
Uri	String	/blog/	The path to the cached page.
Domain	String	www.aliyun.com	The domain name of the website.
Enable	Integer	1	The status of the Static Page Caching policy. Valid values: <ul style="list-style-type: none"> <li><b>1</b>: The policy is enabled.</li> <li><b>0</b>: The policy is disabled.</li> </ul>

Parameter	Type	Example	Description
Mode	String	bypass	The cache mode of the Static Page Caching policy. Valid values: <ul style="list-style-type: none"> <li><b>standard</b>: the Standard mode</li> <li><b>Aggressive</b>: the Enhanced mode</li> <li><b>bypass</b>: the No Cache mode</li> </ul>
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeWebCacheConfigs
&Domains.1=www.aliyun.com
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeWebCacheConfigsResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <DomainCacheConfigs>
    <Domain>www.aliyun.com</Domain>
    <Enable>1</Enable>
    <Mode>bypass</Mode>
    <CustomRules>
      <Name>c1</Name>
      <Uri>/blog/</Uri>
      <Mode>standard</Mode>
      <CacheTtl>86400</CacheTtl>
    </CustomRules>
  </DomainCacheConfigs>
</DescribeWebCacheConfigsResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "DomainCacheConfigs": [
    {
      "Domain": "www.aliyun.com",
      "Enable": 1,
      "Mode": "bypass",
      "CustomRules": [
        {
          "Name": "c1",
          "Uri": "/blog/",
          "Mode": "standard",
          "CacheTtl": 86400
        }
      ]
    }
  ]
}
```

```
}  
  }  
    ]  
  }  
    ]  
  }  
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

# 12.15 Investigation


## 12.15.1 DescribeDDoSEvents


Queries attack events launched against one or more Anti-DDoS Pro or Anti-DDoS Premium instances.


### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDDoSEvents	The operation that you want to perform. Set the value to <b>DescribeDdosEvents</b> .
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N. <div> <b>Note:</b> You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.</div>
<b>PageNumber</b>	Integer	Yes	1	The number of the page to return. Pages start from page <b>1</b> .
<b>PageSize</b>	Integer	Yes	10	The number of entries to return on each page.


Parameter	Type	Required	Example	Description
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

Parameter	Type	Required	Example	Description
<b>EndTime</b>	Long	No	1583683200	<p>The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>

### Response parameters

Parameter	Type	Example	Description
DDoSEvents	Array		The DDoS attack events.
Bps	Long	0	The bandwidth of attack traffic. Unit: bit/s.
EndTime	Long	1583933330	The time when the attack stopped . This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
EventType	String	blackhole	<p>The type of the attack event. Valid values:</p> <ul style="list-style-type: none"> <li><b>defense</b>: Mitigation</li> <li><b>blackhole</b>: Blackhole</li> </ul>
Ip	String	203.***.***.132	The source IP addresses of the attack event.
Port	String	80	The attacked port.



Parameter	Type	Example	Description
Pps	Long	0	The packet forwarding rate of attack traffic. Unit: packets per second.
Region	String	cn	<p>The region from which the attack was launched. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn</b>: mainland China</li> <li><b>alb-ap-northeast-1-gf-x</b>: Japan</li> <li><b>alb-ap-southeast-gf-x</b>: Singapore</li> <li><b>alb-cn-hongkong-gf-x</b>: Hong Kong (China)</li> <li><b>alb-eu-central-1-gf-x</b>: Germany</li> <li><b>alb-us-west-1-gf-x</b>: Western United States</li> </ul> <div>  <b>Note:</b>            The values except <b>cn</b> are only returned when <b>RegionId</b> is <b>ap-southeast-1</b>.         </div>
StartTime	Long	1583933277	The time when the attack event started. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
RequestId	String	0CA72AF5-1795-4350-8C77-50A448A2F334	The ID of the request.
Total	Long	1	The total number of returned attack events.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDDoSEvents
&InstanceId=ddoscoo-cn-mp91j1ao****
&PageNumber=1
&PageSize=10
```

```
&StartTime=1582992000
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeDDoSEventsResponse>
  <RequestId>OCA72AF5-1795-4350-8C77-50A448A2F334</RequestId>
  <Total>1</Total>
  <DDoSEvents>
    <Pps>0</Pps>
    <Bps>0</Bps>
    <EndTime>1583933330</EndTime>
    <EventType>blackhole</EventType>
    <Ip>203. ***. ***.132</Ip>
    <Port></Port>
    <StartTime>1583933277</StartTime>
  </DDoSEvents>
</DescribeDDoSEventsResponse>
```

JSON format

```
{
  "RequestId": "OCA72AF5-1795-4350-8C77-50A448A2F334",
  "Total": 1,
  "DDoSEvents": [
    {
      "Pps": 0,
      "Bps": 0,
      "EndTime": 1583933330,
      "EventType": "blackhole",
      "Ip": "203. ***. ***.132",
      "Port": "",
      "StartTime": 1583933277
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).



## 12.15.2 DescribePortFlowList


Queries the traffic data of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.


## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribePortFlowList	The operation that you want to perform. Set the value to <b>DescribePortFlowList</b> .
<b>EndTime</b>	Long	Yes	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N.   <b>Note:</b> You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.
<b>Interval</b>	Integer	Yes	1000	The intervals for returning traffic data. Unit: seconds.

Parameter	Type	Required	Example	Description
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	null	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

### Response parameters

Parameter	Type	Example	Description
PortFlowList	Array		The traffic data.

Parameter	Type	Example	Description
AttackBps	Long	0	The bandwidth of attack traffic. Unit: bit/s.
AttackPps	Long	0	The packet forwarding rate of attack traffic. Unit: packets per second.
InBps	Long	2176000	The inbound bandwidth. Unit: bit/s.
InPps	Long	2934	The packet forwarding rate of inbound traffic. Unit: packets per second.
Index	Long	0	The index number of the returned data.
OutBps	Long	4389	The outbound bandwidth. Unit: bit/s.
OutPps	Long	5	The packet forwarding rate of outbound traffic. Unit: packets per second.
Region	String	cn	<p>The region from which the traffic is from. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn</b>: mainland China</li> <li><b>alb-ap-northeast-1-gf-x</b>: Japan</li> <li><b>alb-ap-southeast-gf-x</b>: Singapore</li> <li><b>alb-cn-hongkong-gf-x</b>: Hong Kong (China)</li> <li><b>alb-eu-central-1-gf-x</b>: Germany</li> <li><b>alb-us-west-1-gf-x</b>: Western United States</li> </ul> <div>  <b>Note:</b>            The values except <b>cn</b> are only returned when <b>RegionId</b> is <b>ap-southeast-1</b>.         </div>

Parameter	Type	Example	Description
Time	Long	1582992000	The time when the data was recorded . This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
RequestId	String	FFC77501-BDF8-4BC8-9BF5-B295FBC3189B	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribePortFlowList
&EndTime=1583683200
&InstanceId=ddoscoo-cn-mp91j1ao****
&Interval=1000
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribePortFlowListResponse>
  <RequestId>FFC77501-BDF8-4BC8-9BF5-B295FBC3189B</RequestId>
  <PortFlowList>
    <OutPps>5</OutPps>
    <OutBps>4389</OutBps>
    <InBps>2176000</InBps>
    <InPps>2934</InPps>
    <Region>cn</Region>
    <Index>0</Index>
    <AttackBps>0</AttackBps>
    <AttackPps>0</AttackPps>
    <Time>1582992000</Time>
  </PortFlowList>
  <PortFlowList>
    <OutPps>5</OutPps>
    <OutBps>4155</OutBps>
    <InBps>4648000</InBps>
    <InPps>6268</InPps>
    <Region>cn</Region>
    <Index>1</Index>
    <AttackBps>0</AttackBps>
    <AttackPps>0</AttackPps>
    <Time>1582993000</Time>
  </PortFlowList>
```

```
</DescribePortFlowListResponse>
```

JSON format

```
{
  "RequestId": "FFC77501-BDF8-4BC8-9BF5-B295FBC3189B",
  "PortFlowList": [
    {
      "OutPps": 5,
      "OutBps": 4389,
      "InBps": 2176000,
      "InPps": 2934,
      "Region": "cn",
      "Index": 0,
      "AttackBps": 0,
      "AttackPps": 0,
      "Time": 1582992000
    },
    {
      "OutPps": 5,
      "OutBps": 4155,
      "InBps": 4648000,
      "InPps": 6268,
      "Region": "cn",
      "Index": 1,
      "AttackBps": 0,
      "AttackPps": 0,
      "Time": 1582993000
    }
  ]
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.15.3 DescribePortConnsList




Queries the connections established over the port of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribePortConnsList	The operation that you want to perform. Set the value to <b>DescribePortConnsList</b> .

Parameter	Type	Required	Example	Description
<b>EndTime</b>	Long	Yes	1583683200	<p>The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	<p>The ID of instance N.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>
<b>Interval</b>	Integer	Yes	1000	<p>The intervals for returning statistics. Unit: seconds.</p>
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>



Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>Port</b>	String	No	null	The port number that you want to query. If you do not specify this parameter, all ports are queried.

### Response parameters

Parameter	Type	Example	Description
ConnsList	Array		Details about the connections established over the port.
ActConns	Long	2	The number of active connections.
Conns	Long	20	The number of concurrent connections.
Cps	Long	0	The number of new connections.
InActConns	Long	4	The number of inactive connections.

Parameter	Type	Example	Description
Index	Long	0	The index number of the returned data.
Time	Long	1582992000	The time when the statistic was recorded. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
RequestId	String	7 E6BF16 F-27A9-49BC-AD18-F79B409DE753	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribePortConnsList
&EndTime=1583683200
&InstanceIds.1=ddoscoo-cn-mp91j1ao****
&Interval=1000
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribePortConnsListResponse>
  <ConnsList>
    <Conns>20</Conns>
    <Cps>0</Cps>
    <Index>0</Index>
    <ActConns>2</ActConns>
    <InActConns>4</InActConns>
    <Time>1582992000</Time>
  </ConnsList>
  <ConnsList>
    <Conns>24</Conns>
    <Cps>0</Cps>
    <Index>1</Index>
    <ActConns>2</ActConns>
    <InActConns>5</InActConns>
    <Time>1582993000</Time>
  </ConnsList>
  <RequestId>7E6BF16F-27A9-49BC-AD18-F79B409DE753</RequestId>
```

```
</DescribePortConnsListResponse>
```

JSON format

```
{
  "ConnsList": [
    {
      "Conns": 20,
      "Cps": 0,
      "Index": 0,
      "ActConns": 2,
      "InActConns": 4,
      "Time": 1582992000
    },
    {
      "Conns": 24,
      "Cps": 0,
      "Index": 1,
      "ActConns": 2,
      "InActConns": 5,
      "Time": 1582993000
    }
  ],
  "RequestId": "7E6BF16F-27A9-49BC-AD18-F79B409DE753"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.15.4 DescribePortConnsCount




Queries the statistics on the connections established over the ports of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribePortConnsCount	The operation that you want to perform. Set the value to <b>DescribePortConnsCount</b> .

Parameter	Type	Required	Example	Description
<b>EndTime</b>	Long	Yes	1583683200	<p>The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	<p>The ID of instance N.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>Port</b>	String	No	80	The number of port that you want to query. If you do not specify this parameter, all ports are queried.

### Response parameters

Parameter	Type	Example	Description
ActConns	Long	159	The number of active connections.
Conns	Long	46340	The number of concurrent connections.
Cps	Long	0	The number of new connections.
InActConns	Long	121	The number of inactive connections.

Parameter	Type	Example	Description
RequestId	String	48859E14-A9FB-4100-99FF-AAB75CA46776	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribePortConnsCount
&EndTime=1583683200
&InstanceId=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribePortConnsCountResponse>
  <Conns>46340</Conns>
  <RequestId>48859E14-A9FB-4100-99FF-AAB75CA46776</RequestId>
  <Cps>0</Cps>
  <ActConns>159</ActConns>
  <InActConns>121</InActConns>
</DescribePortConnsCountResponse>
```

#### JSON format

```
{
  "Conns": 46340,
  "RequestId": "48859E14-A9FB-4100-99FF-AAB75CA46776",
  "Cps": 0,
  "ActConns": 159,
  "InActConns": 121
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).




## 12.15.5 DescribePortMaxConns

Queries the maximum number of connections that can be established over the ports of one or more Anti-DDoS Pro or Anti-DDoS Premium instances.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribePortMaxConns	The operation that you want to perform. Set the value to <b>DescribePortMaxConns</b> .
<b>EndTime</b>	Long	Yes	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N.   <b>Note:</b> You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.
<b>StartTime</b>	Long	Yes	1582992000	The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
PortMaxConns	Array		Details about the maximum number of connections that are established over a port of the instance.
Cps	Long	100	The maximum number of connections per second (CPS).
Ip	String	203.***.***.117	The IP address of the instance.
Port	String	80	The port of the instance.
RequestId	String	08F79110-2AF5-4FA7-998E-7C5E75EACF9C	The ID of the request.



## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribePortMaxConns
&EndTime=1583683200
&InstanceId= ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribePortMaxConnsResponse>
  <PortMaxConns>
    <Port>80</Port>
    <Ip>203. ***. ***.117</Ip>
    <Cps>0</Cps>
  </PortMaxConns>
  <PortMaxConns>
    <Port>443</Port>
    <Ip>203. ***. ***.117</Ip>
    <Cps>0</Cps>
  </PortMaxConns>
  <RequestId>08F79110-2AF5-4FA7-998E-7C5E75EACF9C</RequestId>
</DescribePortMaxConnsResponse>
```

#### JSON format

```
{
  "PortMaxConns": [
    {
      "Port": "80",
      "Ip": "203. ***. ***.117",
      "Cps": 0
    },
    {
      "Port": "443",
      "Ip": "203. ***. ***.117",
      "Cps": 0
    }
  ],
  "RequestId": "08F79110-2AF5-4FA7-998E-7C5E75EACF9C"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).



## 12.15.6 DescribePortAttackMaxFlow


Queries the peak attack traffic bandwidth and peak attack traffic packet rates of one or more Anti-DDoS Pro or Anti-DDoS Premium instances within a specific period of time.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribePortAttackMaxFlow	The operation that you want to perform. Set the value to <b>DescribePortAttackMaxFlow</b> .
<b>EndTime</b>	Long	Yes	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N.   <b>Note:</b> You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.

Parameter	Type	Required	Example	Description
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

### Response parameters

Parameter	Type	Example	Description
Bps	Long	149559	<p>The peak attack traffic bandwidth. Unit: bit/s.</p>

Parameter	Type	Example	Description
Pps	Long	23	The peak attack traffic packet rate. Unit: packets per second.
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribePortAttackMaxFlow
&EndTime=1583683200
&InstanceId=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribePortAttackMaxFlowResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Bps>149559</Bps>
  <Pps>23</Pps>
</DescribePortAttackMaxFlowResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "Bps": 149559,
  "Pps": 23
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).




## 12.15.7 DescribePortViewSourceCountries

Queries the regions outside China from which requests are sent to one or more Anti-DDoS Pro or Anti-DDoS Premium instances within a specific period of time.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribePortViewSourceCountries	The operation that you want to perform. Set the value to <b>DescribePortViewSourceCountries</b> .
<b>EndTime</b>	Long	Yes	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N.   <b>Note:</b> You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.
<b>StartTime</b>	Long	Yes	1582992000	The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.
SourceCountries	Array		The regions outside China from which requests are sent.
Count	Long	3390671	The number of requests.
CountryId	String	cn	The country ID. For more information about codes of regions outside China, see the Codes of regions outside China table in this topic.

### Codes of regions outside China

Code	Region	Abbreviation
1	China	CN
2	Australia	AU
3	Japan	JP
4	Thailand	TH
5	India	IN
7	United States	US
8	Germany	DE
9	Netherlands	NL
10	Malaysia	MY
11	Angola	AO
12	South Korea	KR
13	Singapore	SG
14	Kampuchea	KH
16	Philippines	PH
17	Vietnam	VN
18	France	FR
19	Poland	PL
20	Spain	ES
21	Russia	RU
22	Switzerland	CH

Code	Region	Abbreviation
23	United Kingdom	GB
24	Italy	IT
25	Czech Republic	CZ
26	Ireland	IE
27	Denmark	DK
28	Portugal	PT
29	Sweden	SE
30	Ghana	GH
31	Turkey	TR
32	Cameroon	CM
33	South Africa	ZA
34	Finland	FI
35	Hungary	HU
36	United Arab Emirates	AE
37	Greece	GR
38	Brazil	BR
39	Austria	AT
40	Jordan	JO
41	Belgium	BE
42	Romania	RO



Code	Region	Abbreviation
43	Luxembourg	LU
44	Argentina	AR
45	Uganda	UG
46	Armenia	AM
47	Tanzania	TZ
48	Burundi	BI
49	Uruguay	UY
50	Bulgaria	BG
51	Ukraine	UA
52	Israel	IL
53	Qatar	QA
54	Iraq	IQ
55	Lithuania	LT
56	Moldova	MD
57	Uzbekistan	UZ
58	Slovakia	SK
59	Kazakhstan	KZ
60	Croatia	HR
61	Georgia	GE
62	Estonia	EE

Code	Region	Abbreviation
63	Gibraltar	GI
64	Latvia	LV
65	Norway	NO
66	Palestine	PS
67	Cyprus	CY
68	Saudi Arabia	SA
69	Iran	IR
70	Canada	CA
71	American Samoa	AS
72	Syria	SY
73	Kuwait	KW
74	Bahrain	BH
75	Lebanon	LB
76	Oman	OM
77	Azerbaijan	AZ
78	Zambia	ZM
79	Zimbabwe	ZW
80	Democratic Republic of the Congo	CD
81	Serbia	RS

Code	Region	Abbreviation
82	Iceland	IS
83	Slovenia	SI
84	Macedonia	MK
85	Liechtenstein	LI
86	Jersey	JE
87	Bosnia and Herzegovina	BA
88	Chile	CL
89	Peru	PE
90	Kyrgyzstan	KG
91	Reunion	RE
92	Tajikistan	TJ
93	Isle of Man	IM
94	Guernsey	GG
95	Malta	MT
96	Libya	LY
97	Yemen	YE
98	Belarus	BY
99	Mayotte	YT
100	Guadeloupe	GP
101	Saint Martin	MF

Code	Region	Abbreviation
102	Martinique	MQ
103	Guyana	GY
104	Kosovo	XK
105	Indonesia	ID
106	Northern Mariana Islands	MP
107	Dominican Republic	DO
108	Mexico	MX
109	Guam	GU
110	Nigeria	NG
111	Venezuela	VE
112	Puerto Rico	PR
113	Mongolia	MN
114	New Zealand	NZ
115	Bangladesh	BD
116	Pakistan	PK
117	Papua New Guinea	PG
118	Trinidad and Tobago	TT
119	Lesotho	LS
120	Colombia	CO
121	Costa Rica	CR

Code	Region	Abbreviation
123	Ecuador	EC
124	Sri Lanka	LK
125	Egypt	EG
126	British Virgin Islands	VG
127	Jamaica	JM
128	Saint Lucia	LC
129	Cayman Islands	KY
130	Grenada	GD
131	Curacao	CW
132	Panama	PA
133	Barbados	BB
134	The Bahamas	BS
135	Nepal	NP
136	Tokelau	TK
137	Maldives	MV
138	Afghanistan	AF
139	New Caledonia	NC
140	Fiji	FJ
141	Wallis and Futuna Islands	WF
142	Albania	AL

Code	Region	Abbreviation
143	San Marino	SM
144	Montenegro	ME
145	East Timor	TL
146	Monaco	MC
147	Guinea	GN
148	Myanmar	MM
149	Greenland	GL
150	Bermuda	BM
151	Saint Vincent and the Grenadines	VC
152	United States Virgin Islands	VI
153	Suriname	SR
154	Saint Barthelamy	BL
155	Haiti	HT
156	Antigua and Barbuda	AG
157	Liberia	LR
158	Kenya	KE
159	Botswana	BW
160	Mozambique	MZ
161	Senegal	SN

Code	Region	Abbreviation
162	Madagascar	MG
163	Namibia	NA
164	Côte d'Ivoire	CI
165	Sudan	SD
166	Malawi	MW
167	Gabon	GA
168	Mali	ML
169	Benin	BJ
170	Chad	TD
171	Cabo Verde	CV
172	Rwanda	RW
173	Republic of the Congo	CG
174	The Gambia	GM
175	Mauritius	MU
176	Algeria	DZ
177	Eswatini	SZ
178	Burkina Faso	BF
179	Sierra Leone	SL
180	Somalia	SO
181	Niger	NE

Code	Region	Abbreviation
182	Central African Republic	CF
183	Togo	TG
184	South Sudan	SS
185	Equatorial Guinea	GQ
186	Seychelles	SC
187	Djibouti	DJ
188	Morocco	MA
189	Mauritania	MR
190	Comoros	KM
191	British Indian Ocean Territory	IO
192	Tunisia	TN
193	Laos	LA
194	Brunei	BN
195	Bhutan	BT
196	Nauru	NR
197	Vanuatu	VU
198	Federated States of Micronesia	FM
199	French Polynesia	PF
200	Tonga	TO



Code	Region	Abbreviation
201	Honduras	HN
202	Bolivia	BO
203	El Salvador	SV
204	Guatemala	GT
205	Nicaragua	NI
206	Belize	BZ
207	Paraguay	PY
208	French Guiana	GF
209	Andorra	AD
210	Faroe Islands	FO
211	Niue	NU
212	Kiribati	KI
213	Marshall Islands	MH
214	Palau	PW
215	Samoa	WS
216	Solomon Islands	SB
217	Tuvalu	TV
218	North Korea	KP
219	Vatican City	VA
220	Eritrea	ER

Code	Region	Abbreviation
221	Ethiopia	ET
222	Guinea-Bissau	GW
223	Sao Tome and Principe	ST
224	Turkmenistan	TM
225	Cuba	CU
226	Dominica	DM
227	Saint Kitts and Nevis	KN
228	Aruba	AW
229	Falkland Islands	FK
230	Turks and Caicos Islands	TC
231	Caribbean Netherlands	BQ
232	Sint Maarten	SX
233	Montserrat	MS
234	Anguilla	AI
235	Saint Pierre and Miquelon	PM
236	Åland Islands	AX
237	Norfolk Island	NF
238	Antarctica	AQ
239	Cook Islands	CK
240	Christmas Island	CX

Code	Region	Abbreviation
241	Other regions in Europe	EU

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceCountries
&EndTime=1583683200
&InstanceId=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribePortViewSourceCountriesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <SourceCountries>
    <Count>3390671</Count>
    <CountryId>cn</CountryId>
  </SourceCountries>
</DescribePortViewSourceCountriesResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "SourceCountries": [
    {
      "Count": 3390671,
      "CountryId": "cn"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).



## 12.15.8 DescribePortViewSourceIps


Queries the Internet service providers (ISPs) from which requests are sent to one or more Anti-DDoS Pro or Anti-DDoS Premium instances within a specific period of time.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribePortViewSourceIps	The operation that you want to perform. Set the value to <b>DescribePortViewSourceIps</b> .
<b>EndTime</b>	Long	Yes	1583683200	<p>The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC. If you do not specify this parameter, the current system time is used as the end time.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	<p>The ID of instance N.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.         </div>

Parameter	Type	Required	Example	Description
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

### Response parameters

Parameter	Type	Example	Description
Isps	Array		Detail about the ISP.

Parameter	Type	Example	Description
Count	Long	3390671	The total number of requests transmitted from the ISP.
Ispld	String	100017	The code of the ISP. For more information, see the ISP codes table.
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### ISP codes

Code	ISP
100017	China Telecom
100026	China Unicom
100025	China Mobile
100027	China Education and Research Network
100020	China Mobile Tietong
1000143	Dr.Peng Telecom & Media Group
100080	Beijing Gehua CATV Network
1000139	National Radio and Television Administration
100023	Oriental Cable Network
100063	Founder Broadband
1000337	China Internet Exchange
100021	21Vianet
1000333	Wasu Media Holding

Code	ISP
100093	Wangsu Science & Technology
1000401	Tencent
100099	Baidu
1000323	Alibaba Cloud
100098	Alibaba

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceIsp
&EndTime=1583683200
&InstanceId=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribePortViewSourceIspResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Isp>
    <Count>3390671</Count>
    <IspId>100017</IspId>
  </Isp>
</DescribePortViewSourceIspResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "Isp": [
    {
      "Count": 3390671,
      "IspId": "100017"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).



## 12.15.9 DescribePortViewSourceProvinces

Queries the regions inside China from which requests are sent to one or more Anti-DDoS Pro or Anti-DDoS Premium instances within a specific period of time.


### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribePortViewSourceProvinces	The operation that you want to perform. Set the value to <b>DescribePortViewSourceProvinces</b> .
<b>InstanceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of instance N.  <b>Note:</b> You can call the <a href="#">DescribeInstanceIds</a> operation to query the IDs of all instances.
<b>StartTime</b>	Long	Yes	1582992000	The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.  <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.



Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>
<b>EndTime</b>	Long	No	1583683200	<p>The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC. If you do not specify this parameter, the current system time is used as the end time.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>

**Response parameters**

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.
SourceProvinces	Array		Details about the region inside China from which the requests are sent.
Count	Long	3390671	The total number of requests that are sent from the region.
ProvinceId	String	440000	The code of the region inside China. For more information about codes of regions inside China, see the Codes of regions inside China table.

**Codes of regions inside China**

Code	Region
110000	Beijing
120000	Tianjin
130000	Hebei
140000	Shanxi
150000	Nei Mongol
210000	Liaoning
220000	Jilin
230000	Heilongjiang
310000	Shanghai
320000	Jiangsu

Code	Region
330000	Zhejiang
340000	Anhui
350000	Fujian
360000	Jiangxi
370000	Shandong
410000	Henan
420000	Hubei
430000	Hunan
440000	Guangdong
450000	Guangxi
460000	Hainan
500000	Chongqing
510000	Sichuan
520000	Guizhou
530000	Yunnan
540000	Xizang
610000	Shaanxi
620000	Gansu
630000	Qinghai
640000	Ningxia

Code	Region
650000	Xinjiang
810000	Hong Kong S.A.R
710000	Taiwan
820000	Macao S.A.R

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribePortViewSourceProvinces
&InstanceId=ddoscoo-cn-mp91j1ao****
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribePortViewSourceProvincesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <SourceProvinces>
    <Count>3390671</Count>
    <ProvinceId>440000</ProvinceId>
  </SourceProvinces>
</DescribePortViewSourceProvincesResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "SourceProvinces": [
    {
      "Count": 3390671,
      "ProvinceId": "440000"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.15.10 DescribeDomainAttackEvents



Queries attack events launched against a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainAttackEvents	The operation that you want to perform. Set the value to <b>DescribeDomainAttackEvents</b> .
<b>EndTime</b>	Long	Yes	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.
<b>PageNumber</b>	Integer	Yes	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .
<b>PageSize</b>	Integer	Yes	10	The number of entries to return on each page.

Parameter	Type	Required	Example	Description
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>
<b>Domain</b>	String	No	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>

## Response parameters

Parameter	Type	Example	Description
DomainAttackEvents	Array		Details about the DDoS attack event.
Domain	String	www.aliyun.com	The attacked domain name.
EndTime	Long	1560320160	The time when the DDoS attack stopped. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
MaxQps	Long	1000	The peak attack QPS.
StartTime	Long	1560312900	The time when the DDoS attack started. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.
TotalCount	Long	1	The total number of returned DDoS attack events.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainAttackEvents
&EndTime=1583683200
&PageNumber=1
&PageSize=10
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

### XML format

```
<DescribeDomainAttackEventsResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <TotalCount>1</TotalCount>
  <DomainAttackEvents>
    <Domain>www.aliyun.com</Domain>
    <MaxQps>1000</MaxQps>
    <StartTime>1560312900</StartTime>
    <EndTime>1560320160</EndTime>
  </DomainAttackEvents>
</DescribeDomainAttackEventsResponse>
```

### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "TotalCount": 1,
  "DomainAttackEvents": [{
    "Domain": "www.aliyun.com",
    "MaxQps": 1000,
    "StartTime": 1560312900,
    "EndTime": 1560320160
  }]
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.15.11 DescribeDomainQPSList

Queries the statistics on the queries per second (QPS) of a website.



### Debugging


OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainQPSList	The operation that you want to perform. Set the value to <b>DescribeDomainQPSList</b> .



Parameter	Type	Required	Example	Description
<b>EndTime</b>	Long	Yes	1583683200	<p>The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>Interval</b>	Long	Yes	1000	The intervals for returning statistics. Unit: seconds.
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>Domain</b>	String	No	www.aliyun.com	<p>The domain name of the website . If you do not specify this parameter, the statistics on the QPS of all domain names are queried.</p> <div>  <b>Note:</b>  A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names. </div>

### Response parameters

Parameter	Type	Example	Description
DomainQPSList	Array		The statistics on the QPS of the website.
AttackQps	Long	1	The attack QPS.
CacheHits	Long	0	The number of cache hits.
Index	Long	0	The index number of the returned data.
MaxAttackQps	Long	37	The peak attack QPS.

Parameter	Type	Example	Description
MaxNormalQps	Long	93	The peak of normal QPS.
MaxQps	Long	130	The peak of total QPS.
Time	Long	1582992000	The time when the statistic was recorded. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
TotalCount	Long	20008	The total number of queries.
TotalQps	Long	1	The total number of QPS.
RequestId	String	327F2ABB-104D-437A-AAB5-D633E29A8C51	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainQPSList
&Interval=1000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeDomainQPSListResponse>
  <DomainQPSList>
    <MaxAttackQps>37</MaxAttackQps>
    <TotalQps>1</TotalQps>
    <TotalCount>20008</TotalCount>
    <MaxQps>130</MaxQps>
    <MaxNormalQps>93</MaxNormalQps>
    <AttackQps>1</AttackQps>
    <Index>0</Index>
    <Time>1582992000</Time>
    <CacheHits>0</CacheHits>
  </DomainQPSList>
  <RequestId>327F2ABB-104D-437A-AAB5-D633E29A8C51</RequestId>
```

```
</DescribeDomainQPSListResponse>
```

JSON format

```
{
  "DomainQPSList": [
    {
      "MaxAttackQps": 37,
      "TotalQps": 1,
      "TotalCount": 20008,
      "MaxQps": 130,
      "MaxNormalQps": 93,
      "AttackQps": 1,
      "Index": 0,
      "Time": 1582992000,
      "CacheHits": 0
    }
  ],
  "RequestId": "327F2ABB-104D-437A-AAB5-D633E29A8C51"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.15.12 DescribeDomainStatusCodeList


Queries the statistics on different response status codes of a website.



### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainStatusCodeList	The operation that you want to perform. Set the value to <b>DescribeDomainStatusCodeList</b> .
<b>Interval</b>	Long	Yes	1000	The intervals for returning statistics. Unit: seconds.

Parameter	Type	Required	Example	Description
<b>QueryType</b>	String	Yes	gf	<p>The source of the statistics. Valid values:</p> <ul style="list-style-type: none"> <li><b>gf</b>: Anti-DDoS Pro or Anti-DDoS Premium</li> <li><b>upstream</b>: origin server</li> </ul>
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>ResourceGroupID</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>

Parameter	Type	Required	Example	Description
<b>EndTime</b>	Long	No	1583683200	<p>The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>Domain</b>	String	No	www.aliyun.com	<p>The domain name of the website . If you do not specify this parameter, the statistics on response status codes of all domain names are queried.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	3B63C0DD-8AC5-44B2-95D6-064CA9296B9C	The ID of the request.
StatusCode List	Array		The statistics on response status codes.
Index	Integer	0	The index number of the returned data.

Parameter	Type	Example	Description
Status200	Long	15520	The number of 200 response status codes.
Status2XX	Long	15520	The number of 2xx response status codes.
Status3XX	Long	0	The number of 3xx response status codes.
Status403	Long	0	The number of 403 response status codes.
Status404	Long	0	The number of 404 response status codes.
Status405	Long	0	The number of 405 response status codes.
Status4XX	Long	4486	The number of 4xx response status codes.
Status501	Long	0	The number of 501 response status codes.
Status502	Long	0	The number of 502 response status codes.
Status503	Long	0	The number of 503 response status codes.
Status504	Long	0	The number of 504 response status codes.
Status5XX	Long	0	The number of 5xx response status codes.

Parameter	Type	Example	Description
Time	Long	1582992000	The time when the statistic was recorded. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainStatusCodeList
&QueryType=gf
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeDomainStatusCodeListResponse>
  <RequestId>3B63C0DD-8AC5-44B2-95D6-064CA9296B9C</RequestId>
  <StatusCodeList>
    <Status501>0</Status501>
    <Status502>0</Status502>
    <Status403>0</Status403>
    <Index>0</Index>
    <Time>1582992000</Time>
    <Status503>0</Status503>
    <Status404>0</Status404>
    <Status504>0</Status504>
    <Status405>0</Status405>
    <Status2XX>15520</Status2XX>
    <Status200>15520</Status200>
    <Status3XX>0</Status3XX>
    <Status4XX>4486</Status4XX>
    <Status5XX>0</Status5XX>
  </StatusCodeList>
</DescribeDomainStatusCodeListResponse>
```

#### JSON format

```
{
  "RequestId": "3B63C0DD-8AC5-44B2-95D6-064CA9296B9C",
  "StatusCodeList": [
    {
      "Status501": 0,
      "Status502": 0,
      "Status403": 0,
      "Index": 0,
      "Time": 1582992000,
      "Status503": 0,
      "Status404": 0,
```



```
"Status504": 0,  
"Status405": 0,  
"Status2XX": 15520,  
"Status200": 15520,  
"Status3XX": 0,  
"Status4XX": 4486,  
"Status5XX": 0  
}  
]  
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.15.13 DescribeDomainOverview


Queries the attack overview of a website, such as the peak HTTP attack traffic and peak HTTPS attack traffic.


### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainOverview	The operation that you want to perform. Set the value to <b>DescribeDomainOverview</b> .
<b>StartTime</b>	Long	Yes	1582992000	The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>EndTime</b>	Long	No	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC. If you do not specify this parameter, the current system time is used as the end time. <div>  <b>Note:</b>  This UNIX timestamp must indicate a time that is accurate to the minute. </div>

Parameter	Type	Required	Example	Description
Domain	String	No	www.aliyun.com	The domain name of the website.   <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.

### Response parameters

Parameter	Type	Example	Description
MaxHttp	Long	1000	The peak HTTP attack traffic. Unit: queries per second.
MaxHttps	Long	1000	The peak HTTPS attack traffic. Unit: queries per second.
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDomainOverview
&StartTime=1582992000
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<DescribeDomainOverviewResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <MaxHttps>1000</MaxHttps>
  <MaxHttp>1000</MaxHttp>
</DescribeDomainOverviewResponse>
```

##### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "MaxHttps": 1000,
  "MaxHttp": 1000
}
```

```
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.15.14 DescribeDomainStatusCodeCount



Queries the statistics on different response status codes of a website within a specific period of time.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainStatusCodeCount	The operation that you want to perform. Set the value to <b>DescribeDomainStatusCodeCount</b> .
<b>EndTime</b>	Long	Yes	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.

Parameter	Type	Required	Example	Description
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>ResourceGroupID</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou:</b> mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1:</b> outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>Domain</b>	String	No	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>

**Response parameters**

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.
Status200	Long	951159	The number of 200 response status codes in a specific period of time.
Status2XX	Long	951472	The number of 2xx response status codes in a specific period of time.
Status3XX	Long	133209	The number of 3xx response status codes in a specific period of time.
Status403	Long	0	The number of 403 response status codes in a specific period of time.
Status404	Long	897	The number of 404 response status codes in a specific period of time.
Status405	Long	0	The number of 405 response status codes in a specific period of time.
Status4XX	Long	5653	The number of 4xx response status codes in a specific period of time.
Status501	Long	0	The number of 501 response status codes in a specific period of time.
Status502	Long	0	The number of 502 response status codes in a specific period of time.
Status503	Long	0	The number of 503 response status codes in a specific period of time.
Status504	Long	0	The number of 504 response status codes in a specific period of time.

Parameter	Type	Example	Description
Status5XX	Long	14	The number of 5xx response status codes in a specific period of time.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDomainStatusCodeCount
&EndTime=1583683200
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeDomainStatusCodeCountResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <Status2XX>951472</Status2XX>
  <Status200>951159</Status200>
  <Status3XX>133209</Status3XX>
  <Status4XX>5653</Status4XX>
  <Status403>0</Status403>
  <Status404>897</Status404>
  <Status405>0</Status405>
  <Status5XX>14</Status5XX>
  <Status501>0</Status501>
  <Status502>0</Status502>
  <Status503>0</Status503>
  <Status504>0</Status504>
</DescribeDomainStatusCodeCountResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "Status2XX": 951472,
  "Status200": 951159,
  "Status3XX": 133209,
  "Status4XX": 5653,
  "Status403": 0,
  "Status404": 897,
  "Status405": 0,
  "Status5XX": 14,
  "Status501": 0,
  "Status502": 0,
  "Status503": 0,
  "Status504": 0
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).



## 12.15.15 DescribeDomainTopAttackList

Queries the peak queries per second (QPS) information of a website, such as the attack QPS and total QPS, within a specified period of time.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainTopAttackList	The operation that you want to perform. Set the value to <b>DescribeDomainTopAttackList</b> .
<b>EndTime</b>	Long	Yes	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.
<b>StartTime</b>	Long	Yes	1582992000	The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.



Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

### Response parameters

Parameter	Type	Example	Description
AttackList	Array		The peak QPS of the website.
Attack	Long	0	The attack QPS. Unit: queries per second.
Count	Long	294	The number of all QPS, which includes normal and attack QPS. Unit: queries per second.
Domain	String	www.aliyun.com	The domain name of the website.
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainTopAttackList
&EndTime=1583683200
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeDomainTopAttackListResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <AttackList>
    <Count>294</Count>
    <Attack>0</Attack>
    <Domain>www.aliyun.com</Domain>
  </AttackList>
</DescribeDomainTopAttackListResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "AttackList": [
    {
      "Count": 294,
      "Attack": 0,
      "Domain": "www.aliyun.com"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).



## 12.15.16 DescribeDomainViewSourceCountries


Queries the regions outside China from which requests are sent to a website within a specific period of time.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

**Request parameters**

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainViewSourceCountries	The operation that you want to perform. Set the value to <b>DescribeDomainViewSourceCountries</b> .
<b>EndTime</b>	Long	Yes	1583683200	<p>The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div> <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.</div>
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div> <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.</div>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is left blank by default, which indicates that the instance belongs to the default resource group.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>Domain</b>	String	No	www.aliyun.com	The domain name of the website. <div>  <b>Note:</b>  A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names. </div>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.
SourceCountries	Array		The regions outside China from which the requests are sent.
Count	Long	3390671	The number of requests.

Parameter	Type	Example	Description
CountryId	String	cn	The country code. For more information about codes of regions outside China, see the Codes of regions outside China table in this topic.

#### Codes of regions outside China

Code	Region	Abbreviation
1	China	CN
2	Australia	AU
3	Japan	JP
4	Thailand	TH
5	India	IN
7	United States	US
8	Germany	DE
9	Netherlands	NL
10	Malaysia	MY
11	Angola	AO
12	South Korea	KR
13	Singapore	SG
14	Kampuchea	KH
16	Philippines	PH
17	Vietnam	VN

Code	Region	Abbreviation
18	France	FR
19	Poland	PL
20	Spain	ES
21	Russia	RU
22	Switzerland	CH
23	United Kingdom	GB
24	Italy	IT
25	Czech Republic	CZ
26	Ireland	IE
27	Denmark	DK
28	Portugal	PT
29	Sweden	SE
30	Ghana	GH
31	Turkey	TR
32	Cameroon	CM
33	South Africa	ZA
34	Finland	FI
35	Hungary	HU
36	United Arab Emirates	AE
37	Greece	GR

Code	Region	Abbreviation
38	Brazil	BR
39	Austria	AT
40	Jordan	JO
41	Belgium	BE
42	Romania	RO
43	Luxembourg	LU
44	Argentina	AR
45	Uganda	UG
46	Armenia	AM
47	Tanzania	TZ
48	Burundi	BI
49	Uruguay	UY
50	Bulgaria	BG
51	Ukraine	UA
52	Israel	IL
53	Qatar	QA
54	Iraq	IQ
55	Lithuania	LT
56	Moldova	MD
57	Uzbekistan	UZ

Code	Region	Abbreviation
58	Slovakia	SK
59	Kazakhstan	KZ
60	Croatia	HR
61	Georgia	GE
62	Estonia	EE
63	Gibraltar	GI
64	Latvia	LV
65	Norway	NO
66	Palestine	PS
67	Cyprus	CY
68	Saudi Arabia	SA
69	Iran	IR
70	Canada	CA
71	American Samoa	AS
72	Syria	SY
73	Kuwait	KW
74	Bahrain	BH
75	Lebanon	LB
76	Oman	OM
77	Azerbaijan	AZ



Code	Region	Abbreviation
78	Zambia	ZM
79	Zimbabwe	ZW
80	Democratic Republic of the Congo	CD
81	Serbia	RS
82	Iceland	IS
83	Slovenia	SI
84	Macedonia	MK
85	Liechtenstein	LI
86	Jersey	JE
87	Bosnia and Herzegovina	BA
88	Chile	CL
89	Peru	PE
90	Kyrgyzstan	KG
91	Reunion	RE
92	Tajikistan	TJ
93	Isle of Man	IM
94	Guernsey	GG
95	Malta	MT
96	Libya	LY

Code	Region	Abbreviation
97	Yemen	YE
98	Belarus	BY
99	Mayotte	YT
100	Guadeloupe	GP
101	Saint Martin	MF
102	Martinique	MQ
103	Guyana	GY
104	Kosovo	XK
105	Indonesia	ID
106	Northern Mariana Islands	MP
107	Dominican Republic	DO
108	Mexico	MX
109	Guam	GU
110	Nigeria	NG
111	Venezuela	VE
112	Puerto Rico	PR
113	Mongolia	MN
114	New Zealand	NZ
115	Bangladesh	BD
116	Pakistan	PK

Code	Region	Abbreviation
117	Papua New Guinea	PG
118	Trinidad and Tobago	TT
119	Lesotho	LS
120	Colombia	CO
121	Costa Rica	CR
123	Ecuador	EC
124	Sri Lanka	LK
125	Egypt	EG
126	British Virgin Islands	VG
127	Jamaica	JM
128	Saint Lucia	LC
129	Cayman Islands	KY
130	Grenada	GD
131	Curacao	CW
132	Panama	PA
133	Barbados	BB
134	The Bahamas	BS
135	Nepal	NP
136	Tokelau	TK
137	Maldives	MV

Code	Region	Abbreviation
138	Afghanistan	AF
139	New Caledonia	NC
140	Fiji	FJ
141	Wallis and Futuna Islands	WF
142	Albania	AL
143	San Marino	SM
144	Montenegro	ME
145	East Timor	TL
146	Monaco	MC
147	Guinea	GN
148	Myanmar	MM
149	Greenland	GL
150	Bermuda	BM
151	Saint Vincent and the Grenadines	VC
152	United States Virgin Islands	VI
153	Suriname	SR
154	Saint Barthelemy	BL
155	Haiti	HT
156	Antigua and Barbuda	AG

Code	Region	Abbreviation
157	Liberia	LR
158	Kenya	KE
159	Botswana	BW
160	Mozambique	MZ
161	Senegal	SN
162	Madagascar	MG
163	Namibia	NA
164	Côte d'Ivoire	CI
165	Sudan	SD
166	Malawi	MW
167	Gabon	GA
168	Mali	ML
169	Benin	BJ
170	Chad	TD
171	Cabo Verde	CV
172	Rwanda	RW
173	Republic of the Congo	CG
174	The Gambia	GM
175	Mauritius	MU
176	Algeria	DZ

Code	Region	Abbreviation
177	Eswatini	SZ
178	Burkina Faso	BF
179	Sierra Leone	SL
180	Somalia	SO
181	Niger	NE
182	Central Africa Republic	CF
183	Togo	TG
184	South Sudan	SS
185	Equatorial Guinea	GQ
186	Seychelles	SC
187	Djibouti	DJ
188	Morocco	MA
189	Mauritania	MR
190	Comoros	KM
191	British Indian Ocean Territory	IO
192	Tunisia	TN
193	Laos	LA
194	Brunei	BN
195	Bhutan	BT
196	Nauru	NR

Code	Region	Abbreviation
197	Vanuatu	VU
198	Federated States of Micronesia	FM
199	French Polynesia	PF
200	Tonga	TO
201	Honduras	HN
202	Bolivia	BO
203	El Salvador	SV
204	Guatemala	GT
205	Nicaragua	NI
206	Belize	BZ
207	Paraguay	PY
208	French Guiana	GF
209	Andorra	AD
210	Faroe Islands	FO
211	Niue	NU
212	Kiribati	KI
213	Marshall Islands	MH
214	Palau	PW
215	Samoa	WS

Code	Region	Abbreviation
216	Solomon Islands	SB
217	Tuvalu	TV
218	North Korea	KP
219	Vatican City	VA
220	Eritrea	ER
221	Ethiopia	ET
222	Guinea-Bissau	GW
223	Sao Tome and Principe	ST
224	Turkmenistan	TM
225	Cuba	CU
226	Dominica	DM
227	Saint Kitts and Nevis	KN
228	Aruba	AW
229	Falkland Islands	FK
230	Turks and Caicos Islands	TC
231	Caribbean Netherlands	BQ
232	Sint Maarten	SX
233	Montserrat	MS
234	Anguilla	AI
235	Saint Pierre and Miquelon	PM



Code	Region	Abbreviation
236	Åland Islands	AX
237	Norfolk Island	NF
238	Antarctica	AQ
239	Cook Islands	CK
240	Christmas Island	CX
241	Other regions in Europe	EU

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDomainViewSourceCountries
&EndTime=1583683200
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeDomainViewSourceCountriesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <SourceCountries>
    <Count>3390671</Count>
    <CountryId>cn</CountryId>
  </SourceCountries>
</DescribeDomainViewSourceCountriesResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "SourceCountries": [
    {
      "Count": 3390671,
      "CountryId": "cn"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.15.17 DescribeDomainViewSourceProvinces



Queries the regions inside China from which requests are sent to a website within a specific period of time.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainViewSourceProvinces	The operation that you want to perform. Set the value to <b>DescribeDomainViewSourceProvinces</b> .
<b>EndTime</b>	Long	Yes	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.

Parameter	Type	Required	Example	Description
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>ResourceGroupID</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou:</b> mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1:</b> outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>Domain</b>	String	No	www.aliyun.com	<p>The domain name of the website.</p> <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>

**Response parameters**

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.
SourceProvinces	Array		The information of the region inside China from which the requests are sent.
Count	Long	3390671	The number of requests.
ProvinceId	String	440000	The ID of the region inside China. For more information about codes of regions inside China, see the Codes of regions inside China table in this topic.

**Codes of regions inside China**

Code	Region
110000	Beijing
120000	Tianjin
130000	Hebei
140000	Shanxi
150000	Nei Mongol
210000	Liaoning
220000	Jilin
230000	Heilongjiang
310000	Shanghai

Code	Region
320000	Jiangsu
330000	Zhejiang
340000	Anhui
350000	Fujian
360000	Jiangxi
370000	Shandong
410000	Henan
420000	Hubei
430000	Hunan
440000	Guangdong
450000	Guangxi
460000	Hainan
500000	Chongqing
510000	Sichuan
520000	Guizhou
530000	Yunnan
540000	Xizang
610000	Shaanxi
620000	Gansu
630000	Qinghai

Code	Region
640000	Ningxia
650000	Xinjiang
810000	Hong Kong S.A.R
710000	Taiwan
820000	Macao S.A.R

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainViewSourceProvinces
&EndTime=1583683200
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeDomainViewSourceProvincesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <SourceProvinces>
    <Count>3390671</Count>
    <ProvinceId>440000</ProvinceId>
  </SourceProvinces>
</DescribeDomainViewSourceProvincesResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "SourceProvinces": [
    {
      "Count": 3390671,
      "ProvinceId": "440000"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.15.18 DescribeDomainViewTopCostTime


Queries the top N URLs that require the longest time to respond to requests within a specific period of time.

### Debugging


OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainViewTopCostTime	The operation that you want to perform. Set the value to <b>DescribeDomainViewTopCostTime</b> .
<b>EndTime</b>	Long	Yes	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.

Parameter	Type	Required	Example	Description
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>Top</b>	Integer	Yes	5	<p>The number of URLs to query. Valid values: <b>1</b> to <b>100</b>.</p>
<b>ResourceGroupID</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>



Parameter	Type	Required	Example	Description
<b>Domain</b>	String	No	www.aliyun.com	The domain name of the website.   <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.
UrlList	Array		The URLs who require the longest time to respond to requests.
CostTime	Float	3000	The response duration. Unit: milliseconds.
Domain	String	www.aliyun.com	The domain name of the website.
Url	String	LW==	The URL that is Base64-encoded.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeDomainViewTopCostTime
&EndTime=1583683200
&StartTime=1582992000
&Top=5
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<DescribeDomainViewTopCostTimeResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <UrlList>
    <CostTime>3000</CostTime>
    <Domain>www.aliyun.com</Domain>
```

```
<Url>Lw==</Url>
</UrlList>
</DescribeDomainViewTopCostTimeResponse>
```

JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "UrlList": [
    {
      "CostTime": 3000,
      "Domain": "www.aliyun.com",
      "Url": "Lw=="
    }
  ]
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.15.19 DescribeDomainViewTopUrl



Queries the top N URLs that receive the most requests within a specific period of time.


### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainViewTopUrl	The operation that you want to perform. Set the value to <b>DescribeDomainViewTopUrl</b> .

Parameter	Type	Required	Example	Description
<b>EndTime</b>	Long	Yes	1583683200	<p>The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>StartTime</b>	Long	Yes	1582992000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            This UNIX timestamp must indicate a time that is accurate to the minute.         </div>
<b>Top</b>	Integer	Yes	5	<p>The number of URLs to query. Valid values: <b>1</b> to <b>100</b>.</p>
<b>ResourceGroupid</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>Domain</b>	String	No	www.aliyun.com	The domain name of the website. <div>  <b>Note:</b>  A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names. </div>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.
UrlList	Array		The URLs that receive the most requests.
Count	Long	3390671	The total number of requests to the URL.
Domain	String	www.aliyun.com	The domain name of the website.
Url	String	Lw==	The URL that is Base64-encoded.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDomainViewTopUrl
```

```
&EndTime=1583683200
&StartTime=1582992000
&Top=5
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeDomainViewTopUrlResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
  <UrlList>
    <Count>3390671</Count>
    <Domain>www.aliyun.com</Domain>
    <Url>Lw==</Url>
  </UrlList>
</DescribeDomainViewTopUrlResponse>
```

JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E",
  "UrlList": [
    {
      "Count": 3390671,
      "Domain": "www.aliyun.com",
      "Url": "Lw=="
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).



## 12.15.20 DescribeDomainQpsWithCache


Queries the queries per second (QPS) information of a website, such as the total QPS, QPS blocked by different protection policies, and cache hit ratio.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

**Request parameters**

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDomainQpsWithCache	The operation that you want to perform. Set the value to <b>DescribeDomainQpsWithCache</b> .
<b>EndTime</b>	Long	Yes	1583683200	The end of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.
<b>StartTime</b>	Long	Yes	1582992000	The beginning of the time range to query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> This UNIX timestamp must indicate a time that is accurate to the minute.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>Domain</b>	String	No	www.aliyun.com	The domain name of the website. <div>  <b>Note:</b>  A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names. </div>

### Response parameters

Parameter	Type	Example	Description
Blocks	List	[20,30,20]	The attack QPS.
CacheHits	List	[0.3,0.4,0.5]	The cache hit ratios. This parameter is decimals. For example, 0.5 indicates that the cache hit ratio is 50%.

Parameter	Type	Example	Description
CcBlockQps	List	[1,0,0]	Details about the QPS blocked by the Frequency Control policy.
CcJsQps	List	[1,0,0]	Details about the QPS for which the Frequency Control policy triggers Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA).
Interval	Integer	20384	The intervals between every two adjacent records. Unit: seconds.
IpBlockQps	List	[1,0,0]	Details about the QPS blocked by the blacklist for domain names.
PreciseBlocks	List	[1,0,0]	Details about the QPS blocked by the Accurate Access Control policy.
PreciseJsQps	List	[1,0,0]	Details about the QPS for which the Accurate Access Control policy triggers the JavaScript challenge.
RegionBlocks	List	[1,0,0]	Details about the QPS blocked by the Blocked Regions policy.
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.
StartTime	Long	1582992000	The start time of the query. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Totals	List	[100,400,200]	The total numbers of returned QPS.



## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDomainQpsWithCache
&EndTime=1583683200
&StartTime=1582992000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeDomainQpsWithCacheResponse>
  <Interval>20384</Interval>
  <StartTime>1582992000</StartTime>
  <Totals>100</Totals>
  <Totals>400</Totals>
  <Totals>200</Totals>
  <Blocks>20</Blocks>
  <Blocks>30</Blocks>
  <Blocks>20</Blocks>
  <CacheHits>0.3</CacheHits>
  <CacheHits>0.4</CacheHits>
  <CacheHits>0.5</CacheHits>
  <CcBlockQps>1</CcBlockQps>
  <CcBlockQps>0</CcBlockQps>
  <CcBlockQps>0</CcBlockQps>
  <CcJsQps>1</CcJsQps>
  <CcJsQps>0</CcJsQps>
  <CcJsQps>0</CcJsQps>
  <IpBlockQps>1</IpBlockQps>
  <IpBlockQps>0</IpBlockQps>
  <IpBlockQps>0</IpBlockQps>
  <PreciseBlocks>1</PreciseBlocks>
  <PreciseBlocks>0</PreciseBlocks>
  <PreciseBlocks>0</PreciseBlocks>
  <PreciseJsQps>1</PreciseJsQps>
  <PreciseJsQps>0</PreciseJsQps>
  <PreciseJsQps>0</PreciseJsQps>
  <RegionBlocks>1</RegionBlocks>
  <RegionBlocks>0</RegionBlocks>
  <RegionBlocks>0</RegionBlocks>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DescribeDomainQpsWithCacheResponse>
```

#### JSON format

```
{
  "Interval": 20384,
  "StartTime": 1582992000,
  "Totals": [
    100,
    400,
    200
  ],
  "Blocks": [
    20,
    30,
    20
  ],
  "CacheHits": [
    0.3,
    0.4,
    0.5
  ],
  "CcBlockQps": [
    1,
    0,
    0
  ],
  "CcJsQps": [
    1,
    0,
    0
  ],
  "IpBlockQps": [
    1,
    0,
    0
  ],
  "PreciseBlocks": [
    1,
    0,
    0
  ],
  "PreciseJsQps": [
    1,
    0,
    0
  ],
  "RegionBlocks": [
    1,
    0,
    0
  ],
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

```
    ],
    "CacheHits": [
      0.3,
      0.4,
      0.5
    ],
    "CcBlockQps": [
      1,
      0,
      0
    ],
    "CcJsQps": [
      1,
      0,
      0
    ],
    "IpBlockQps": [
      1,
      0,
      0
    ],
    "PreciseBlocks": [
      1,
      0,
      0
    ],
    "PreciseJsQps": [
      1,
      0,
      0
    ],
    "RegionBlocks": [
      1,
      0,
      0
    ],
    "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
  }
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.16 Log analysis

### 12.16.1 DescribeSlsOpenStatus

Checks whether Log Service is activated.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeSlsOpenStatus	The operation that you want to perform. Set the value to <b>DescribeSlsOpenStatus</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

## Response parameters

Parameter	Type	Example	Description
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.
SlsOpenStatus	Boolean	true	Indicates whether Log Service is activated. Valid values: <ul style="list-style-type: none"><li>• <b>true</b></li><li>• <b>false</b></li></ul>

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeSlsOpenStatus
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeSlsOpenStatusResponse>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
  <SlsOpenStatus>true</SlsOpenStatus>
</DescribeSlsOpenStatusResponse>
```

#### JSON format

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "SlsOpenStatus": true
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.16.2 DescribeSlsAuthStatus

Checks whether Anti-DDoS Pro or Anti-DDoS Premium is authorized to access Log Service.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeSlsAuthStatus	The operation that you want to perform. Set the value to <b>DescribeSlsAuthStatus</b> .

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.
SlsAuthStatus	Boolean	true	Indicates whether Anti-DDoS Pro or Anti-DDoS Premium is authorized to access Log Service. Valid values: <ul style="list-style-type: none"><li>• <b>true</b></li><li>• <b>false</b></li></ul>

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeSlsAuthStatus
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<DescribeSlsAuthStatusResponse>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
  <SlsAuthStatus>true</SlsAuthStatus>
</DescribeSlsAuthStatusResponse>
```

#### JSON format

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "SlsAuthStatus": true
}
```

#### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.16.3 DescribeLogStoreExistStatus

Checks whether a Logstore is created for Anti-DDoS Pro or Anti-DDoS Premium.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

#### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeLogStoreExistStatus	The operation that you want to perform. Set the value to <b>DescribeLogStoreExistStatus</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
ExistStatus	Boolean	true	Indicates whether a Logstore is created for Anti-DDoS Pro or Anti-DDoS Premium. Valid values: <ul style="list-style-type: none"><li>• <b>true</b></li><li>• <b>false</b></li></ul>
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeLogStoreExistStatus
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeLogStoreExistStatus?
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
  <ExistStatus>true</ExistStatus>
</DescribeLogStoreExistStatus?
```

##### JSON format

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "ExistStatus": true
}
```

```
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.16.4 DescribeSlsLogstoreInfo

Queries the Logstore information of Anti-DDoS Pro or Anti-DDoS Premium, such as log storage capacity and duration.

## Debugging


OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeSlsLogstoreInfo	The operation that you want to perform. Set the value to <b>DescribeSlsLogstoreInfo</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.



## Response parameters

Parameter	Type	Example	Description
LogStore	String	ddoscoo-logstore	The Logstore of the instance.
Project	String	ddoscoo-project-181071506993****-cn-hangzhou	The Log Service project of the instance.
Quota	Long	3298534883328	The available log storage capacity. Unit: bytes.
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.
Ttl	Integer	180	The log storage duration. Unit: days.
Used	Long	0	The used log storage capacity. Unit: bytes. <div> <b>Note:</b> The statistics on Log Service are delayed for about two hours.</div>

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeSlsLogstoreInfo
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeSlsLogstoreInfoResponse>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
  <LogStore>ddoscoo-logstore</LogStore>
  <Project>ddoscoo-project-181071506993****-cn-hangzhou</Project>
  <Quota>3298534883328</Quota>
  <Ttl>180</Ttl>
  <Used>0</Used>
```

```
</DescribeSlsLogstoreInfoResponse>
```

JSON format

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "LogStore": "ddoscoo-logstore",
  "Project": "ddoscoo-project-181071506993****-cn-hangzhou",
  "Quota": 3298534883328,
  "Ttl": 180,
  "Used": 0
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.16.5 ModifyFullLogTtl

Modifies the full log storage duration for Anti-DDoS Pro or Anti-DDoS Premium.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	ModifyFullLogTtl	The operation that you want to perform. Set the value to <b>ModifyFullLogTtl</b> .
<b>Ttl</b>	Integer	Yes	30	The log storage duration of a website. Valid values: <b>30 to 180</b> . Unit: days.

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=ModifyFullLogTtl
&Ttl=30
&<Common request parameters>
```

#### Sample success responses

#### XML format

```
<ModifyFullLogTtlResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
```

```
</ModifyFullLogTtlResponse>
```

JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.16.6 DescribeWebAccessLogDispatchStatus

Checks whether the Log Analysis feature is enabled for all domain names.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebAccessLogDispatchStatus	The operation that you want to perform. Set the value to <b>DescribeWebAccessLogDispatchStatus</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>PageNumber</b>	Integer	No	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .
<b>PageSize</b>	Integer	No	10	The number of entries to return on each page.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.
SlsConfigStatus	Array		The status of the Log Analysis feature of all domain names.
Domain	String	www.aliyun.com	The domain name.
Enable	Boolean	true	Indicates whether the Log Analysis feature is enabled. Valid values: <ul style="list-style-type: none"><li><b>true</b></li><li><b>false</b></li></ul>
TotalCount	Integer	1	The total number of returned domain names.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeWebAccessLogDispatchStatus
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeWebAccessLogDispatchStatus>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
  <TotalCount>1</TotalCount>
  <SlsConfigStatus>
    <Enable>true</Enable>
    <Domain>www.aliyun.com</Domain>
  </SlsConfigStatus>
</DescribeWebAccessLogDispatchStatus>
```

#### JSON format

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "TotalCount": 1,
  "SlsConfigStatus": [
    {
      "Enable": true,
      "Domain": "www.aliyun.com"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.16.7 DescribeWebAccessLogStatus

Queries the Log Analysis configuration of a single website, such as the feature status and the Log Service project and Logstore that are used.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebAccessLogStatus	The operation that you want to perform. Set the value to <b>DescribeWebAccessLogStatus</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <div>  <b>Note:</b>            A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

## Response parameters

Parameter	Type	Example	Description
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.

Parameter	Type	Example	Description
SlsLogstore	String	ddoscoo-logstore	The Logstore of the instance.
SlsProject	String	ddoscoo-project-128965410602****-cn-hangzhou	The Log Service project of the instance.
SlsStatus	Boolean	true	Indicates whether the Log Analysis feature is enabled for the website. Valid values: <ul style="list-style-type: none"><li>• <b>true</b></li><li>• <b>false</b></li></ul>

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeWebAccessLogStatus
&Domain=www.aliyun.com
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeWebAccessLogStatusResponse>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
  <SlsStatus>true</SlsStatus>
  <SlsProject>ddoscoo-project-128965410602****-cn-hangzhou</SlsProject>
  <SlsLogstore>ddoscoo-logstore</SlsLogstore>
</DescribeWebAccessLogStatusResponse>
```

#### JSON format

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "SlsStatus": true,
  "SlsProject": "ddoscoo-project-128965410602****-cn-hangzhou",
  "SlsLogstore": "ddoscoo-logstore"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).




## 12.16.8 EnableWebAccessLogConfig

Enables the Log Analysis feature for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	EnableWebAccessLogConfig	The operation that you want to perform. Set the value to <b>EnableWebAccessLogConfig</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.  <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=EnableWebAccessLogConfig
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<EnableWebAccessLogConfigResponse>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
</EnableWebAccessLogConfigResponse>
```

##### JSON format

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.16.9 DisableWebAccessLogConfig

Disables the Log Analysis feature for a website.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DisableWebAccessLogConfig	The operation that you want to perform. Set the value to <b>DisableWebAccessLogConfig</b> .
<b>Domain</b>	String	Yes	www.aliyun.com	The domain name of the website.   <b>Note:</b> A forwarding rule must be configured for the domain name. You can call the <a href="#">DescribeDomains</a> operation to query all domain names.
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>

Parameter	Type	Required	Example	Description
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=DisableWebAccessLogConfig
&Domain=www.aliyun.com
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DisableWebAccessLogConfigResponse>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</requestId>
</DisableWebAccessLogConfigResponse>
```

##### JSON format

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.16.10 DescribeWebAccessLogEmptyCount

Queries the remaining quota that you can clear the Logstore.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeWebAccessLogEmptyCount	The operation that you want to perform. Set the value to <b>DescribeWebAccessLogEmptyCount</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

## Response parameters

Parameter	Type	Example	Description
AvailableCount	Integer	10	The remaining quota that you can clear the Logstore.
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeWebAccessLogEmptyCount
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeWebAccessLogEmptyCountResponse>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
  <AvailableCount>10</AvailableCount>
</DescribeWebAccessLogEmptyCountResponse>
```

#### JSON format

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80",
  "AvailableCount": 10
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.16.11 EmptySlsLogstore

Clears the Logstore of Anti-DDoS Pro or Anti-DDoS Premium.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	EmptySlsLogstore	The operation that you want to perform. Set the value to <b>EmptySlsLogstore</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

## Response parameters

Parameter	Type	Example	Description
RequestId	String	CF33B4C3-196E-4015-AADD-5CAD00057B80	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=EmptySlsLogstore
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<EmptySlsLogstoreResponse>
  <RequestId>CF33B4C3-196E-4015-AADD-5CAD00057B80</RequestId>
</EmptySlsLogstoreResponse>
```

#### JSON format

```
{
  "RequestId": "CF33B4C3-196E-4015-AADD-5CAD00057B80"
}
```

#### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.17 System configuration and logs

### 12.17.1 DescribeStsGrantStatus

Checks whether Anti-DDoS Pro or Anti-DDoS Premium is authorized to access other cloud services.


#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

#### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeStsGrantStatus	The operation that you want to perform. Set the value to <b>DescribeStsGrantStatus</b> .



Parameter	Type	Required	Example	Description
<b>Role</b>	String	Yes	AliyunDDoS COODefaultRole	<p>The role that is used to check. Set the value to <b>AliyunDDoS COODefaultRole</b>, which indicates the default role of Anti-DDoS Pro or Anti-DDoS Premium.</p> <div>  <b>Note:</b>            Anti-DDoS Pro or Anti-DDoS Premium uses the default role to access other cloud services.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

Parameter	Type	Example	Description
StsGrant	STRUCT		The authorization status of Anti-DDoS Pro or Anti-DDoS Premium.
Status	Integer	1	Indicates whether Anti-DDoS Pro or Anti-DDoS Premium is authorized to access other cloud services. Valid values: <ul style="list-style-type: none"><li><b>0</b>: not authorized</li><li><b>1</b>: authorized</li></ul>

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeStsGrantStatus
&Role=AliyunDDoSDefaultRole
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeStsGrantStatus
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <StsGrant>
    <Status>1</Status>
  </StsGrant>
</DescribeStsGrantStatus>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "StsGrant": {
    "Status": 1
  }
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.17.2 DescribeBackSourceCidr

Queries the back-to-origin CIDR blocks of Anti-DDoS Pro or Anti-DDoS Premium.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeBackSourceCidr	The operation that you want to perform. Set the value to <b>DescribeBackSourceCidr</b> .
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>Line</b>	String	No	coop-line-001	The Internet service provider (ISP) line that you want to query.

## Response parameters

Parameter	Type	Example	Description
Cidrs	List	[ "47. ***. ***.0/25", "47. ***. ***.128/25" ]	The back-to-origin CIDR blocks of Anti-DDoS Pro or Anti-DDoS Premium.
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeBackSourceCidr
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeBackSourceCidrResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <Cidrs>47. ***. ***.0/25</Cidrs>
  <Cidrs>47. ***. ***.128/25</Cidrs>
</DescribeBackSourceCidrResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "Cidrs": [
    "47. ***. ***.0/25",
    "47. ***. ***.128/25"
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.17.3 DescribeOpEntities

Queries operations logs of Anti-DDoS Pro.



### Note:


This operation is suitable only for Anti-DDoS Pro.


You can query operations performed on Anti-DDoS Pro, such as configuring burstable protection bandwidth, deactivating the black hole, configuring diversion from origin server, using mitigation sessions, changing the IP addresses of ECS origin servers, and clearing logs.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeOpEntities	The operation that you want to perform. Set the value to <b>DescribeOpEntities</b> .
<b>EndTime</b>	Long	Yes	1583683200000	The end of the time range to query. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.   <b>Note:</b> The time must be in the latest 30 days.
<b>PageNumber</b>	Integer	Yes	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .
<b>PageSize</b>	Integer	Yes	10	The number of entries to return on each page. Maximum value: <b>50</b> .

Parameter	Type	Required	Example	Description
<b>StartTime</b>	Long	Yes	1582992000000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            The time must be in the latest 30 days.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Set the value to <b>cn-hangzhou</b>, which indicates an Anti-DDoS Pro instance.</p>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>
<b>EntityType</b>	Integer	No	1	<p>The type of the operation object that you want to query. Valid values:</p> <ul style="list-style-type: none"> <li><b>1:</b> IP addresses of Anti-DDoS Pro instances</li> <li><b>2:</b> mitigation sessions</li> <li><b>3:</b> ECS instances</li> <li><b>4:</b> all logs</li> </ul>
<b>EntityObject</b>	String	No	203.***.***.132	<p>The operation object that you want to query.</p>

**Response parameters**

Parameter	Type	Example	Description
OpEntities	Array		Details about the operations log.
EntityObject	String	203.***.***.132	The operation object.
EntityType	Integer	1	The type of the operation object. Valid values: <ul style="list-style-type: none"><li>• <b>1</b>: IP address of Anti-DDoS Pro instances</li><li>• <b>2</b>: mitigation sessions</li><li>• <b>3</b>: ECS instances</li><li>• <b>4</b>: all logs</li></ul>
GmtCreate	Long	1584451769000	The time when the operation was performed. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
OpAccount	String	128965410602****	The Alibaba Cloud account that is used to perform the operation.

Parameter	Type	Example	Description
OpAction	Integer	9	<p>The type of the operation. Valid values :</p> <ul style="list-style-type: none"><li>• <b>1</b>: configuring burstable protection bandwidth.</li><li>• <b>5</b>: using mitigation sessions.</li><li>• <b>8</b>: changing IP addresses of ECS origin servers.</li><li>• <b>9</b>: deactivating the black hole.</li><li>• <b>10</b>: configuring diversion from origin server.</li><li>• <b>11</b>: clearing all logs.</li><li>• <b>12</b>: downgrading the specifications of instances. This operation is performed to downgrade the burstable protection bandwidth if the instance expires or the account has overdue payments.</li><li>• <b>13</b>: restoring the specifications of instances. This operation is performed to restore the burstable protection bandwidth if the instance is renewed or you have paid the overdue payments under your account.</li></ul>



Parameter	Type	Example	Description
OpDesc	String	<pre>{"newEntity":{"actionMethod":"undo"}}</pre>	<p>Details about the operation. This parameter is a JSON string. The fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>newEntity</b>: the values of the parameters after the operation. This field must be of the STRING type.</li> <li>• <b>oldEntity</b>: the values of the parameters before the operation. This field must be of the STRING type.</li> </ul> <p>Both <b>newEntity</b> and <b>oldEntity</b> are JSON strings. The returned parameters vary with <b>OpAction</b>.</p> <p>If <b>OpAction</b> is <b>1, 12</b>, or <b>13</b>, the returned parameter is described as follows:</p> <ul style="list-style-type: none"> <li>• <b>elasticBandwidth</b>: the burstable protection bandwidth. It is of the INTEGER type.</li> </ul> <p>For example: <pre>{"newEntity":{"elasticBandwidth":300},"oldEntity":{"elasticBandwidth":300}}</pre></p> <p>If <b>OpAction</b> is <b>5</b>, the returned parameters are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>bandwidth</b>: the burstable protection bandwidth. It is of the INTEGER type. Unit: Gbit/s.</li> <li>• <b>count</b>: the total number of mitigation sessions. It is of the INTEGER type.</li> <li>• <b>deductCount</b>: the number of used mitigation sessions. It is of the INTEGER type.</li> <li>• <b>expireTime</b>: the expiration time of the mitigation sessions. It is of the LONG type. This value is</li> </ul>

Parameter	Type	Example	Description
RequestId	String	FB24D70C-71F5-4000-8CD8-22CDA0C53CD1	The ID of the request.
TotalCount	Long	1	The total number of returned operation records.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeOpEntities
&EndTime=1583683200000
&PageNumber=1
&PageSize=10
&StartTime=1582992000000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeOpEntitiesResponse>
  <TotalCount>1</TotalCount>
  <RequestId>FB24D70C-71F5-4000-8CD8-22CDA0C53CD1</RequestId>
  <OpEntities>
    <EntityType>1</EntityType>
    <GmtCreate>1584451769000</GmtCreate>
    <OpAccount>128965410602****</OpAccount>
    <OpDesc>
      <newEntity>
        <actionMethod>undo</actionMethod>
      </newEntity>
    </OpDesc>
    <OpAction>9</OpAction>
    <EntityObject>203. **. *.132</EntityObject>
  </OpEntities>
</DescribeOpEntitiesResponse>
```

#### JSON format

```
{
  "TotalCount": 1,
  "RequestId": "FB24D70C-71F5-4000-8CD8-22CDA0C53CD1",
  "OpEntities": [
    {
      "EntityType": 1,
      "GmtCreate": 1584451769000,
      "OpAccount": "128965410602****",
      "OpDesc": {
        "newEntity": {
          "actionMethod": "undo"
        }
      }
    }
  ],
}
```

```
"OpAction": 9,
"EntityObject": "203. ***. ***.132"
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.17.4 DescribeDefenseRecords

Queries the logs of advanced mitigation sessions of Anti-DDoS Premium.




### Note:


This operation is suitable only for Anti-DDoS Premium.


## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeDefenseRecords	The operation that you want to perform. Set the value to <b>DescribeDefenseRecords</b> .
<b>EndTime</b>	Long	Yes	1583683200000	The end of the time range to query. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC. <div> <b>Note:</b> The time must be in the latest 90 days.</div>

Parameter	Type	Required	Example	Description
<b>PageNumber</b>	Integer	Yes	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .
<b>PageSize</b>	Integer	Yes	10	The number of entries to return on each page. Maximum value: <b>50</b> .
<b>StartTime</b>	Long	Yes	1582992000000	<p>The beginning of the time range to query. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.</p> <div>  <b>Note:</b>            The time must be in the latest 90 days.         </div>
<b>RegionId</b>	String	No	ap-southeast-1	The region ID of the instance. Set the value to <b>ap-southeast-1</b> , which indicates an Anti-DDoS Premium instance.
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the domain belongs to the default resource group.

Parameter	Type	Required	Example	Description
<b>InstanceId</b>	String	No	ddoscoo-cn-mp91j1ao****	The ID of the instance.   <b>Note:</b> You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.

### Response parameters

Parameter	Type	Example	Description
DefenseRecords	Array		Details about the log of an advanced mitigation session.
AttackPeak	Long	6584186000	The peak attack traffic. Unit: bit/s.
EndTime	Long	1583683200000	The end time of the advanced mitigation session. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
EventCount	Integer	2	The number of attacks.
InstanceId	String	ddoscoo-cn-mp91j1ao****	The ID of the instance.
StartTime	Long	1582992000000	The start time of the advanced mitigation session. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Example	Description
Status	Integer	0	The status of the advanced mitigation session. Valid values: <ul style="list-style-type: none"><li>• <b>0</b>: The advanced mitigation session is being used.</li><li>• <b>1</b>: The advanced mitigation session has been used.</li></ul>
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.
TotalCount	Long	1	The total number of advanced mitigation sessions.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDefenseRecords
&EndTime=1583683200000
&PageNumber=1
&PageSize=10
&StartTime=1582992000000
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeDefenseRecordsResponse>
  <TotalCount>1</TotalCount>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <DefenseRecords>
    <StartTime>1582992000000</StartTime>
    <EndTime>1583683200000</EndTime>
    <InstanceId>ddoscoo-cn-mp91j1ao****</InstanceId>
    <Status>0</Status>
    <AttackPeak>10</AttackPeak>
    <EventCount>1</EventCount>
  </DefenseRecords>
</DescribeDefenseRecordsResponse>
```

#### JSON format

```
{
  "TotalCount": 1,
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "DefenseRecords": [
    {
      "StartTime": 1582992000000,
```

```
"EndTime": 1583683200000,
"InstanceId": "ddoscoo-cn-mp91j1ao****",
"Status": 0,
"AttackPeak": 10,
"EventCount": 1
}
]
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.17.5 DescribeAsyncTasks

Queries details about asynchronous export tasks, such as the task IDs, start time, end time, task status, task parameters, and task results.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

### Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeAsyncTasks	The operation that you want to perform. Set the value to <b>DescribeAsyncTasks</b> .
<b>PageNumber</b>	Integer	Yes	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .
<b>PageSize</b>	Integer	Yes	10	The number of entries to return on each page. Maximum value: <b>20</b> .

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	No	cn-hangzhou	The region ID of the instance. Valid values: <ul style="list-style-type: none"><li>• <b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li><li>• <b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li></ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.

### Response parameters

Parameter	Type	Example	Description
AsyncTasks	Array		Details about the asynchronous export task.
EndTime	Long	157927362000	The end time of the task. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
StartTime	Long	156927362000	The start time of the task. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.



Parameter	Type	Example	Description
TaskId	Long	1	The ID of the task.
TaskParams	String	{"instanceId": "ddoscoo-cn- mp91j1ao****"}	<p>Details about the asynchronous export task. The parameter is a JSON string. The returned field in the value varies with <b>TaskType</b>.</p> <p>If the value of <b>TaskType</b> is <b>1</b>, <b>3</b>, <b>4</b>, <b>5</b>, or <b>6</b>, the returned fields in the value are described as follows:</p> <ul style="list-style-type: none"><li>• <b>instanceId</b>: the ID of the instance. This field must be of the STRING type.</li></ul> <p>If the value of <b>TaskType</b> is <b>2</b>, the returned field in the value is described as follows:</p> <ul style="list-style-type: none"><li>• <b>domain</b>: the domain name of the website. This field must be of the STRING type.</li></ul>

Parameter	Type	Example	Description
TaskResult	String	<pre>{   "instanceId": "ddoscoo-cn-mp91j1ao****",   "url": "https://****.oss-cn-beijing.aliyuncs.com/heap.bin?Expires=1584785140&amp;OSSAccessKeyId=TMP.3KfzD82FyRJevJdEkRX6JEFHhvbvRBBb75PZJnyJmksA2QkMm47xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcTBrN3rDu3v&amp;Signature=Sj8BNcsxJLE8l5qm4cjNlDt8gv****"} </pre>	<p>The task result. This parameter is a JSON string. The returned fields vary with <b>TaskType</b>.</p> <p>If the value of <b>TaskType</b> is <b>1</b>, <b>3</b>, <b>4</b>, <b>5</b>, or <b>6</b>, the returned fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>instanceId</b>: the ID of the instance. This field must be of the STRING type.</li> <li>• <b>url</b>: the URL to download the exported file from OSS. This field must be of the STRING type.</li> </ul> <p>If the value of <b>TaskType</b> is <b>2</b>, the returned fields in the value are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>domain</b>: the domain name of the website. This field must be of the STRING type.</li> <li>• <b>url</b>: the URL to download the exported file from OSS. This field must be of the STRING type.</li> </ul>
TaskStatus	Integer	2	<p>The status of the task. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: The task is initializing.</li> <li>• <b>1</b>: The task is in progress.</li> <li>• <b>2</b>: The task is succeeded.</li> <li>• <b>3</b>: The task failed.</li> </ul>

Parameter	Type	Example	Description
TaskType	Integer	5	The type of the task. Valid values: <ul style="list-style-type: none"> <li><b>1</b>: the task to export the port forwarding rules of an instance</li> <li><b>2</b>: the task to export the website forwarding rules of an instance</li> <li><b>3</b>: the task to export the session persistence and health check settings of an instance</li> <li><b>4</b>: the task to export the anti-DDoS protection policies of an instance</li> <li><b>5</b>: the task to download the blacklist for source IP addresses of an instance</li> <li><b>6</b>: the task to download the whitelist for source IP addresses of an instance</li> </ul>
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.
TotalCount	Integer	1	The total number of returned asynchronous export tasks.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAsyncTasks
&PageNumber=1
&PageSize=10
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeAsyncTasksResponse>
  <TotalCount>1</TotalCount>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
  <AsyncTasks>
    <TaskId>1</TaskId>
    <TaskType>5</TaskType>
    <TaskStatus>2</TaskStatus>
    <StartTime>156927362</StartTime>
    <EndTime>157927362</EndTime>
    <TaskParams>
```

```

        <instanceId>ddoscoo-cn-mp91j1ao****</instanceId>
      </TaskParams>
      <TaskResult>
        <instanceId>ddoscoo-cn-mp91j1ao****</instanceId>
        <url>https://****.oss-cn-beijing.aliyuncs.com/heap.bin?Expires=1584785140&
amp;OSSAccessKeyId=TMP.3KfzD82FyRjevJdEkRX6JEFHhbmRBBb75PZJnyJmksA2QkMm47
xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcTBrN3rDu3v&Signature=Sj8BNcsxJLE8l5qm4cjN
lDt8gv****</url>
      </TaskResult>
    </AsyncTasks>
  </DescribeAsyncTasksResponse>

```

#### JSON format

```

{
  "TotalCount": 1,
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc",
  "AsyncTasks": [
    {
      "TaskId": 1,
      "TaskType": 5,
      "TaskStatus": 2,
      "StartTime": 156927362,
      "EndTime": 157927362,
      "TaskParams": {
        "instanceId": "ddoscoo-cn-mp91j1ao****"
      },
      "TaskResult": {
        "instanceId": "ddoscoo-cn-mp91j1ao****",
        "url": "https://****.oss-cn-beijing.aliyuncs.com/heap.bin?Expires=1584785140
&OSSAccessKeyId=TMP.3KfzD82FyRjevJdEkRX6JEFHhbmRBBb75PZJnyJmksA2QkMm47
xFAFDgMhEV8Nm6Vxr8xExMfiy9LsUFAcLcTBrN3rDu3v&Signature=Sj8BNcsxJLE8l5qm4cjN
lDt8gv****"
      }
    }
  ]
}

```

#### Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.17.6 CreateAsyncTask

Creates an asynchronous export task to export forwarding rules for websites, port forwarding rules, session persistence and health check settings, anti-DDoS protection policies, IP address blacklist, or IP address whitelist.

#### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

**Request parameters**

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	CreateAsyncTask	The operation that you want to perform. Set the value to <b>CreateAsyncTask</b> .
<b>TaskParams</b>	String	Yes	{"instanceId": "ddoscoo-cn-mp91j1ao****"}	<p>Details about the asynchronous export task. This parameter is a JSON string. The field in the value varies with <b>TaskType</b>.</p> <p>If you set <b>TaskType</b> to <b>1</b>, <b>3</b>, <b>4</b>, <b>5</b>, or <b>6</b>, the field in the value is described as follows:</p> <ul style="list-style-type: none"><li>• <b>instanceId</b>: the ID of the instance. This field is required and must be of the STRING type.</li></ul> <p>If you set <b>TaskType</b> to <b>2</b>, the field in the value is described as follows:</p> <ul style="list-style-type: none"><li>• <b>domain</b>: the domain name of the website, which must be of the STRING type. If you do not specify this field, the forwarding rules of all websites are exported.</li></ul>

Parameter	Type	Required	Example	Description
<b>TaskType</b>	Integer	Yes	5	<p>The type of the asynchronous export task. Valid values:</p> <ul style="list-style-type: none"> <li><b>1:</b> the task to export the port forwarding rules of an instance</li> <li><b>2:</b> the task to export the forwarding rules of a website protected by an instance</li> <li><b>3:</b> the task to export the session persistence and health check settings of an instance</li> <li><b>4:</b> the task to export the anti-DDoS protection policies of an instance</li> <li><b>5:</b> the task to download the blacklist for source IP addresses of an instance</li> <li><b>6:</b> the task to download the whitelist for source IP addresses of an instance</li> </ul>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou:</b> mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1:</b> outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	<p>The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.</p>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=CreateAsyncTask
&TaskParams={"instanceId": "ddoscoo-cn-mp91j1ao****"}
&TaskType=5
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<CreateAsyncTaskResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</CreateAsyncTaskResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


## 12.17.7 DeleteAsyncTask

Deletes an asynchronous export task.

### Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteAsyncTask	The operation that you want to perform. Set the value to <b>DeleteAsyncTask</b> .
<b>TaskId</b>	Integer	Yes	1	<p>The ID of the task that you want to delete.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeAsyncTasks</a> operation to query the IDs of all asynchronous export tasks.         </div>
<b>RegionId</b>	String	No	cn-hangzhou	<p>The region ID of the instance. Valid values:</p> <ul style="list-style-type: none"> <li><b>cn-hangzhou</b>: mainland China, which indicates an Anti-DDoS Pro instance</li> <li><b>ap-southeast-1</b>: outside mainland China, which indicates an Anti-DDoS Premium instance</li> </ul>
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.



## Response parameters

Parameter	Type	Example	Description
RequestId	String	0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DeleteAsyncTask
&TaskId=1
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DeleteAsyncTaskResponse>
  <RequestId>0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc</RequestId>
</DeleteAsyncTaskResponse>
```

#### JSON format

```
{
  "RequestId": "0bcf28g5-d57c-11e7-9bs0-d89d6717dxbc"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.18 Tag

### 12.18.1 DescribeTagKeys

Queries all tag keys.

**Note:**

The tag feature is suitable only for Anti-DDoS Pro.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

**Request parameters**

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeTagKeys	The operation that you want to perform. Set the value to <b>DescribeTagKeys</b> .
<b>RegionId</b>	String	Yes	cn-hangzhou	The region ID of the instance. Set the value to <b>cn-hangzhou</b> , which indicates an Anti-DDoS Pro instance.
<b>ResourceType</b>	String	Yes	INSTANCE	The type of the resource. Set the value to <b>INSTANCE</b> , which indicates an Anti-DDoS Pro instance.
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>PageSize</b>	Integer	No	10	The number of entries to return on each page.
<b>PageNumber</b>	Integer	No	1	The number of the page to return. For example, to query the returned results on the first page, set the value to <b>1</b> .

## Response parameters

Parameter	Type	Example	Description
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	1B0D6FCD-ED11-46B7-9903-D5A45509EC11	The ID of the request.
TagKeys	Array		The information of the tag key.
TagCount	Integer	6	The total number of resources bound to the tag key.
TagKey	String	aa1	The tag key.
TotalCount	Integer	3	The total number of returned tag keys.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeTagKeys
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeTagKeysResponse>
  <TotalCount>3</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>1B0D6FCD-ED11-46B7-9903-D5A45509EC11</RequestId>
  <PageNumber>1</PageNumber>
  <TagKeys>
    <TagCount>6</TagCount>
    <TagKey>aa1</TagKey>
  </TagKeys>
  <TagKeys>
    <TagCount>1</TagCount>
    <TagKey>aa134</TagKey>
  </TagKeys>
  <TagKeys>
```

```
<TagCount>6</TagCount>
<TagKey>aa2</TagKey>
</TagKeys>
</DescribeTagKeysResponse>
```

JSON format

```
{
  "TotalCount":3,
  "PageSize":10,
  "RequestId":"1B0D6FCD-ED11-46B7-9903-D5A45509EC11",
  "PageNumber":1,
  "TagKeys":[
    {
      "TagCount":6,
      "TagKey":"aa1"
    },
    {
      "TagCount":1,
      "TagKey":"aa134"
    },
    {
      "TagCount":6,
      "TagKey":"aa2"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.18.2 DescribeTagResources

Queries the tags bound to resources.



### Note:


The tag feature is suitable only for Anti-DDoS Pro.



## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DescribeTagResources	The operation that you want to perform. Set the value to <b>DescribeTagResources</b> .

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	Yes	cn-hangzhou	The region ID of the instance. Set the value to <b>cn-hangzhou</b> , which indicates an Anti-DDoS Pro instance.
<b>ResourceType</b>	String	Yes	INSTANCE	The type of the resource. Set the value to <b>INSTANCE</b> , which indicates an Anti-DDoS Pro instance.
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>ResourceIds.N</b>	RepeatList	No	ddoscoo-cn-mp91j1ao****	<p>The ID of resource N whose tags you want to query. The resource indicates the instance.</p> <div>  <b>Note:</b>            You must either specify <b>ResourceIds.N</b> or specify both <b>Tags.N.Key</b> and <b>Tags.N.Value</b>. You can call the <a href="#">DescribeInstances</a> operation to query the IDs of all instances.         </div>

Parameter	Type	Required	Example	Description
<b>Tags.N.Key</b>	String	No	testkey	<p>The key of tag N that you want to query.</p> <div>  <b>Note:</b>            You must either specify <b>ResourceIds.N</b> or specify both <b>Tags.N.Key</b> and <b>Tags.N.Value</b>. If you specify the <b>Tags.N.Key</b> parameter, you must also specify the <b>Tags.N.Value</b> parameter.         </div>
<b>Tags.N.Value</b>	String	No	testvalue	<p>The value of tag N that you want to query.</p> <div>  <b>Note:</b>            You must either specify <b>ResourceIds.N</b> or both <b>Tags.N.Key</b> and <b>Tags.N.Value</b>. If you specify the <b>Tag.N.Key</b> parameter, you must also specify the <b>Tags.N.Value</b> parameter.         </div>
<b>NextToken</b>	String	No	RGuYpqDdKh zXb8C3. D1BwQgc1tM BsoxdGiEKH HUUCf****	The token used to query the next page. If the next page does not exist, leave this parameter empty.

### Response parameters

Parameter	Type	Example	Description
NextToken	String	RGuYpqDdKh zXb8C3. D1BwQgc1tM BsoxdGiEKHHUUCf ****	The token used to query the next page. If the value of this parameter is empty, the next page does not exist.
RequestId	String	36E698F7-48A4-48D0-9554-0BB4BAAB99B3	The ID of the request.

Parameter	Type	Example	Description
TagResources	Array		The tag bound to the resource.
TagResource			
ResourceId	String	ddoscoo-cn-mp91j1ao****	The ID of the resource. The resource indicates the instance.
ResourceType	String	INSTANCE	The type of the resource. The value is <b>INSTANCE</b> , which indicates an Anti-DDoS Pro instance.
TagKey	String	aa1	The key of the tag bound to the resource.
TagValue	String	aa1_1	The value of the tag bound to the resource.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeTagResources
&RegionId=cn-hangzhou
&ResourceType=INSTANCE
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeTagResources>
  <NextToken>RGuYpqDdKhZxb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****</NextToken>
  <RequestId>36E698F7-48A4-48D0-9554-0BB4BAAB99B3</RequestId>
  <TagResources>
    <ResourceId>ddoscoo-cn-mp91j1ao****</ResourceId>
    <TagKey>aa1</TagKey>
    <ResourceType>INSTANCE</ResourceType>
    <TagValue>aa1_1</TagValue>
  </TagResources>
</DescribeTagResources>
```

#### JSON format

```
{
  "NextToken": "RGuYpqDdKhZxb8C3.D1BwQgc1tMBsoxdGiEKHHUUCf****",
  "RequestId": "36E698F7-48A4-48D0-9554-0BB4BAAB99B3",
  "TagResources": [
    {
```

```
"ResourceId":"ddoscoo-cn-mp91j1ao****",
"TagKey":"aa1",
"ResourceType":"INSTANCE",
"TagValue":"aa1_1"
}
]
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.18.3 CreateTagResources

Binds tags to resources.



### Note:

The tag feature is suitable only for Anti-DDoS Pro.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	CreateTagResources	The operation that you want to perform. Set the value to <b>CreateTagResources</b> .
<b>RegionId</b>	String	Yes	cn-hangzhou	The region ID of the instance. Set the value to <b>cn-hangzhou</b> , which indicates an Anti-DDoS Pro instance.



Parameter	Type	Required	Example	Description
<b>ResourceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	<p>The ID of resource N to which you want to bind with a tag. The resource indicates the instance.</p> <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstancels</a> operation to query the IDs of all instances.         </div>
<b>ResourceType</b>	String	Yes	INSTANCE	The type of the resource. Set the value to <b>INSTANCE</b> , which indicates an Anti-DDoS Pro instance.
<b>ResourceGroupId</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>Tags.N.Key</b>	String	No	testkey	The key of tag N that you want to bind to the resource.
<b>Tags.N.Value</b>	String	No	testvalue	The value of tag N that you want to bind to the resource.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=CreateTagResources
&RegionId=cn-hangzhou
&ResourceIds.1=ddoscoo-cn-mp91j1ao****
&ResourceType=INSTANCE
&Tag.1.Key=testkey
&Tag.1.Value=testvalue
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<CreateTagResourcesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</CreateTagResourcesResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.18.4 DeleteTagResources

Unbinds tags from resources.



### Note:

The tag feature is suitable only for Anti-DDoS Pro.

## Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

## Request parameters

Parameter	Type	Required	Example	Description
<b>Action</b>	String	Yes	DeleteTagResources	The operation that you want to perform. Set the value to <b>DeleteTagResources</b> .

Parameter	Type	Required	Example	Description
<b>RegionId</b>	String	Yes	cn-hangzhou	The region ID of the instance. Set the value to <b>cn-hangzhou</b> , which indicates an Anti-DDoS Pro instance.
<b>ResourceIds.N</b>	RepeatList	Yes	ddoscoo-cn-mp91j1ao****	The ID of resource N from which you want to unbind tags. The resource indicates the instance.  <div>  <b>Note:</b>            You can call the <a href="#">DescribeInstancelds</a> operation to query the IDs of all instances.         </div>
<b>ResourceType</b>	String	Yes	INSTANCE	The type of the resource. Set the value to <b>INSTANCE</b> , which indicates an Anti-DDoS Pro instance.
<b>ResourceGroupID</b>	String	No	default	The ID of the resource group to which the instance belongs in Resource Management. This parameter is empty by default, which indicates that the instance belongs to the default resource group.
<b>TagKey.N</b>	RepeatList	No	testkey	The key of tag N that you want to unbind.
<b>All</b>	Boolean	No	false	Specifies whether to unbind all tags from the specified resource. Valid values: <ul style="list-style-type: none"> <li><b>true</b></li> <li><b>false</b></li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/?Action=DeleteTagResources
&RegionId=cn-hangzhou
&ResourceIds.1=ddoscoo-cn-mp91j1ao****
&ResourceType=INSTANCE
TagKey.1=testkey
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DeleteTagResourcesResponse>
  <RequestId>C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E</RequestId>
</DeleteTagResourcesResponse>
```

#### JSON format

```
{
  "RequestId": "C33EB3D5-AF96-43CA-9C7E-37A81BC06A1E"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 12.19 Error codes

The following table lists the error codes that the Anti-DDoS Pro or Anti-DDoS Premium API operations can return.

Error code	Description
DomainNotExist	The error message returned because the specified domain name does not exist.
DomainExist	The error message returned because the specified domain name belongs to another user.

Error code	Description
WebRulePortDeny	The error message returned because the port has been used in forwarding rules for website services.
InvalidParameter.JSONError	The error message returned because the JSON format is incorrect.
ExceedFuncSpec	The error message returned because the function plan cannot meet your requirements.
ExceedNoStandardPort	The error message returned because the port is an invalid non-standard port.
InvalidWebRule	The error message returned because the forwarding rule for a website is invalid.
NetworkRuleExist	The error message returned because a forwarding rule has been configured for the port.
NetworkRuleConflict	The error message returned because the port forwarding rules conflict.
ExceedWebRuleLimit	The error message returned because the maximum number of protected domain names has been reached.
ExceedNetworkRuleLimit	The error message returned because the maximum number of protected ports has been reached.
InvalidDomain	The error message returned because the domain name is invalid.
UnBlackholeLimit	The error message returned because the quota that you can deactivate the black hole state has been reached.
InvalidIp	The error message returned because the specified IP address or CIDR block is invalid.
DomainOwnerError	The error message returned because the specified domain name belongs to another user.
InvalidParams	The error message returned because you are not authorized.
SchedulerNameConflict	The error message returned because the traffic scheduling rules conflict.

Error code	Description
CcRuleExist	The error message returned because the frequency control rule already exists.
CDNDomainExist	The error message returned because the CDN domain name already exists.
IpBlackholing	The error message returned because the IP address is in the black hole.
InvalidSwitch	The error message returned because the status switch of the last scheduling rule on the default line is disallowed.
ParamsConflict	The error message returned because a conflict has occurred among parameters, such as the record type, record value, line, and region ID.
UnkownError	The error message returned because an unknown error has occurred.
InstanceNotExist	The error message returned because the instance does not exist.