

# Alibaba Cloud

## Cloud Firewall API Reference

Document Version:

## Legal disclaimer

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

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

# Document conventions

Style	Description	Example
 <b>Danger</b>	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.
 <b>Warning</b>	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.
 <b>Notice</b>	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.
 <b>Note</b>	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>	<b>Bold</b> formatting is used for buttons, menus, page names, and other UI elements.	Click <b>OK</b> .
<b>Courier font</b>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[ ] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

# Table of Contents

1. List of operations by function	06
2. Request method	07
3. Common parameters	10
4. Access control	13
4.1. AddControlPolicy	13
4.2. DeleteControlPolicy	19
4.3. DescribeControlPolicy	21
4.4. DescribeDomainResolve	32
4.5. DescribePolicyPriorUsed	33
4.6. ModifyControlPolicyPosition	35
4.7. ModifyControlPolicy	36
4.8. Strict mode	42
4.8.1. DescribePolicyAdvancedConfig	42
4.8.2. ModifyPolicyAdvancedConfig	43
4.9. VPC firewalls	45
4.9.1. CreateVpcFirewallControlPolicy	45
4.9.2. DescribeVpcFirewallControlPolicy	50
4.9.3. ModifyVpcFirewallControlPolicy	60
4.9.4. ModifyVpcFirewallControlPolicyPosition	65
4.9.5. DeleteVpcFirewallControlPolicy	67
4.9.6. DescribeVpcFirewallPolicyPriorUsed	69
4.9.7. DescribeVpcFirewallAclGroupList	71
4.9.8. ResetVpcFirewallRuleHitCount	74
5. Firewall switch	76
5.1. PutEnableFwSwitch	76
5.2. PutDisableFwSwitch	78

---

5.3. PutEnableAllFwSwitch	80
5.4. PutDisableAllFwSwitch	81
6.Address books	83
6.1. AddAddressBook	83
6.2. DeleteAddressBook	86
6.3. ModifyAddressBook	87
6.4. DescribeAddressBook	90

# 1. List of operations by function

The following tables list API operations available for use in Cloud Firewall.

## Access control

Operation	Description
<a href="#">DescribePolicyPriorUsed</a>	Queries the priority range of access control policies that match specific query conditions.
<a href="#">ModifyControlPolicyPosition</a>	Modifies the priority of an access control policy.
<a href="#">DescribeControlPolicy</a>	Queries information about all the access control policies that match specific query conditions.
<a href="#">AddControlPolicy</a>	Creates an access control policy.
<a href="#">DeleteControlPolicy</a>	Deletes an access control policy.
<a href="#">ModifyControlPolicy</a>	Modifies an access control policy.

## Address book

Operation	Description
<a href="#">AddAddressBook</a>	Creates an access control address book.
<a href="#">DeleteAddressBook</a>	Deletes an access control address book.
<a href="#">ModifyAddressBook</a>	Modifies an access control address book.
<a href="#">DescribeAddressBook</a>	Queries detailed information about access control address books.

## 2. Request method

To send a Cloud Firewall API request, you must send an HTTP GET request to the Cloud Firewall endpoint. You must add the request parameters that correspond to the API operation being called. After you call the API, the system returns a response. The request and response are encoded in UTF-8.

### Request syntax

Cloud Firewall API operations use the RPC protocol. You can call Cloud Firewall API operations by sending HTTP GET requests.

The request syntax is as follows:


```
https://Endpoint/?Action=xx&Parameters
```

where:

- **Endpoint:** the endpoint of the Cloud Firewall API is `cloudfw.cn-hangzhou.aliyuncs.com`.
- **Action:** the name of the operation being performed. For example, to add an access control policy, you must set the Action parameter to `AddControlPolicy`.
- **Version:** the version of the Cloud Firewall API is `2017-12-07`.
- **Parameters:** the request parameters for the operation. Separate multiple parameters with ampersands (&).

Request parameters include both common parameters and operation-specific parameters. Common request parameters include the API version number and authentication information. For more information about common request parameters, see [Common parameters](#).

The following example demonstrates how to call the `AddControlPolicy` operation to add an access control policy:

 **Note** The following code has been edited to ease reading.

```
http(s)://cloudfw.cn-hangzhou.aliyuncs.com/? Action=AddControlPolicy
&Format=xml
&Version=2017-12-07
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
...
```

### API signature

You must sign all API requests to ensure security. Cloud Firewall uses the request signature to verify the identity of the API caller.

Cloud Firewall implements symmetric encryption with an AccessKey pair to verify the identity of the request sender. An AccessKey pair is an identity credential issued to Alibaba Cloud accounts and RAM users that is similar to a logon username and password. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. The AccessKey ID is used to verify the identity of the user, while the AccessKey secret is used to encrypt and verify the signature string. You must keep your AccessKey secret strictly confidential.

You must add the signature to the Cloud Firewall API request in the following format:

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSnc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

Take AddControlPolicy as an example. If the AccessKey ID is `testid` and the AccessKey secret is `testsecret`, the original request URL is as follows:

```
https://cloudfw.cn-hangzhou.aliyuncs.com/?Action=AddControlPolicy
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-12-07
&SignatureVersion=1.0
```

To calculate the signature, perform the following operations:

1. Use the request parameters to create the string to be signed.

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DAddControlPolicy&Format%3DXML&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version%3D2018-12-03
```

2. Calculate the HMAC value of the string.


Add an ampersand (&) to the end of the AccessKey secret. The result is used as the key to calculate the HMAC value. In this example, the key is `testsecret&`.

```
CT9X0VtwR86fNWSnc6v8YGOjuE=
```

3. Add the signature to the request parameters.



```
https://cloudfw.cn-hangzhou.aliyuncs.com/?Action=AddControlPolicy
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2017-12-07
&SignatureVersion=1.0
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

 **Note** Alibaba Cloud offers SDKs and third-party SDKs in multiple languages, helping you to calculate the signature. For more information about Alibaba Cloud SDKs, see [Alibaba Cloud SDKs](#).

## 3.Common parameters

This topic describes the common parameters for API operations provided by Cloud Firewall.

### Common request parameters

Parameter	Type	Required	Description
Region	String	Yes	The region ID of the Cloud Firewall instance. Set the value to <code>cn-hangzhou</code> (indicating mainland China).
Format	String	No	The format in which to return the response. Default value: <code>JSON</code> . Valid values: <ul style="list-style-type: none"> <li><code>JSON</code></li> <li><code>XML</code></li> </ul>
Version	String	Yes	The version number of the API, in the format of <code>YYYY-MM-DD</code> . Set the value to <code>2017-12-07</code> .
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The signature string of the current request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to <code>HMAC-SHA1</code> .

Parameter	Type	Required	Description
Timestamp	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, 2013-01-10T12:00:00Z indicates January 10, 2013, 20:00:00 (UTC+8).
SignatureVersion	String	Yes	The version of the signature encryption algorithm. Set the value to 1.0.
SignatureNonce	String	Yes	A unique, random number used to prevent replay attacks. You must use different numbers for different requests.
ResourceOwnerAccount	String	No	The account that owns the resource to be accessed through this API request.

### Examples

```
https://cloudfw.cn-hangzhou.aliyuncs.com/?Action=AddControlPolicy
&BizId=13688
&Region=cn
&Format=xml
&Version=2017-12-07
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
```

### Common response parameters

API responses use the HTTP response format where a 2xx status code indicates a successful call and a 4xx or 5xx status code indicates a failed call.

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.

- 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",
  /*Response data*/
}
```

# 4. Access control


## 4.1. AddControlPolicy


### 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
AclAction	String	Yes		The action that Cloud Firewall performs on the traffic. Valid values: <ul style="list-style-type: none"><li>• <b>accept</b>: Allow</li><li>• <b>drop</b>: Deny</li><li>• <b>log</b>: Monitor</li></ul>
Action	String	Yes		The operation that you want to perform. Set the value to AddControlPolicy.

Parameter	Type	Required	Example	Description
ApplicationName	String	Yes		<p>The type of applications to which the policy is applied.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• ANY</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• MySQL</li> <li>• SMTP</li> <li>• SMTPS</li> <li>• RDP</li> <li>• VNC</li> <li>• SSH</li> <li>• Redis</li> <li>• MQTT</li> <li>• MongoDB</li> <li>• Memcache</li> <li>• SSL</li> </ul> <p> <b>Note</b> The value of ANY indicates that the policy is applied to all types of applications.</p>
Description	String	Yes		The description of the access control policy.

Parameter	Type	Required	Example	Description
Destination	String	Yes		<p>The destination address to define in the access control policy.</p> <ul style="list-style-type: none"> <li>If the DestinationType parameter is set to net, this parameter specifies the destination CIDR block. Example: 1.2.3.4/24</li> <li>If the DestinationType parameter is set to group, this parameter specifies the name of the destination address book. Example: db_group</li> <li>If the DestinationType parameter is set to domain, this parameter specifies the destination domain name. Example: *.aliyuncs.com</li> <li>If the DestinationType parameter is set to location, this parameter specifies the destination region. For more information about region codes, see the following section. Example: ["BJ11", "ZB"]</li> </ul>
DestinationType	String	Yes		<p>The type of the destination address to define in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>net: destination CIDR block</li> <li>group: destination address book</li> <li>domain: destination domain name</li> <li>location: destination region</li> </ul>
Direction	String	Yes		<p>The traffic direction to define in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>in: inbound traffic</li> <li>out: outbound traffic</li> </ul>
NewOrder	String	Yes		<p>The priority of the access control policy. The priority value starts from 1. The smaller the priority number, the higher the priority.</p> <div style="background-color: #e0f2f7; padding: 5px; border: 1px solid #ccc;"> <p> <b>Note</b> The value of -1 indicates the lowest priority.</p> </div>

Parameter	Type	Required	Example	Description
Proto	String	Yes		<p>The security protocol type to define in the access control policy. If you cannot determine the protocol type, you can set this parameter to ANY. Valid values:</p> <ul style="list-style-type: none"> <li>• ANY</li> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>
Source	String	Yes		<p>The source address to define in the access control policy.</p> <ul style="list-style-type: none"> <li>• If the SourceType parameter is set to net, this parameter specifies the source CIDR block. Example: 1.2.3.0/24</li> <li>• If the SourceType parameter is set to group, this parameter specifies the name of the source address book. Example: db_group</li> <li>• If the SourceType parameter is set to location, this parameter specifies the source region. For more information about region codes, see the following section. Example: ["BJ11", "ZB"]</li> </ul>
SourceType	String	Yes		<p>The source address type to define in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>• net: source CIDR block</li> <li>• group: source address book</li> <li>• location: source region</li> </ul>
DestPort	String	No		<p>The destination port to define in the access control policy.</p> <div style="background-color: #e0f2f7; padding: 5px; border: 1px solid #ccc;"> <p> <b>Note</b> If the DestPortType parameter is set to port, this parameter is required.</p> </div>



Parameter	Type	Required	Example	Description
DestPortGroup	String	No		<p>The name of the destination port address book to define in the access control policy.</p> <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p> <b>Note</b> If the DestPortType parameter is set to group, this parameter is required.</p> </div>
DestPortType	String	No		<p>The type of the destination port to define in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>• port: port</li> <li>• group: port address book</li> </ul>
Lang	String	No		<p>The language of the request and response. Valid values:</p> <ul style="list-style-type: none"> <li>• en: English</li> <li>• zh: Chinese</li> </ul>
SourceIp	String	No		<p>The source IP address of the request.</p>

The region codes are as follows:

- Mainland China: ZD
- Beijing: BJ11
- Tianjin: TJ12
- Hebei Province: HB13
- Shanxi Province: SX14
- Liaoning Province: LN21
- Jilin Province: JL22
- Shanghai: SH31
- Jiangsu Province: JS32
- Zhejiang Province: ZJ33
- Anhui Province: AH34
- Fujian Province: FJ35
- Jiangxi Province: JX36
- Shandong Province: SD37
- Henan Province: HN41
- Hubei Province: HB42

- Hunan Province: HN43
- Guangdong Province: GD44
- Hainan Province: HN46
- Chongqing: CQ50
- Sichuan Province: SC51
- Guizhou Province: GZ52
- Yunnan Province: YN53
- Shaanxi Province: SX61
- Gansu Province: GS62
- Qinghai Province: QH63
- Heilongjiang Province: HLJ23
- Tibet Autonomous Region: XZ54
- Guangxi Zhuang Autonomous Region: GX45
- Inner Mongolia Autonomous Region: NMG15
- Ningxia Hui Autonomous Region: NX64
- Xinjiang Uygur Autonomous Region: XJ65
- Taiwan Province: TW
- Hong Kong SAR: HK
- Macao SAR: MO
- Outside China: ZB
- Asia (except China): ZC
- Europe: EU
- Africa: AF
- North America: NA
- South America: LA
- Oceania: OA
- Antarctica: AQ

## Response parameters

Parameter	Type	Example	Description
AclUuid	String		The unique ID of the access control policy.
RequestId	String		The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=AddControlPolicy
&AclAction=accept
&ApplicationName=ANY
&Description=demo_rule_1
&Destination=1.2.3.4/24
&DestinationType=net
&Direction=in
&NewOrder=-1
&Proto=TCP
&Source=1.2.3.0/24
&SourceType=net
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<AddControlPolicy>
  <RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
  <AclUuid>00281255-d220-4db1-8f4f-c4df221ad84c</AclUuid>
</AddControlPolicy>
```

#### JSON format

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "AclUuid": "00281255-d220-4db1-8f4f-c4df221ad84c"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

# 4.2. DeleteControlPolicy

## 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
AclUuid	String	Yes		The unique ID of the access control policy. You can call the DescribeControlPolicy operation to query the ID.
Action	String	Yes		The operation that you want to perform. Set the value to DeleteControlPolicy.
Direction	String	Yes		The traffic direction defined in the access control policy. Valid values: <ul style="list-style-type: none"> <li>in: inbound traffic</li> <li>out: outbound traffic</li> </ul>
Lang	String	No		The language of the request and response. Valid values: <ul style="list-style-type: none"> <li>en: English</li> <li>zh: Chinese</li> </ul>
SourceIp	String	No		The source IP address of the request.

## Response parameters

Parameter	Type	Example	Description
RequestId	String		The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DeleteControlPolicy
&AclUuid=00281255-d220-4db1-8f4f-c4df221ad84c
&Direction=in
&<Common request parameters>
```

### Sample success responses

**XML format**

```
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
```

**JSON format**

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

**Error codes**

For a list of error codes, visit the [API Error Center](#).

## 4.3. DescribeControlPolicy

Queries information about all the access control policies that meet specific query conditions.


**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	DescribeControlPolicy	The operation that you want to perform. Set the value to <b>DescribeControlPolicy</b> .
CurrentPage	String	Yes	1	The number of the page to return. Default value: 1
Direction	String	Yes	in	The direction of the traffic to which the access control policy applies. Valid values: <ul style="list-style-type: none"> <li>in: inbound traffic</li> <li>out: outbound traffic</li> </ul>

Parameter	Type	Required	Example	Description
PageSize	String	Yes	10	The number of entries to return on each page. Maximum value: 50.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>
Source	String	No	1.2.3.5	The source address defined in the access control policy. Fuzzy match is supported. The valid values of this parameter depend on the value of the SourceType parameter. <ul style="list-style-type: none"> <li>If SourceType is set to <code>net</code>, the value of this parameter is an IP address or CIDR block. Example: 10.0.1.0/24.</li> <li>If SourceType is set to <code>group</code>, the value of this parameter is an address book. Example: db_group. If the address book does not contain any IP addresses, all source addresses are queried.</li> <li>If SourceType is set to <code>location</code>, the value of this parameter is a region. Example: beijing.</li> <li>If SourceType is <code>not specified</code>, all types of source addresses are queried.</li> </ul>

Parameter	Type	Required	Example	Description
Destination	String	No	1.2.3.0	<p>The destination address defined in the access control policy. Fuzzy match is supported. The valid values of this parameter depend on the value of the DestinationType parameter.</p> <ul style="list-style-type: none"> <li>If DestinationType is set to <code>net</code>, the value of this parameter is an IP address or CIDR block. Example: 10.0.3.0/24.</li> <li>If DestinationType is set to <code>domain</code>, the value of this parameter is a domain name. Example: aliyun.</li> <li>If DestinationType is set to <code>group</code>, the value of this parameter is an address book. Example: db_group.</li> <li>If DestinationType is set to <code>location</code>, the value of this parameter is a region. Example: beijing.</li> <li>If DestinationType is <code>not specified</code>, all types of destination addresses are queried.</li> </ul>
Description	String	No	test	<p>The description of the access control policy. Fuzzy match is supported.</p> <div style="background-color: #e0f2f7; padding: 5px; border: 1px solid #ccc;"> <p> <b>Note</b> If this parameter is not specified, the descriptions of all access control policies are queried.</p> </div>

Parameter	Type	Required	Example	Description
Proto	String	No	TCP	The protocol type of traffic to which the access control policy applies. Valid values: <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> <li>• ANY: all types of protocols</li> <li>• Not specified: all types of protocols</li> </ul>
AclAction	String	No	accept	The action that Cloud Firewall performs on the traffic. Valid values: <ul style="list-style-type: none"> <li>• accept: allows the traffic.</li> <li>• drop: denies the traffic.</li> <li>• log: monitors the traffic.</li> <li>• Not specified: all actions.</li> </ul>
Release	String	No	true	Specifies whether the access control policy is enabled. By default, an access control policy is enabled after it is created. Valid values: <ul style="list-style-type: none"> <li>• true: The access control policy is enabled.</li> <li>• false: The access control policy is not enabled.</li> </ul>
AclUuid	String	No	00281255-d220-4db1-8f4f-c4df221ad84c	The unique ID of the access control policy.

## Response parameters

Parameter	Type	Example	Description
PageNo	String	1	The number of the page to return.
PageSize	String	10	The number of entries returned per page.
Policys	Array		The information about the access control policy.



Parameter	Type	Example	Description
AclAction	String	accept	The action that Cloud Firewall performs on the traffic. Valid values: <ul style="list-style-type: none"> <li>• <b>accept</b>: allows the traffic.</li> <li>• <b>drop</b>: denies the traffic.</li> <li>• <b>log</b>: monitors the traffic.</li> </ul>
AclUuid	String	00281255-d220-4db1-8f4f-c4df221ad84c	The unique ID of the access control policy.
ApplicationId	String	10***	The application ID defined in the access control policy.
ApplicationName	String	HTTP	The application type defined in the access control policy. Valid values: <ul style="list-style-type: none"> <li>• <b>FTP</b></li> <li>• <b>HTTP</b></li> <li>• <b>HTTPS</b></li> <li>• <b>Memcache</b></li> <li>• <b>MongoDB</b></li> <li>• <b>MQTT</b></li> <li>• <b>MySQL</b></li> <li>• <b>RDP</b></li> <li>• <b>Redis</b></li> <li>• <b>SMTP</b></li> <li>• <b>SMTPS</b></li> <li>• <b>SSH</b></li> <li>• <b>SSL</b></li> <li>• <b>VNC</b></li> <li>• <b>ANY</b>: all types of applications</li> </ul>
Description	String	test	The description of the access control policy.
DestPort	String	80	The destination port defined in the access control policy.
DestPortGroup	String	my_port_group	The name of the destination port address book defined in the access control policy.

Parameter	Type	Example	Description
DestPortGroupPorts	List	[80,443]	The ports in the destination port address book.
DestPortType	String	port	The destination port type defined in the access control policy. Valid values: <ul style="list-style-type: none"> <li>port: port</li> <li>group: port address book</li> </ul>
Destination	String	1.2.3.4/24	The destination address defined in the access control policy. The valid values of this parameter depend on the value of the DestinationType parameter. Valid values: <ul style="list-style-type: none"> <li>If DestinationType is set to net, the value of this parameter is an IP address or CIDR block. Example: 10.0.3.0/24.</li> <li>If DestinationType is set to domain, the value of this parameter is a domain name. For example, aliyuncs.com.</li> <li>If DestinationType is set to group, the value of this parameter is an address book. Example: db_group.</li> <li>If DestinationType is set to location, the value of this parameter is a region. For information about region codes, see <a href="#">AddControlPolicy</a>. Example: ["BJ11", "ZB"].</li> </ul>
DestinationGroupCidrs	List	["1.2.3.0/24", "1.2.3.1/32"]	The CIDR blocks in the destination address book defined in the access control policy.

Parameter	Type	Example	Description
DestinationGroupType	String	ip	<p>The type of the destination address book defined in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>ip</b>: an address book that includes one or more IP addresses</li> <li>• <b>tag</b>: an address book that includes one or more IP addresses with Elastic Compute Service (ECS) tags</li> <li>• <b>domain</b>: an address book that includes one or more domain names</li> <li>• <b>threat</b>: an address book that includes one or more malicious IP addresses or domain names</li> <li>• <b>backsrc</b>: an address book that includes one or more back-to-origin addresses of Anti-DDoS Pro or Premium instances or WAF instances.</li> </ul>
DestinationType	String	net	<p>The destination address type defined in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>net</b>: CIDR block</li> <li>• <b>group</b>: address book</li> <li>• <b>domain</b>: domain name</li> <li>• <b>location</b>: region</li> </ul>
Direction	String	in	<p>The direction of traffic to which the access control policy applies. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>in</b>: inbound traffic</li> <li>• <b>out</b>: outbound traffic</li> </ul>
DnsResult	String	1.1.1.1,2.2.2.2	The DNS resolution result.
DnsResultTime	Long	1579261141	The timestamp of the DNS resolution result.
HitTimes	Integer	100	The number of policy hits.

Parameter	Type	Example	Description
Order	Integer	1	<p>The priority of the access control policy.</p> <p>The priority value starts from 1. A smaller value indicates a higher priority.</p> <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p> <b>Note</b> The value of -1 indicates the lowest priority.</p> </div>
Proto	String	TCP	<p>The security protocol type defined in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>• ANY</li> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>
Release	String	true	<p>Indicates whether the access control policy is enabled. By default, an access control policy is enabled after it is created. Valid values:</p> <ul style="list-style-type: none"> <li>• true: The access control policy is enabled.</li> <li>• false: The access control policy is not enabled.</li> </ul>
Source	String	1.2.3.0/24	<p>The source address defined in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>• If SourceType is set to <code>net</code>, the value of this parameter is a CIDR block. Example: 10.0.1.0/24.</li> <li>• If SourceType is set to <code>group</code>, the value of this parameter is an address book. Example: db_group.</li> <li>• If SourceType is set to <code>location</code>, the value of this parameter is a region. For information about the location codes, see <a href="#">AddControlPolicy</a>. Example: ["BJ11", "ZB"].</li> </ul>
SourceGroupCidrs	List	["10.0.0.0/24", "10.0.0.1/32"]	<p>The CIDR blocks in the source address book defined in the access control policy.</p>

Parameter	Type	Example	Description
SourceGroupType	String	ip	<p>The type of the source address book defined in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li><b>ip:</b> an address book that includes one or more IP addresses</li> <li><b>tag:</b> an address book that includes one or more IP addresses with ECS tags</li> <li><b>domain:</b> an address book that includes one or more domain names</li> <li><b>threat:</b> an address book that includes one or more malicious IP addresses or domain names</li> <li><b>backsrc:</b> an address book that includes one or more back-to-origin addresses of Anti-DDoS Pro or Premium instances or WAF instances</li> </ul>
SourceType	String	net	<p>The type of the source address book defined in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li><b>net:</b> source CIDR block</li> <li><b>group:</b> source address book</li> <li><b>location:</b> source region</li> </ul>
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	The ID of the request.
TotalCount	String	100	The total number of the returned access control policies.

## Examples

### Sample requests

```

http(s)://[Endpoint]/? Action=DescribeControlPolicy
&CurrentPage=1
&Direction=in
&PageSize=10
&<Common request parameters>

```

### Sample success responses

`XML` format

```
<DescribeControlPolicyResponse>
<TotalCount>58</TotalCount>
<PageNo>1</PageNo>
<PageSize>10</PageSize>
<RequestId>A08BC58F-A83D-43EB-BC31-2F0D723929CC</RequestId>
<Policys>
<ApplicationName>RDP</ApplicationName>
<Description>11</Description>
<HitTimes>0</HitTimes>
<DestinationType>net</DestinationType>
<SourceType>net</SourceType>
<Proto>TCP</Proto>
<Order>5</Order>
<ApplicationId>27</ApplicationId>
<Direction>in</Direction>
<DestPortType>port</DestPortType>
<Source>1.1.1.1/32</Source>
<DestPort>1/1</DestPort>
<AclAction>accept</AclAction>
<AclUuid>53d82f0e-9bf1-4761-ab3b-a070b4811234</AclUuid>
<Destination>1.1.1.1/32</Destination>
<DnsResult>1.1.1.1,2.2.2.2</DnsResult>
<DnsResultTime>1579261141</DnsResultTime>
</Policys>
</DescribeControlPolicyResponse>
```

JSON format

```
{
  "TotalCount":58,
  "PageNo":1,
  "PageSize":10,
  "RequestId":"A08BC58F-A83D-43EB-BC31-2F0D723929CC",
  "Policies":[
    {
      "DestinationGroupCidrs":[

      ],
      "SourceGroupCidrs":[

      ],
      "ApplicationName":"RDP",
      "Description":"11",
      "HitTimes":0,
      "DestinationType":"net",
      "SourceType":"net",
      "Proto":"TCP",
      "Order":5,
      "ApplicationId":"27",
      "Direction":"in",
      "DestPortType":"port",
      "Source":"1.1.1.1/32",
      "DestPort":"1/1",
      "AclAction":"accept",
      "DestPortGroupPorts":[

      ],
      "AclUuid":"53d82f0e-9bf1-4761-ab3b-a070b4811234",
      "Destination":"1.1.1.1/32",
      "DnsResult": "1.1.1.1,2.2.2.2",
      "DnsResultTime": 1579261141
    }
  ]
}
```

## Error code

For a list of error codes, visit the [API Error Center](#).

## 4.4. DescribeDomainResolve

You can call this operation to obtain DNS resolution results. The results can only be obtained from Alibaba Cloud DNS, and can be obtained only when the domain names are resolved by using Alibaba Cloud DNS.

### 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
Domain	String	Yes	www.aliyun.com	The domain name to be resolved.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	The ID of the request.
ResolveResult	Struct		The DNS resolution result.
IpAddr	String	11.1.1.1,12.1.1.1	The resolved IP addresses. Separate multiple IP addresses with commas (,).
UpdateTime	Long	1579091739	The timestamp generated when DNS resolution was performed.

### Examples



### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDomainResolve
&Domain=www.aliyun.com
&<Common request parameters>
```

### Sample success responses

#### JSON format

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "ResolveResult": {
    IpAddrs:"11.1.1.1,12.1.1.1",
    UpdateTime:1579091739
  },
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).

## 4.5. DescribePolicyPriorUsed

### 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		The operation that you want to perform. Set the value to DescribePolicyPriorUsed.
Direction	String	Yes		The traffic direction defined in the access control policy. Valid values: <ul style="list-style-type: none"> <li>in: inbound traffic</li> <li>out: outbound traffic</li> </ul>

Parameter	Type	Required	Example	Description
Lang	String	No		The language of the request and response. Valid values: <ul style="list-style-type: none"> <li>en: English</li> <li>zh: Chinese</li> </ul>
SourceIp	String	No		The source IP address of the request.

### Response parameters

Parameter	Type	Example	Description
End	Integer		The lowest priority among the returned access control policies.
RequestId	String		The ID of the request.
Start	Integer		The highest priority among the returned access control policies.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=DescribePolicyPriorUsed
&Direction=in
&<Common request parameters>
```

#### Sample success responses

##### XML format

```
<DescribePolicyPriorUsed>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
<Start>1</Start>
<End>150</End>
</DescribePolicyPriorUsed>
```

##### JSON format

```
{
  "End":150,
  "Start":1,
  "RequestId":"CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

# 4.6. ModifyControlPolicyPosition

## 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		The operation that you want to perform. Set the value to <code>ModifyControlPolicyPosition</code> .
Direction	String	Yes		The traffic direction defined in the access control policy. Valid values: <ul style="list-style-type: none"> <li><code>in</code>: inbound traffic</li> <li><code>out</code>: outbound traffic</li> </ul>
NewOrder	String	Yes		The priority of the access control policy after modification.
OldOrder	String	Yes		The priority of the access control policy before modification.
Lang	String	No		The language of the request and response. Valid values: <ul style="list-style-type: none"> <li><code>en</code>: English</li> <li><code>zh</code>: Chinese</li> </ul>

Parameter	Type	Required	Example	Description
SourceIp	String	No		The source IP address of the request.

### Response parameters

Parameter	Type	Example	Description
RequestId	String		The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=ModifyControlPolicyPosition
&Direction=in
&NewOrder=1
&OldOrder=5
&<Common request parameters>
```

#### Sample success responses

**XML format**

```
<ModifyControlPolicyPosition>
<RequestId>850A84D6-0DE4-4797-A1E8-00090125EEB1</RequestId>
</ModifyControlPolicyPosition>
```

**JSON format**

```
{
  "RequestId": "850A84D6-0DE4-4797-A1E8-00090125EEB1"
}
```

### Error codes

For a list of error codes, visit the [API Error Center](#).


## 4.7. ModifyControlPolicy

### 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
AclAction	String	Yes		The action that Cloud Firewall performs on the traffic. Valid values: <ul style="list-style-type: none"> <li>• <b>accept</b>: Allow</li> <li>• <b>drop</b>: Deny</li> <li>• <b>log</b>: Monitor</li> </ul>
AclUuid	String	Yes		The unique ID of the access control policy. You can call the DescribeControlPolicy operation to query the ID.
Action	String	Yes		The operation that you want to perform. Set the value to ModifyControlPolicy.

Parameter	Type	Required	Example	Description
ApplicationName	String	Yes		<p>The application type defined in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• ANY</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• MySQL</li> <li>• SMTP</li> <li>• SMTPS</li> <li>• RDP</li> <li>• VNC</li> <li>• SSH</li> <li>• Redis</li> <li>• MQTT</li> <li>• MongoDB</li> <li>• Memcache</li> <li>• SSL</li> </ul> <p> <b>Note</b> The value of ANY indicates that the policy is applied to all types of applications.</p>
Description	String	Yes		The description of the access control policy.

Parameter	Type	Required	Example	Description
Destination	String	Yes		<p>The destination address defined in the access control policy.</p> <ul style="list-style-type: none"> <li>If the DestinationType parameter is set to net, this parameter specifies the destination CIDR block. Example: 1.2.3.4/24</li> <li>If the DestinationType parameter is set to group, this parameter specifies the name of the destination address book. Example: db_group</li> <li>If the DestinationType parameter is set to domain, this parameter specifies the destination domain name. Example: *.aliyuncs.com</li> <li>If the DestinationType parameter is set to location, this parameter specifies the destination region. For more information about region codes, see the following section. Example: ["BJ11", "ZB"]</li> </ul>
DestinationType	String	Yes		<p>The type of the destination address defined in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>net: destination CIDR block</li> <li>group: destination address book</li> <li>domain: destination domain name</li> <li>location: destination region</li> </ul>
Direction	String	Yes		<p>The traffic direction defined in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>in: inbound traffic</li> <li>out: outbound traffic</li> </ul>
Proto	String	Yes		<p>The security protocol type defined in the access control policy. If you cannot determine the protocol type, you can set this parameter to ANY. Valid values:</p> <ul style="list-style-type: none"> <li>ANY</li> <li>TCP</li> <li>UDP</li> <li>ICMP</li> </ul>

Parameter	Type	Required	Example	Description
Source	String	Yes		<p>The source address defined in the access control policy.</p> <ul style="list-style-type: none"> <li>If the SourceType parameter is set to net, this parameter specifies the source CIDR block. Example: 1.2.3.0/24</li> <li>If the SourceType parameter is set to group, this parameter specifies the name of the source address book. Example: db_group</li> <li>If the SourceType parameter is set to location, this parameter specifies the source region. For more information about region codes, see the following section. Example: ["BJ11", "ZB"]</li> </ul>
SourceType	String	Yes		<p>The source address type defined in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>net: source CIDR block</li> <li>group: source address book</li> <li>location: source region</li> </ul>
DestPort	String	No		<p>The destination port defined in the access control policy.</p>
DestPortGroup	String	No		<p>The name of the destination port address book defined in the access control policy.</p>
DestPortType	String	No		<p>The type of the destination port defined in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>port: port</li> <li>group: port address book</li> </ul>
Lang	String	No		<p>The language of the request and response. Valid values:</p> <ul style="list-style-type: none"> <li>en: English</li> <li>zh: Chinese</li> </ul>



Parameter	Type	Required	Example	Description
SourceIp	String	No		The source IP address of the request.

## Response parameters

Parameter	Type	Example	Description
RequestId	String		The ID of the request.

## Examples

### Sample requests

```

http(s)://[Endpoint]/? Action=ModifyControlPolicy
&AclAction=accept
&AclUuid=00281255-d220-4db1-8f4f-c4df221ad84c
&ApplicationName=ANY
&Description=demo_rule_1
&Destination=1.2.3.4/24
&DestinationType=net
&Direction=in
&Proto=TCP
&Source=1.2.3.0/24
&SourceType=net
&<Common request parameters>

```

### Sample success responses

#### XML format

```

<ModifyControlPolicy>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ModifyControlPolicy>

```

#### JSON format

```

{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}

```

## Error codes

For a list of error codes, visit the [API Error Center](#).

# 4.8. Strict mode

## 4.8.1. DescribePolicyAdvancedConfig

Queries whether the strict mode is enabled for an access control 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
Action	String	Yes	DescribePolicyAdvancedConfig	The operation that you want to perform. Set the value to <b>DescribePolicyAdvancedConfig</b> .
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>

### Response parameters

Parameter	Type	Example	Description
InternetSwitch	String	off	Indicates whether the strict mode is enabled for the access control policy. Valid values: <ul style="list-style-type: none"> <li>on: The strict mode is enabled.</li> <li>off: The strict mode is disabled.</li> </ul>

Parameter	Type	Example	Description
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125EEB1	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribePolicyAdvancedConfig
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribePolicyAdvancedConfigResponse>
<RequestId>850A84D6-0DE4-4797-A1E8-00090125EEB1</RequestId>
<InternetSwitch>off</InternetSwitch>
</DescribePolicyAdvancedConfigResponse>
```

#### JSON format

```
{
  "RequestId": "850A84D6-0DE4-4797-A1E8-00090125EEB1",
  "InternetSwitch": "off"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 4.8.2. ModifyPolicyAdvancedConfig

Controls whether to enable the strict mode for an access control 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
Action	String	Yes	ModifyPolicyAdvancedConfig	The operation that you want to perform. Set the value to <b>ModifyPolicyAdvancedConfig</b> .
InternetSwitch	String	Yes	off	Specifies whether to enable the strict mode for the access control policy. Valid values: <ul style="list-style-type: none"> <li>on: Enable the strict mode.</li> <li>off: Disable the strict mode.</li> </ul>
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>

### Response parameters

Parameter	Type	Example	Description
RequestId	String	B2841452-CB8D-4F7D-B247-38E1CF7334F8	The ID of the request.

### Examples

#### Sample requests

```
http(s)://[Endpoint]/? Action=ModifyPolicyAdvancedConfig
&InternetSwitch=off
&<Common request parameters>
```

#### Sample success responses

XML format

```
<ModifyPolicyAdvancedConfigResponse>
<RequestId>B2841452-CB8D-4F7D-B247-38E1CF7334F8</RequestId>
</ModifyPolicyAdvancedConfigResponse>
```

**JSON format**

```
{
  "RequestId": "B2841452-CB8D-4F7D-B247-38E1CF7334F8"
}
```


**Error codes**

For a list of error codes, visit the [API Error Center](#).

## 4.9. VPC firewalls

### 4.9.1. CreateVpcFirewallControlPolicy

Adds an access control policy to a specific policy group for a Virtual Private Cloud (VPC) firewall.

 **Note** You must create different access control policies for a VPC firewall used to protect Cloud Enterprise Network (CEN) and a VPC firewall used to protect Express Connect.


**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	CreateVpcFirewallControlPolicy	The operation that you want to perform. Set the value to <b>CreateVpcFirewallControlPolicy</b> .
AclAction	String	Yes	accept	The action that Cloud Firewall performs on the traffic. Valid values: <ul style="list-style-type: none"> <li><b>accept</b>: allows the traffic.</li> <li><b>drop</b>: denies the traffic.</li> <li><b>log</b>: monitors the traffic.</li> </ul>

Parameter	Type	Required	Example	Description
ApplicationName	String	Yes	HTTP	<p>The application type that the access control policy supports. Valid values:</p> <ul style="list-style-type: none"> <li>• FTP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• MySQL</li> <li>• SMTP</li> <li>• SMTPS</li> <li>• RDP</li> <li>• VNC</li> <li>• SSH</li> <li>• Redis</li> <li>• MQTT</li> <li>• MongoDB</li> <li>• Memcache</li> <li>• SSL</li> <li>• ANY: indicates that all application types are supported.</li> </ul>
Description	String	Yes	test	The description of the access control policy.
Destination	String	Yes	10.2.3.0/24	<p>The destination address in the access control policy.</p> <p>Set this parameter in the following way:</p> <ul style="list-style-type: none"> <li>• If the <b>DestinationType</b> parameter is set to <code>net</code>, set the value to a Classless Inter-Domain Routing (CIDR) block. Example: 10.2.3.0/24.</li> <li>• If the <b>DestinationType</b> parameter is set to <code>group</code>, set the value to the name of an address book. Example: db_group.</li> <li>• If the <b>DestinationType</b> parameter is set to <code>domain</code>, set the value to a domain name. Example: *.aliyuncs.com.</li> </ul>

Parameter	Type	Required	Example	Description
DestinationType	String	Yes	net	<p>The type of the destination address in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>net</b>: CIDR block</li> <li>• <b>group</b>: address book</li> <li>• <b>domain</b>: domain name</li> </ul>
NewOrder	String	Yes	-1	<p>The priority of the access control policy.</p> <p>The priority value starts from 1. A smaller priority value indicates a higher priority.</p> <div style="background-color: #e0f2f1; padding: 5px; border: 1px solid #ccc;"> <p> <b>Note</b> The value of -1 indicates the lowest priority.</p> </div>
Proto	String	Yes	TCP	<p>The security protocol in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>ANY</b>: indicates that all protocols are supported.</li> <li>• <b>TCP</b></li> <li>• <b>UDP</b></li> <li>• <b>ICMP</b></li> </ul>
Source	String	Yes	10.2.3.0/24	<p>The source address in the access control policy.</p> <ul style="list-style-type: none"> <li>• If the <b>SourceType</b> parameter is set to <b>net</b>, set the value to a CIDR block. Example: 10.2.3.0/24.</li> <li>• If the <b>SourceType</b> parameter is set to <b>group</b>, set the value to the name of an address book. Example: db_group.</li> </ul>
SourceType	String	Yes	net	<p>The type of the source address in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>net</b>: CIDR block</li> <li>• <b>group</b>: address book</li> </ul>

Parameter	Type	Required	Example	Description
VpcFirewallId	String	Yes	vfw-a42bbb7b887148c9****	<p>The ID of the policy group to which you want to add the access control policy.</p> <ul style="list-style-type: none"> <li>If the VPC firewall is used to protect CEN, set the value to the ID of the CEN instance that the VPC firewall protects. Example: cen-ervw5jbw1234****.</li> <li>If the VPC firewall is used to protect Express Connect, set the value to the ID of the VPC firewall instance. Example: vfw-a42bbb748c91234****.</li> </ul> <div style="background-color: #e1f5fe; padding: 5px; border: 1px solid #cfcfcf;"> <p> <b>Note</b> You can call the <a href="#">DescribeVpcFirewallAclGroupList</a> operation to query the ID of the policy group.</p> </div>
Lang	String	No	zh	<p>The natural language of the request and response. Valid values:</p> <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>
DestPort	String	No	80	<p>The destination port in the access control policy.</p> <div style="background-color: #e1f5fe; padding: 5px; border: 1px solid #cfcfcf;"> <p> <b>Note</b> This parameter must be specified if the DestPortType parameter is set to port .</p> </div>
DestPortType	String	No	net	<p>The type of the destination port in the access control policy. Valid values:</p> <ul style="list-style-type: none"> <li>port: port</li> <li>group: address book</li> </ul>



Parameter	Type	Required	Example	Description
DestPortGroup	String	No	my_port_group	<p>The address book of destination ports in the access control policy.</p> <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;"> <p> <b>Note</b> This parameter must be specified if the <b>DestPortType</b> parameter is set to <code>group</code> .</p> </div>

## Response parameters

Parameter	Type	Example	Description
AclUuid	String	00281255-d220-4db1-8f4f-c4df221ad84c	The unique ID of the access control policy.
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	The ID of the request.

## Examples

### Sample requests

```

http(s)://[Endpoint]/?Action=CreateVpcFirewallControlPolicy
&VpcFirewallId=vfw-a42bbb7b887148c9****
&AclAction=accept
&ApplicationName=ANY
&Description=demo_rule_1
&Destination=10.2.3.0/24
&DestinationType=net
&NewOrder=-1
&Proto=TCP
&Source=10.2.3.0/24
&SourceType=net
&<Common request parameters>

```

### Sample success responses

`XML` format

```
<CreateVpcFirewallControlPolicyResponse>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
<AclUuid>00281255-d220-4db1-8f4f-c4d*****</AclUuid>
</CreateVpcFirewallControlPolicyResponse>
```

#### JSON format


```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "AclUuid": "00281255-d220-4db1-8f4f-c4d*****"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 4.9.2. DescribeVpcFirewallControlPolicy

Queries the information about the access control policies that meet specific query conditions for a specific VPC firewall.

 **Note** The VPC firewall instance used to protect each Cloud Enterprise Network (CEN) and the VPC firewall instance used to protect each Express Connect use different access control 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
Action	String	Yes	DescribeVpcFirewallControlPolicy	The operation that you want to perform. Set the value to <code>DescribeVpcFirewallControlPolicy</code> .
CurrentPage	String	Yes	1	The number of the page to return. Default value: 1.

Parameter	Type	Required	Example	Description
PageSize	String	Yes	10	The number of entries to return on each page. Maximum value: 50.
VpcFirewallId	String	Yes	vfw-a42bbb7b887148c9****	The ID of the access control policy group that you want to query. You can call the <code>DescribeVpcFirewallAclGroupList</code> operation to obtain the ID. Valid values: <ul style="list-style-type: none"> <li>If the VPC firewall is used to protect a CEN, the ID of the CEN instance is used. Example: cen-ervw0g12b5jw****</li> <li>If the VPC firewall is used to protect an Express Connect, the ID of the VPC firewall instance is used. Example: vfw-a42bbb7b887148c9****</li> </ul>
Lang	String	No	zh	The natural language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>

Parameter	Type	Required	Example	Description
Source	String	No	10.0.1.0/24	<p>The source address in the access control policy. Fuzzy match is supported.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>If <code>SourceType</code> is set to <code>net</code>, the value of this parameter is a CIDR block. Example: 10.0.1.0/24</li> <li>If <code>SourceType</code> is set to <code>group</code>, the value of this parameter is an address book. Example: db_group</li> <li>If <code>SourceType</code> is not specified, all the sources are queried.</li> </ul> <p> <b>Note</b> The valid values of this parameter depend on the value of the <code>SourceType</code> parameter.</p>

Parameter	Type	Required	Example	Description
Destination	String	No	10.0.3.0	<p>The destination address in the access control policy. Fuzzy match is supported.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>If <code>DestinationType</code> is set to <code>net</code>, the value of this parameter is a CIDR block. Example: 10.0.3.0/24</li> <li>If <code>DestinationType</code> is set to <code>domain</code>, the value of this parameter is a domain name. Example: aliyun.com</li> <li>If <code>DestinationType</code> is set to <code>group</code>, the value of this parameter is an address book. Example: db_group</li> <li>If <code>DestinationType</code> is not specified, all destination addresses are queried.</li> </ul> <p><b>Note</b> The valid values of this parameter depend on the value of the <code>DestinationType</code> parameter.</p>
Description	String	No	test	<p>The description of the access control policy. Fuzzy match is supported.</p> <p><b>Note</b> If this parameter is not specified, the descriptions of all access control policies are queried.</p>

Parameter	Type	Required	Example	Description
Proto	String	No	TCP	<p>The protocol type in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> <li>• If this parameter is not specified, all protocol types are queried.</li> <li>• If this parameter is set to <b>ANY</b>, all protocol types are queried.</li> </ul>
AclAction	String	No	accept	<p>The action that Cloud Firewall performs on the traffic.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• <b>accept</b>: allows the traffic.</li> <li>• <b>drop</b>: denies the traffic.</li> <li>• <b>log</b>: monitors the traffic.</li> <li>• If this parameter is not specified, all access control policies are queried.</li> </ul>


## Response parameters

Parameter	Type	Example	Description
Policys	Array		The information about the access control policies.
AclAction	String	accept	<p>The action that Cloud Firewall performs on the traffic.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• <b>accept</b>: allows the traffic.</li> <li>• <b>drop</b>: denies the traffic.</li> <li>• <b>log</b>: monitors the traffic.</li> </ul>
AclUuid	String	00281255-d220-4db1-8f4f-c4df221a****	The unique ID of the access control policy.
ApplicationId	String	10**	The application ID in the access control policy.

Parameter	Type	Example	Description
ApplicationName	String	HTTP	<p>The application type that the access control policy supports.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> <li>• MySQL</li> <li>• SMTP</li> <li>• SMTPS</li> <li>• RDP</li> <li>• VNC</li> <li>• SSH</li> <li>• Redis</li> <li>• MQTT</li> <li>• MongoDB</li> <li>• Memcache</li> <li>• SSL</li> <li>• ANY (indicates that all application types are supported)</li> </ul>
Description	String	test	The description of the access control policy.
DestPort	String	80	The destination port in the access control policy.
DestPortGroup	String	my_port_group	The destination port address book in the access control policy.
DestPortGroupPorts	List	[80,443]	The ports in the destination port address book.
DestPortType	String	port	<p>The destination port type in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• port: port</li> <li>• group: port address book</li> </ul>

Parameter	Type	Example	Description
Destination	String	10.0.3.0/24	<p>The destination address in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>If <b>DestinationType</b> is set to <code>net</code>, the value of this parameter is a CIDR block. Example: 10.0.3.0/24</li> <li>If <b>DestinationType</b> is set to <code>domain</code>, the value of this parameter is a domain name. Example: aliyuncs.com</li> <li>If <b>DestinationType</b> is set to <code>group</code>, the value of this parameter is an address book. Example: db_group</li> </ul> <p><b>Note</b> The valid values of this parameter depend on the value of the <b>DestinationType</b> parameter.</p>
DestinationGroupCidrs	List	["10.0.4.0/24", "10.0.0.1/32"]	The CIDR blocks in the destination address book of the access control policy.
DestinationType	String	net	<p>The destination address type in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>net</b>: CIDR block</li> <li><b>group</b>: address book</li> <li><b>domain</b>: domain name</li> </ul>
Direction	String	in	<p>The direction of traffic to which the access control policy applies.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li><b>in</b>: inbound traffic</li> <li><b>out</b>: outbound traffic</li> </ul>
HitTimes	Integer	100	The number of hits for the access control policy.



Parameter	Type	Example	Description
Order	Integer	1	<p>The priority of the access control policy.</p> <p>The priority value starts from 1. A smaller priority value indicates a higher priority. The value -1 indicates the lowest priority.</p>
Proto	String	TCP	<p>The protocol type in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> <li>• ANY (All protocol types are queried.)</li> </ul>
Source	String	10.0.6.0/24	<p>The source address in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• If <code>SourceType</code> is set to <code>net</code>, the value of this parameter is a CIDR block. Example: 10.0.6.0/24</li> <li>• If <code>SourceType</code> is set to <code>group</code>, the value of this parameter is an address book. Example: db_group</li> </ul> <div style="background-color: #e0f2f1; padding: 5px; border: 1px solid #ccc;"> <p> <b>Note</b> The valid values of this parameter depend on the value of the <code>SourceType</code> parameter.</p> </div>
SourceGroupCidrs	List	["10.0.6.0/24", "10.0.0.2/32"]	The CIDR blocks in the source address book of the access control policy.
SourceType	String	net	<p>The source address type in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• <code>net</code>: CIDR block</li> <li>• <code>group</code>: address book</li> </ul>

Parameter	Type	Example	Description
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	The ID of the request.
TotalCount	String	20	The total number of access control policies that meet the query conditions.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeVpcFirewallControlPolicy
&VpcFirewallId=vfw-a42bbb7b887148c9****
&CurrentPage=1
&PageSize=10
&<Common request parameters>
```

### Sample success responses

`XML` format

```
<DescribeVpcFirewallControlPolicyResponse>
<TotalCount>1</TotalCount>
<PageNo>1</PageNo>
<PageSize>10</PageSize>
<RequestId>A08BC58F-A83D-43EB-BC31-2F0D723929CC</RequestId>
<Policies>
<ApplicationName>HTTP</ApplicationName>
<Description>11</Description>
<HitTimes>0</HitTimes>
<DestinationType>net</DestinationType>
<SourceType>net</SourceType>
<Proto>TCP</Proto>
<Order>5</Order>
<ApplicationId>27</ApplicationId>
<DestPortType>port</DestPortType>
<Source>10.1.1.1/32</Source>
<DestPort>80/80</DestPort>
<AclAction>accept</AclAction>
<AclUuid>53d82f0e-9bf1-4761-ab3b-a070b4811234</AclUuid>
<Destination>10.2.1.1/32</Destination>
</Policies>
</DescribeVpcFirewallControlPolicyResponse>
```

JSON format

```
{
  "TotalCount":1,
  "PageNo":1,
  "PageSize":10,
  "RequestId":"A08BC58F-A83D-43EB-BC31-2F0D723929CC",
  "Policies":[
    {
      "DestinationGroupCidrs":[

      ],
      "SourceGroupCidrs":[

      ],
      "ApplicationName":"HTTP",
      "Description":"11",
      "HitTimes":0,
      "DestinationType":"net",
      "SourceType":"net",
      "Proto":"TCP",
      "Order":5,
      "ApplicationId":"27",
      "DestPortType":"port",
      "Source":"10.1.1.1/32",
      "DestPort":"80/80",
      "AclAction":"accept",
      "DestPortGroupPorts":[


      ],
      "AclUuid":"53d82f0e-9bf1-4761-ab3b-a070b4811234",
      "Destination":"10.2.1.1/32"
    }
  ]
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

### 4.9.3. ModifyVpcFirewallControlPolicy

Modifies the configuration of an access control policy in a specific policy group for a VPC firewall.

 **Note** The VPC firewall instance used to protect each Cloud Enterprise Network (CEN) and the VPC firewall instance used to protect each Express Connect use different access control 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
Action	String	Yes	ModifyVpcFirewallControlPolicy	The operation that you want to perform. Set the value to <b>ModifyVpcFirewallControlPolicy</b> .
AclAction	String	Yes	accept	The action that Cloud Firewall performs on the traffic. Valid values: <ul style="list-style-type: none"> <li><b>accept</b>: allows the traffic.</li> <li><b>drop</b>: denies the traffic.</li> <li><b>log</b>: monitors the traffic.</li> </ul>
AclUuid	String	Yes	00281255-d220-4db1-8f4f-c4df221ad84c	The unique ID of the access control policy. If you want to modify an access control policy, you must provide the ID of the policy. You can call the <b>DescribeVpcFirewallControlPolicy</b> operation to obtain the ID.

Parameter	Type	Required	Example	Description
ApplicationName	String	Yes	HTTP	<p>The application type that the access control policy supports.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• ANY (indicates that all application types are supported)</li> <li>• FTP</li> <li>• HTTP</li> <li>• HTTPS</li> <li>• MySQL</li> <li>• SMTP</li> <li>• SMTPS</li> <li>• RDP</li> <li>• VNC</li> <li>• SSH</li> <li>• Redis</li> <li>• MQTT</li> <li>• MongoDB</li> <li>• Memcache</li> <li>• SSL</li> </ul>
Description	String	Yes	test	The description of the access control policy.
Destination	String	Yes	10.2.3.0/24	<p>The destination address in the access control policy.</p> <ul style="list-style-type: none"> <li>• If DestinationType is set to <code>net</code>, the value of this parameter is a CIDR block. Example: 10.2.3.0/24</li> <li>• If DestinationType is set to <code>group</code>, the value of this parameter is an address book. Example: db_group</li> <li>• If DestinationType is set to <code>domain</code>, the value of this parameter is a domain name. Example: *.aliyuncs.com</li> </ul>

Parameter	Type	Required	Example	Description
DestinationType	String	Yes	net	<p>The type of the destination address in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• <b>net</b>: CIDR block</li> <li>• <b>group</b>: address book</li> <li>• <b>domain</b>: domain name</li> </ul>
Proto	String	Yes	TCP	<p>The type of the security protocol in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• <b>ANY</b> (indicates all protocol types)</li> <li>• <b>TCP</b></li> <li>• <b>UDP</b></li> <li>• <b>ICMP</b></li> </ul>
Source	String	Yes	10.2.4.0/24	<p>The source address in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• If <b>SourceType</b> is set to <b>net</b>, the value of this parameter is a CIDR block. Example: 10.2.4.0/24</li> <li>• If <b>SourceType</b> is set to <b>group</b>, the value of this parameter is an address book. Example: db_group</li> </ul>
SourceType	String	Yes	net	<p>The type of the source address in the access control policy.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• <b>net</b>: CIDR block</li> <li>• <b>group</b>: address book</li> </ul>

Parameter	Type	Required	Example	Description
VpcFirewallId	String	Yes	vfw-a42bbb7b887148c9****	<p>The ID of the access control policy group. You can call the DescribeVpcFirewallAclGroupList operation to obtain the ID.</p> <ul style="list-style-type: none"> <li>If the VPC firewall is used to protect a CEN, the ID of the CEN instance is used. Example: cen-ervw0g12b5jbw****</li> <li>If the VPC firewall is used to protect an Express Connect, the ID of the VPC firewall instance is used. Example: vfw-a42bbb7b887148c9****</li> </ul>
Lang	String	No	zh	<p>The natural language of the request and response. Valid values:</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>
DestPort	String	No	80	The destination port in the access control policy.
DestPortType	String	No	port	<p>The type of the destination port in the access control policy.</p> <ul style="list-style-type: none"> <li>port: port</li> <li>group :port address book</li> </ul>
DestPortGroup	String	No	my_port_group	The destination port address book in the access control policy.

### Response parameters

Parameter	Type	Example	Description
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	The ID of the request.

### Examples

#### Sample requests



```
http(s)://[Endpoint]/? Action=ModifyVpcFirewallControlPolicy
&VpcFirewallId=vfw-a42bbb7b887148c9****
&AclAction=accept
&AclUuid=00281255-d220-4db1-8f4f-c4df221ad84c
&ApplicationName=ANY
&Description=demo_rule_1
&Destination=10.2.3.0/24
&DestinationType=net
&Proto=TCP
&Source=10.2.4.0/24
&SourceType=net
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<ModifyVpcFirewallControlPolicyResponse>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ModifyVpcFirewallControlPolicyResponse>
```

#### JSON format

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 4.9.4. ModifyVpcFirewallControlPolicyPosition

Modifies the priority of an access control policy in a specific policy group for a VPC firewall.

### 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	ModifyVpcFirewallControlPolicyPosition	The operation that you want to perform. Set the value to <b>ModifyVpcFirewallControlPolicyPosition</b> .
NewOrder	String	Yes	1	The new priority of the access control policy.
OldOrder	String	Yes	5	The original priority of the access control policy.
VpcFirewallId	String	Yes	vfw-a42bbb7b887148c9****	The ID of the access control policy group. You can call the DescribeVpcFirewallAclGroupList operation to obtain the ID.  Valid values: <ul style="list-style-type: none"> <li>If the VPC firewall is used to protect a Cloud Enterprise Network (CEN), the ID of the CEN instance is used. Example: cen-ervw0g12b5jbw****</li> <li>If the VPC firewall is used to protect an Express Connect, the ID of the VPC firewall instance is used. Example: vfw-a42bbb7b887148c9****</li> </ul>
Lang	String	No	zh	The natural language of the request and response. Valid values:  Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	850A84D6-0DE4-4797-A1E8-00090125EEB1	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=ModifyVpcFirewallControlPolicyPosition
&VpcFirewallId=vfw-a42bbb7b887148c9****
&NewOrder=1
&OldOrder=5
&<Common request parameters>
```

### Sample success responses

XML format

```
<ModifyVpcFirewallControlPolicyPositionResponse>
<RequestId>850A84D6-0DE4-4797-A1E8-00090125EEB1</RequestId>
</ModifyVpcFirewallControlPolicyPositionResponse>
```

JSON format


```
{
  "RequestId": "850A84D6-0DE4-4797-A1E8-00090125EEB1"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 4.9.5. DeleteVpcFirewallControlPolicy

Deletes an access control policy from a specific policy group for a VPC firewall.

 **Note** The VPC firewall instance used to protect each Cloud Enterprise Network (CEN) and the VPC firewall instance used to protect each Express Connect use different access control 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
Action	String	Yes	DeleteVpcFirewallControlPolicy	The operation that you want to perform. Set the value to <b>DeleteVpcFirewallControlPolicy</b> .
AclUuid	String	Yes	00281255-d220-4db1-8f4f-c4df2214****	The unique ID of the access control policy. If you want to delete an access control policy, you must provide the ID of the policy. You can call the <b>DescribeVpcFirewallControlPolicy</b> operation to obtain the ID.
VpcFirewallId	String	Yes	vfw-a42bbb7b887148c91****	The ID of the access control policy group. You can call the <b>DescribeVpcFirewallAclGroupList</b> operation to obtain the ID.  Valid values: <ul style="list-style-type: none"> <li>If the VPC firewall is used to protect a CEN, the ID of the CEN instance is used. Example: cen-ervw0g12b5jbw****</li> <li>If the VPC firewall is used to protect an Express Connect, the ID of the VPC firewall instance is used. Example: vfw-a42bbb7b887148c9****</li> </ul>
Lang	String	No	zh	The natural language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	The ID of the request.

## Examples

## Sample requests

```
http(s)://[Endpoint]/? Action=DeleteVpcFirewallControlPolicy
&VpcFirewallId=vfw-a42bbb7b887148c9****
&AclUuid=00281255-d220-4db1-8f4f-c4df221ad84c
&<Common request parameters>
```

## Sample success responses

### XML format

```
<DeleteVpcFirewallControlPolicyResponse>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</DeleteVpcFirewallControlPolicyResponse>
```

### JSON format

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 4.9.6. DescribeVpcFirewallPolicyPriorUsed

Queries the priority range of access control policies in a specific policy group for a VPC firewall.

### 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	DescribeVpcFirewallPolicyPriorUsed	The operation that you want to perform. Set the value to <code>DescribeVpcFirewallPolicyPriorUsed</code> .

Parameter	Type	Required	Example	Description
VpcFirewallId	String	Yes	vfw-a42bbb7b887148c9****	<p>The ID of the access control policy group. You can call the DescribeVpcFirewallAclGroupList operation to obtain the ID.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>If the VPC firewall is used to protect a Cloud Enterprise Network (CEN), the ID of the CEN instance is used. Example: cen-ervw0g12b5jw****</li> <li>If the VPC firewall is used to protect an Express Connect, the ID of the VPC firewall instance is used. Example: vfw-a42bbb7b887148c9****</li> </ul>
Lang	String	No	zh	<p>The natural language of the request and response. Valid values:</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>

## Response parameters

Parameter	Type	Example	Description
End	Integer	150	The lowest priority for the access control policies in the policy group.
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	The ID of the request.
Start	Integer	1	The highest priority for the access control policies in the policy group.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeVpcFirewallPolicyPriorUsed
&VpcFirewallId=vfw-a42bbb7b887148c9****
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeVpcFirewallPolicyPriorUsedResponse>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
<Start>1</Start>
<End>150</End>
</DescribeVpcFirewallPolicyPriorUsedResponse>
```

JSON format

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D",
  "Start": 1,
  "End": 150
}
```

Error codes

For a list of error codes, visit the [API Error Center](#).

## 4.9.7. DescribeVpcFirewallAclGroupList

Queries information about access control policy groups for VPC firewalls.

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	DescribeVpcFirewallAclGroupList	The operation that you want to perform. Set the value to DescribeVpcFirewallAclGroupList.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The natural language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>
FirewallConfigureStatus	String	No	configured	Specifies whether VPC firewalls are configured. <ul style="list-style-type: none"> <li>notconfigured: VPC firewalls are not configured.</li> <li>configured: VPC firewalls are configured.</li> <li>If you do not specify this parameter, all access control policy groups are queried, regardless of whether VPC firewalls are configured.</li> </ul>
CurrentPage	String	No	1	The number of the page to return. Default value: 1.
PageSize	String	No	10	The number of entries to return on each page. Maximum value: 50.

## Response parameters

Parameter	Type	Example	Description
AclGroupList	Array		The information about access control policy groups for VPC firewalls.



Parameter	Type	Example	Description
AclGroupId	String	vfw-a42bbb7b887148c9****	<p>The ID of the access control policy group. You can call the <code>DescribeVpcFirewallAclGroupList</code> operation to obtain the ID.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>If the VPC firewall is used to protect a CEN, the ID of the CEN instance is returned. Example: cen-ervw0g12b5jbw****</li> <li>If the VPC firewall is used to protect an Express Connect, the ID of the VPC firewall instance is returned. Example: vfw-a42bbb7b887148c9****</li> </ul>
AclGroupName	String	group_test	<p>The name of the access control policy group.</p> <ul style="list-style-type: none"> <li>If the VPC firewall is used to protect a CEN, the name of the CEN instance is returned.</li> <li>If the VPC firewall is used to protect an Express Connect, the name of the VPC firewall is returned.</li> </ul>
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	The ID of the request.
TotalCount	Integer	1	The total number of the access control policy groups for the VPC firewalls.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeVpcFirewallAclGroupList
&FirewallConfigureStatus=configured
&<Common request parameters>
```

### Sample success responses

`XML` format

```
<DescribeVpcFirewallAclGroupListResponse>
<TotalCount>1</TotalCount>
<AclGroupList>
<AclGroupId>vfw-a42bbb7b887148c9****</AclGroupId>
<AclGroupName>group_test</AclGroupName>
</AclGroupList>
</DescribeVpcFirewallAclGroupListResponse>
```

#### JSON format

```
{"TotalCount":1,"AclGroupList":[{"AclGroupId":"vfw-a42bbb7b887148c9****","AclGroupName":"group_test"}]}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

## 4.9.8. ResetVpcFirewallRuleHitCount

Resets the count on hits of an access control policy in a specific policy group for a VPC firewall.

### 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	ResetVpcFirewallRuleHitCount	The operation that you want to perform. Set the value to <code>ResetVpcFirewallRuleHitCount</code> .
AclUuid	String	Yes	00281255-d220-4db1-8f4f-c4df221ad84c	The unique ID of the access control policy. If you want to delete an access control policy, you must provide the ID of the policy. You can call the <code>DescribeVpcFirewallControlPolicy</code> operation to obtain the ID.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The natural language of the request and response. Valid values:  Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=ResetVpcFirewallRuleHitCount
&AclUuid=00281255-d220-4db1-8f4f-c4df221a1234
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<ResetVpcFirewallRuleHitCountResponse>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ResetVpcFirewallRuleHitCountResponse>
```

#### JSON format

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

# 5.Firewall switch

## 5.1. PutEnableFwSwitch

You can call this operation to turn on a firewall switch.

### 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	PutEnableFwSwitch	The operation that you want to perform. Set the value to PutEnableFwSwitch.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>
IpaddrList.N	RepeatList	No	["1.2.3.4","5.6.7.8"]	The list of IP addresses.
RegionList.N	RepeatList	No	["cn-hangzhou","cn-shanghai"]	The list of regions.

Parameter	Type	Required	Example	Description
ResourceTypeList.N	RepeatList	No	["EcsPublicIp","NatEip"]	<p>The list of asset types.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>BastionHostIP: the IP address of a bastion host</li> <li>EcsEIP: the EIP of an ECS instance</li> <li>EcsPublicIP: the public IP address of an ECS instance</li> <li>EIP</li> <li>EniEIP: the EIP of an ENI</li> <li>NatEIP: the EIP of a NAT gateway</li> <li>SlbEIP: the EIP of an SLB instance</li> <li>SlbPublicIP: the public IP address of an SLB instance</li> <li>NatPublicIP: the public IP address of a NAT gateway</li> <li>HAVIP: the HA VIP</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	B2841452-CB8D-4F7D-B247-38E1CF7334F8	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=PutEnableFwSwitch&IpaddrList=["1.2.3.4","5.6.7.8"]
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<RequestId>B2841452-CB8D-4F7D-B247-38E1CF7334F8</RequestId>
```

#### JSON format

```
{
  "RequestId": "B2841452-CB8D-4F7D-B247-38E1CF7334F8"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

# 5.2. PutDisableFwSwitch

You can call this operation to turn off a firewall switch.

## 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	PutDisableFwSwitch	The operation that you want to perform. Set the value to PutDisableFwSwitch.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>
IpaddrList.N	RepeatList	No	["1.2.3.4","5.6.7.8"]	The list of IP addresses.
RegionList.N	RepeatList	No	["cn-hangzhou","cn-shanghai"]	The list of regions.

Parameter	Type	Required	Example	Description
ResourceTypeList.N	RepeatList	No	["EcsPublicIp","NatEip"]	<p>The list of asset types.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>BastionHostIP: the IP address of a bastion host</li> <li>EcsEIP: the EIP of an ECS instance</li> <li>EcsPublicIP: the public IP address of an ECS instance</li> <li>EIP</li> <li>EniEIP: the EIP of an ENI</li> <li>NatEIP: the EIP of a NAT gateway</li> <li>SlbEIP: the EIP of an SLB instance</li> <li>SlbPublicIP: the public IP address of an SLB instance</li> <li>NatPublicIP: the public IP address of a NAT gateway</li> <li>HAVIP: the HA VIP</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	B2841452-CB8D-4F7D-B247-38E1CF7334F8	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=PutDisableFwSwitch&IpaddrList=["1.2.3.4","5.6.7.8"]
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<RequestId>B2841452-CB8D-4F7D-B247-38E1CF7334F8</RequestId>
```

#### JSON format

```
{
  "RequestId": "B2841452-CB8D-4F7D-B247-38E1CF7334F8"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

# 5.3. PutEnableAllFwSwitch

You can call this operation to turn on all firewall switches.

## 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	PutEnableAllFwSwitch	The operation that you want to perform. Set the value to PutEnableAllFwSwitch.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: Chinese</li> <li>en: English</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String	B2841452-CB8D-4F7D-B247-38E1CF7334F8	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=PutEnableAllFwSwitch
&<Common request parameters>
```

### Sample success responses



**XML format**

```
<RequestId>B2841452-CB8D-4F7D-B247-38E1CF7334F8</RequestId>
```

**JSON format**

```
{  
  "RequestId": "B2841452-CB8D-4F7D-B247-38E1CF7334F8"  
}
```

**Error codes**

For a list of error codes, visit the [API Error Center](#).

## 5.4. PutDisableAllFwSwitch

You can call this operation to turn off all firewall switches.

**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	PutDisableAllFwSwitch	The operation that you want to perform. Set the value to PutDisableAllFwSwitch.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: <ul style="list-style-type: none"><li>zh: Chinese</li><li>en: English</li></ul>

**Response parameters**

Parameter	Type	Example	Description
RequestId	String	B2841452-CB8D-4F7D-B247-38E1CF7334F8	The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=PutDisableAllFwSwitch
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<RequestId>B2841452-CB8D-4F7D-B247-38E1CF7334F8</RequestId>
```

#### JSON format

```
{
  "RequestId": "B2841452-CB8D-4F7D-B247-38E1CF7334F8"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

# 6.Address books


## 6.1. AddAddressBook

### 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		The operation that you want to perform. Set the value to AddAddressBook.
Description	String	Yes		The description of the address book.
GroupName	String	Yes		The name of the address book.
GroupType	String	Yes		The type of the address book. Valid values: <ul style="list-style-type: none"><li>ip: IP address book</li><li>domain: domain address book</li><li>port: port address book</li><li>tag: ECS tag address book</li></ul>

Parameter	Type	Required	Example	Description
AddressList	String	No		<p>The addresses to specify in the address book. Separate multiple addresses with commas (,).</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 5px 0;"> <p> <b>Note</b> If the GroupType parameter is set to ip, port or domain, this parameter is required.</p> </div> <ul style="list-style-type: none"> <li>• If the GroupType parameter is set to ip, this parameter specifies the IP addresses. Example: 1.2.3.4/32, 1.2.3.0/24</li> <li>• If the GroupType parameter is set to port, this parameter specifies the ports or the port ranges. Example: 80, 100/200</li> <li>• If the GroupType parameter is set to domain, this parameter specifies the domain names. Example: demo1.aliyun.com, demo2.aliyun.com</li> </ul>
AutoAddTagEcs	String	No		<p>Specifies whether to automatically add ECS public IP addresses to the address book if they match the specified tags. Valid values:</p> <ul style="list-style-type: none"> <li>• 1: Yes</li> <li>• 0: No</li> </ul>
Lang	String	No		<p>The language of the request and response. Valid values:</p> <ul style="list-style-type: none"> <li>• en: English</li> <li>• zh: Chinese</li> </ul>
SourceIp	String	No		<p>The source IP address of the request.</p>
TagList.N.TagKey	String	No		<p>The key of the ECS tag.</p>
TagList.N.TagValue	String	No		<p>The value of the ECS tag.</p>

Parameter	Type	Required	Example	Description
TagRelation	String	No		<p>The logical relation among ECS tags. Valid values:</p> <ul style="list-style-type: none"> <li>• <b>and</b>: Only ECS public IP addresses that match all the specified tags are added to the address book.</li> <li>• <b>or</b>: ECS public IP addresses that match any of the specified tags are added to the address book.</li> </ul>

## Response parameters

Parameter	Type	Example	Description
GroupUuid	String		The unique ID of the address book returned.
RequestId	String		The ID of the request.

## Examples

### Sample requests

```

http(s)://[Endpoint]/? Action=AddAddressBook
&Description=DEMO address book
&GroupName=demo_address_book
&GroupType=ip
&AddressList=1.2.3.4/32,1.2.3.0/24
&<Common request parameters>

```

### Sample success responses

#### XML format

```

<AddAddressBook>
<RequestId>B2841452-CB8D-4F7D-B247-38E1CF7334F8</RequestId>
<GroupUuid>0580bbd0-24cd-47ae-9e5a-f5a099251e32</GroupUuid>
</AddAddressBook>

```

#### JSON format

```
{
  "RequestId": "B2841452-CB8D-4F7D-B247-38E1CF7334F8",
  "GroupUuid": "0580bbd0-24cd-47ae-9e5a-f5a099251e32"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

# 6.2. DeleteAddressBook

## 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		The operation that you want to perform. Set the value to DeleteAddressBook.
GroupUuid	String	Yes		The unique ID of the address book. You can call the DescribeAddressBook operation to query the ID.
Lang	String	No		The language of the request and response. Valid values: <ul style="list-style-type: none"> <li>zh: English</li> <li>zh: Chinese</li> </ul>
SourceIp	String	No		The source IP address of the request.

## Response parameters

Parameter	Type	Example	Description
RequestId	String		The ID of the request.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DeleteAddressBook
&GroupUuid=0657ab9d-fe8b-4174-b2a6-6baf358ea4ad
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DeleteAddressBook>
<RequestId>850A84D6-0DE4-4797-A1E8-00090125EEB1</RequestId>
</DeleteAddressBook>
```

#### JSON format

```
{
  "RequestId": "850A84D6-0DE4-4797-A1E8-00090125EEB1"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).


# 6.3. ModifyAddressBook

## 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		The operation that you want to perform. Set the value to ModifyAddressBook.
Description	String	Yes		The description of the address book.

Parameter	Type	Required	Example	Description
GroupName	String	Yes		The name of the address book.
GroupUuid	String	Yes		The unique ID of the address book. You can call the DescribeAddressBook operation to query the ID.
AddressList	String	No		<p>The addresses to be added to the address book. Separate multiple addresses with commas (,).</p> <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 5px 0;"> <p> <b>Note</b> If the GroupType parameter is set to ip, port, or domain, this parameter is required.</p> </div> <ul style="list-style-type: none"> <li>If the GroupType parameter is set to ip, this parameter specifies the IP addresses. Example: 1.2.3.4/32, 1.2.3.0/24</li> <li>If the GroupType parameter is set to port, this parameter specifies the ports or port ranges. Example: 80, 100/200</li> <li>If the GroupType parameter is set to domain, this parameter specifies the domain names. Example: demo1.aliyun.com, demo2.aliyun.com</li> </ul>
AutoAddTagEcs	String	No		<p>Specifies whether to automatically add ECS public IP addresses to the address book if they match the specified tags. Valid values:</p> <ul style="list-style-type: none"> <li>1: Yes</li> <li>0: No</li> </ul>
Lang	String	No		<p>The language of the request and response. Valid values:</p> <ul style="list-style-type: none"> <li>en: English</li> <li>zh: Chinese</li> </ul>



Parameter	Type	Required	Example	Description
SourceIp	String	No		The source IP address of the request.
TagList.N.TagKey	String	No		The key of the ECS tag.
TagList.N.TagValue	String	No		The value of the ECS tag.
TagRelation	String	No		<p>The logical relation among ECS tags. Valid values:</p> <ul style="list-style-type: none"> <li><b>and:</b> Only ECS public IP addresses that match all the specified tags are added to the address book.</li> <li><b>or:</b> ECS public IP addresses that match any of the specified tags are added to the address book.</li> </ul>

## Response parameters

Parameter	Type	Example	Description
RequestId	String		The ID of the request.

## Examples

### Sample requests

```

http(s)://[Endpoint]/? Action=ModifyAddressBook
&GroupUuid=0657ab9d-fe8b-4174-b2a6-6baf358ea4ad
&Description=DEMO address book
&GroupName=demo_address_book
&GroupType=ip
&AddressList=1.1.1/32,2.2.2.0/24
&<Common request parameters>

```

### Sample success responses

XML format

```
<ModifyAddressBook>
<RequestId>CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D</RequestId>
</ModifyAddressBook>
```

#### JSON format

```
{
  "RequestId": "CBF1E9B7-D6A0-4E9E-AD3E-2B47E6C2837D"
}
```

## Error codes

For a list of error codes, visit the [API Error Center](#).

# 6.4. DescribeAddressBook

## 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		The operation that you want to perform. Set the value to DescribeAddressBook.
ContainPort	String	No		The port that is contained in the address book. This parameter only takes effect when the GroupType parameter is set to port.
CurrentPage	String	No		The number of the page to return. Default value: 1.

Parameter	Type	Required	Example	Description
GroupType	String	No		The type of the address book. Valid values: <ul style="list-style-type: none"> <li>ip: IP address book</li> <li>domain: domain address book</li> <li>port: port address book</li> <li>tag: Elastic Compute Service (ECS) tag address book</li> </ul>
Lang	String	No		The language of the request and response. Valid values: <ul style="list-style-type: none"> <li>en: English</li> <li>zh: Chinese</li> </ul>
PageSize	String	No		The number of entries to return on each page. Maximum value: 50.
Query	String	No		The query condition that specifies the address book.
SourceIp	String	No		The source IP address of the request.

## Response parameters

Parameter	Type	Example	Description
Acls	Array		The information about the address book.
AddressList	List		The addresses in the address book.
AddressListCount	Integer		The number of addresses in the returned address book.
AutoAddTags	Integer		Indicates whether ECS public IP addresses that match the specified tags are automatically added to the address book. Valid values: <ul style="list-style-type: none"> <li>1: Yes</li> <li>0: No</li> </ul>

Parameter	Type	Example	Description
Description	String		The description of the address book.
Global	Integer		Indicates whether the address book is global. Valid values: <ul style="list-style-type: none"> <li>1: Yes</li> <li>0: No</li> </ul>
GroupName	String		The name of the address book.
GroupType	String		The type of the address book. Valid values: <ul style="list-style-type: none"> <li>ip: IP address book</li> <li>domain: domain address book</li> <li>port: port address book</li> <li>tag: ECS tag address book</li> </ul>
GroupUuid	String		The unique ID of the returned address book.
ReferenceCount	Integer		The number of times that the address book is referenced.
TagList	Array		The tags that are used to add matching ECS public IP addresses to the address book.
TagKey	String		The key of the ECS tag.
TagValue	String		The value of the ECS tag.
TagRelation	String		The logical relation among ECS tags. <ul style="list-style-type: none"> <li>and: Only ECS public IP addresses that match all the specified tags are added to the address book.</li> <li>or: ECS public IP addresses that match any of the specified tags are added to the address book.</li> </ul>
PageNo	String		The page number of the returned page.

Parameter	Type	Example	Description
PageSize	String		The number of entries returned on each page.
RequestId	String		The ID of the request.
TotalCount	String		The total number of address books.

## Examples

### Sample requests

```
http(s)://[Endpoint]/? Action=DescribeAddressBook
&<Common request parameters>
```

### Sample success responses

#### XML format

```
<DescribeAddressBook>
<TotalCount>123</TotalCount>
<PageSiNo>1</PageSiNo>
<PageSize>1</PageSize>
<RequestId>B36F150A-1E27-43AA-B72C-D2AC712F09DA</RequestId>
<Acls>
<Description>9-3 IP address book</Description>
<GroupType>ip</GroupType>
<AddressList>1.2.3.4/32</AddressList>
<AddressList>0.0.0.0/0</AddressList>
<GroupName>9-3 IP address book</GroupName>
<AutoAddTagEcs>0</AutoAddTagEcs>
<TagValue></TagValue>
<TagRelation></TagRelation>
<ReferenceCount>0</ReferenceCount>
<TagKey></TagKey>
<AddressListCount>2</AddressListCount>
<GroupUuid>a3c5e-018e-4c08-bea8-eafc95d1a54e</GroupUuid>
<Global>0</Global>
</Acls>
</DescribeAddressBook>
```

**JSON format**

```
{
  "TotalCount":123,
  "PageSize":1,
  "RequestId":"B36F150A-1E27-43AA-B72C-D2AC712F09DA",
  "Acls":[
    {
      "Description":"9-3 IP address book",
      "GroupType":"ip",
      "AddressList":[
        "1.2.3.4/32",
        "0.0.0.0/0"
      ],
      "GroupName":"9-3 IP address book",
      "AutoAddTagEcs":0,
      "TagValue":"",
      "TagRelation":"",
      "TagList":[],
      "ReferenceCount":0,
      "TagKey":"",
      "AddressListCount":2,
      "GroupUuid":"a3c5e-018e-4c08-bea8-eafc95d1a54e",
      "Global":0
    }
  ],
  "PageSiNo":1
}
```

**Error codes**

For a list of error codes, visit the [API Error Center](#).