Alibaba Cloud
Web应用防火墙

API Reference

Issue: 20200514

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

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

Document conventions

Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings** > **Network** > **Set network type**.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

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

Contents

1 Release notes

After the protection engine upgraded in Web Application Firewall, the API is completely updated. The version is upgraded to 2019-09-10, and the APIs and parameters are changed.

- If your Web Application Firewall instances are upgraded to the new protection engine version, see API references for new engine documents to call the API service.

  For more information about the new protection engine, see #unique_5.
- If you have not upgraded to the new protection engine and are still using the previous version of the API, see API references for legacy engine documents to call the API service.

  Note:
  You can log in the Web Application Firewall console, go to the **System Management** > **Product Information** page to check the protection engine version of your instance.

  - If the software version is earlier than 5.0.0.0 (for example, 4.5.1.1), the current instance is an legacy version.
  - If the software version number does not appear on the **Product Information** page, the instance is upgraded to the new version.

Compared with version 2018-01-17, this version has the following differences.

Note:
Changes have been made to both request and response parameters. For more information, see the related topics describing API operations.

API (2019-09-10)	API (2018-01-17)	Description
instance information		
DescribeInstanceInfo	DescribePayInfo	Queries the information of a WAF instance.
DescribeInstanceSpecInfo	None	New operation. Queries the specification of a WAF instance.

API (2019-09-10)	API (2018-01-17)	Description
None	DescribeRegions	Not supported. Version 2019-09-10 automatically recognizes the region based on the endpoint of the API operation.
None	DescribeWafSourceIpSegment	Not supported. We recommend that you view the back-to-origin CIDR block of a WAF instance in the WAF console.
Domain configurations		
CreateDomain	CreateDomainConfig	Specifies the information about a domain and adds the domain to a WAF instance.
DescribeDomain	DescribeDomainConfig	Updated. In the 2019-09-10 version, this operation obtains more information about domains added to a WAF instance.
ModifyDomain	ModifyDomainConfig	Modifies the configurations of a specific domain.
DeleteDomain	DeleteDomainConfig	Deletes the configuration of a specific domain.
DescribeDomainNames	DescribeDomainNames	Obtains a list of domains that are added to a WAF instance.
ModifyLogServiceStatus	None	New operation. Enables or disables log collection for the real-time log query and analysis feature of a specific domain.
ModifyLogRetrievalStatus	None	New operation. Enables or disables log retrieval for a specific domain.
DescribeDomainBasicConfigs	None	New operation. Queries the protection status in the domain configurations.

API (2019-09-10)	API (2018-01-17)	Description
DescribeDomainAdvanceConfigs	None	Obtains detailed configurations of a domain.
CreateCertificate	CreateCertAndKey	Uploads the certificate and private key of a protected domain.
CreateCertificateByCertificateId	None	New operation. Upload a certificate for the specified domain name based on the certificate ID.
DescribeCertMatchStatus	None	New operation. Checks whether the information about the uploaded certificate of a domain matches the private key.
DescribeCertificates	None	New operation. Queries the available certificate of a specific domain.
Protection configurations **Note:** Changes have been made to the overall design logic of API operations related to protection configurations. You can use common API operations to enable and disable protection modules, and manage configuration rules. The previous module-specific API operations are no longer supported.		
ModifyDomainIpv6Status	None	New operation. Enables or disables IPv6 protection for a specific domain.
DescribeProtectionModuleStatus	None	New operation. You can query the status of WAF protection modules, including Web intrusion prevention, data security, advanced protection, Bot management, and access control or throttling.

API (2019-09-10)	API (2018-01-17)	Description
ModifyProtectionModuleStatus	None	New operation. You can enable or disable the specified WAF feature, which includes the web intrusion prevention, data security, advanced protection, Bot management, and access control or throttling modules.
DescribeProtectionModuleMode	None	New operation. This can be used to query the protection features of WAF for a specified domain, including the regular expression engine, big data deep learning engine, HTTP flood protection, data risk control, and active defense. The current prevention mode.
ModifyProtectionModuleMode	None	New operation. You can call this operation to modify the configurations of rules in the following protection modules: WAF regular expression protection engine, big data deep learning engine, HTTP flood protection, data risk control, and active defense.
DescribeProtectionModuleRules	None	New operation. You can call this operation to query the configuration records of rules in a specific protection module, such as Web intrusion prevention, data security, Bot management, access control and throttling, and website whitelist.

API (2019-09-10)	API (2018-01-17)	Description
CreateProtectionModuleRule	None	New operation. You can call this operation to create configuration rules in a specified WAF protection module, including Web intrusion prevention, data security, advanced protection, Bot management, and access control and traffic throttling.
ModifyProtectionModuleRule	None	New operation. You can call this operation to modify the configuration rules in a specified WAF feature, including Web intrusion prevention, data security, advanced protection, Bot management, access control or throttling, and whitelist.
ModifyProtectionRuleStatus	ModifyProtectionRuleStatus	Updated. You can call this operation to enable or disable the WAF protection feature for a specified domain, including website tamper-proofing, legitimate crawlers, crawler threat intelligence, custom protection policies, and the whitelist of websites. The specified rule in the Ram user SDK.
DescribeDomainRuleGroup	None	New operation. Queries the ID of the protection rule group of the RegEx protection engine configured for a specific domain.

API (2019-09-10)	API (2018-01-17)	Description
SetDomainRuleGroup	None	New operation. Selects a protection rule group for the RegEx protection engine used by a specific domain. The system provides three default protection rule groups. You can also choose a custom rule group.
ModifyProtectionRuleCacheStatus	ModifyProtectionRule CacheStatus	Updates cached pages of a specific domain protected by tamper protection rules.

2 New engine

2.1 API overview

This topic describes the API operations provided by Web Application Firewall (WAF).

instance information

Name	Description
DescribeInstanceInfo	Queries the information of a WAF instance in a specific region.
DescribeInstanceSpecInfo	Queries the specification of a WAF instance in a specific region.

Domain configurations

Name	Description
DescribeDomain	Queries the configurations of a specific domain.
CreateDomain	You can call this operation to add a domain to WAF.
ModifyDomain	Modifies the configurations of a specific domain.
DeleteDomain	Removes a specified domain from a WAF instance.
DescribeDomainNames	Obtains a list of domains that have been added to a specific WAF instance.

Name	Description
ModifyLogServiceStatus	Enables or disables log collection in the real-time log analysis feature for a specific domain.
ModifyLogRetrievalStatus	Enables or disables log retrieval for a specific domain.
DescribeDomainBasicConfigs	Queries the protection settings in domain configuration records.
DescribeDomainAdvanceConfigs	Queries the details in the configuration records of domains added to WAF.
CreateCertificate	Uploads a certificate and a private key for a specific domain.
CreateCertificateByCertificateId	You can call this operation to upload a certificate for a specified domain name based on the certificate ID.
DescribeCertMatchStatus	Checks whether the certificate of a specified domain matches with the private key.
DescribeCertificates	Queries available SSL certificates associated with a specific domain.

Protection configurations

Name	Description
ModifyDomainIpv6Status	You can call this operation to enable or disable protection for a specified domain against malicious IPv6 traffic.
DescribeProtectionModuleStatus	You can call this operation to query the DescribeProtectionModuleStatus status of each protection module, including Web intrusion prevention, data security, advanced protection, Bot management, and access control or throttling.
ModifyProtectionModuleStatus	You can call this operation to enable or disable the protection of a specified WAF feature, such as Web intrusion prevention, data security, advanced protection, Bot management, and access control or throttling.

Name	Description
DescribeProtectionModuleMode	Queries the protection mode of a specified protection module, including the RegEx protection engine, big data deep learning engine, HTTP flood protection feature, data risk control feature, and positive security model.
ModifyProtectionModuleMode	Modifies the protection mode of a specific protection module, including the RegEx protection engine, big data deep learning engine, HTTP flood protection feature, data risk control feature, and positive security model.
DescribeProtectionModuleRules	You can call this operation to query the configuration records of DescribeProtectionModuleRules in a specific WAF feature, such as Web intrusion prevention, data security, Bot management, access control or throttling, and website whitelist.

Name	Description
CreateProtectionModuleRule	You can call this operation to create rules in a specified WAF feature, such as Web intrusion prevention, data security, Bot management, access control or throttling, and website whitelist.
ModifyProtectionModuleRule	You can call this operation to modify the ModifyProtectionModuleRules of a Web intrusion prevention service (WAF) feature, such as Web intrusion prevention, data security, advanced protection, anti-Bot, access control and throttling, and whitelist.
ModifyProtectionRuleStatus	Call the ModifyProtectionRuleStatus API to enable or disable the WAF protection features for the specified domain, including website tamper-proofing, legitimate crawler defense, crawler threat intelligence, custom protection policies, and website whitelist. The specified rule in the Ram user SDK.

Name	Description
DescribeDomainRuleGroup	Queries the ID of the rule group of the RegEx protection engine configured for a specified domain to implement web application protection.
SetDomainRuleGroup	Selects a default rule group or customizes a rule group for a specified domain to implement web application protection.
ModifyProtectionRuleCacheStatus	Updates cached pages of a specific domain protected by tamper protection rules.

2.2 Request method

To send a Web Application Firewall (WAF) API request, you must send an HTTP GET request to the WAF 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

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

The request syntax is as follows:

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

In the request:

- **Endpoint**: the endpoint of the WAF API varies with the region.
  - Mainland China: wafopenapi.cn-hangzhou.aliyuncs.com
  - Outside mainland China: wafopenapi.ap-southeast-1.aliyuncs.com
- **Action**: the operation that you want to perform. For example, to obtain a list of the domains added to WAF, you must set the Action parameter to **DescribeDomainNames**.
- **Version**: the version of the API to be used. The current WAF API version is 2019-09-10.
- **Parameters**: the request parameters for the operation. Separate multiple parameters with ampersands (&).

  Request parameters include both common parameters and operation-specific parameters. Common parameters include the API version and authentication information. For more information, see Common parameters.

The following example demonstrates how to call the **DescribeDomainNames** operation to obtain a list of the domains added to WAF.

Note:
To improve readability, the API request is displayed in the following format.

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Format=xml
&Version=2019-09-10
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
...
```

API authorization

To ensure the security of your account, we recommend that you call the WAF API as a RAM user. To call the WAF API as a RAM user, you must create an account for the RAM user and grant the account required permissions.

Signature method

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

WAF 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=
CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-
4e0ad82fd6cf
```

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

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2019-09-10
&SignatureVersion=1.0
```

Perform the following operations to calculate the signature:

1. Use the request parameters to compose a string-to-sign.

   ```
   GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeDomainNames&Region%3Dcn
   &InstanceId%3Dwaf_elasticity-cn-0xldbqtm005&Format%3DXML&SignatureMethod
   %3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&
   SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version
   %3D2019-09-10
   ```

2. Calculate the HMAC value of the string-to-sign.

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

   ```
   CT9X0VtwR86fNWSnsc6v8YGOjuE=
   ```

3. Add the signature to the request parameters:

   ```
   https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
   &Region=cn
   &InstanceId=waf_elasticity-cn-0xldbqtm005
   &TimeStamp=2016-02-23T12:46:24Z
   &Format=XML
   &AccessKeyId=testid
   &SignatureMethod=HMAC-SHA1
   &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
   &Version=2019-09-10
   &SignatureVersion=1.0
   ```

```
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

2.3 Common parameters

Common request parameters

Common request parameters must be included in all WAF API requests.

Table 2-1: Common request parameters

Parameter	Type	Require	Description
Format	String	Yes	The format in which to return the response. Valid values: • JSON (default) • XML
Version	String	No	The version number of the API, in the format of YYYY-MM-DD. Set this value to 2019-09-10
AccessKeyId	String	No	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	No	The signature string in the API request.
SignatureMethod	String	No	The encryption method of the signature string. Set the value to HMAC-SHA1
Timestamp	String	No	The UTC time when the request is signed. The timestamp follows the ISO8601 standard and is in the format of YYYY-MM-DDThh:mm:ssZ. For example, 20:00:00 on January 10, 2013 (UTC+8) is written as 2013-01-10T12:00:00Z.
SignatureVersion	String	No	The version of the signature encryption algorithm. Set the value to 1.0.
SignatureNonce	String	No	A unique, random number used to prevent replay attacks. You must use different numbers for multiple requests.
ResourceOwnerAccount	String	Yes	The account that owns the resource to be accessed by the current request.

Sample requests

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2019-09-10
&SignatureVersion=1.0
&Signature=Signature
```

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. Response data can be returned in either the JSON or XML format. You can specify the response format when you are making the request. The default response format is XML.

Every response returns a unique **RequestId** (request ID) regardless of whether the call is successful.

- XML format

```
<?xml xml version="1.0" encoding="utf-8"? >
   <!--Result Root Node-->
   <Operation Name+Response>
      <!-Return Request Tag-->
      <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
      <!-Return Result Data-->
   </Operation Name+Response>
```

- JSON format

```
{
   "RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
   /*Return Result Data*/
   }
```

2.4 Instance information

2.4.1 DescribeInstanceInfo

You can call this operation to query the information of the WAF instance in a specified region.

Note:

The InstanceId parameter is not required to call this operation.

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	Boolean	No	DescribeInstanceInfo	The operation that you want to perform. Set the value to **DescribeInstanceInfo**.
InstanceSource	String	Yes	waf-cloud	The source of the WAF instance. Default value: **waf-cloud**.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.
ResourceGroupId	String	Yes	rg-atstuj3rtoptyui	The ID of the resource group to which the WAF instance belongs. By default, no value is specified, which indicates that the WAF instance belongs to the default resource group.

Response parameters

Parameter	Type	Example	Description
InstanceInfo	Struct		The information of the WAF instance.

Parameter	Type	Example	Description
EndDate	Long	1512921600	The timestamp (in seconds) indicating when the WAF instance expires. **Note:** For a pay-as-you-go instance, the returned value indicates the time when the trial period ends.
InDebt	Integer	1	Indicates whether the WAF instance has overdue payments. Valid values: • **0**: The instance has overdue payments. • **1**: The instance does not have overdue payments and is working properly. **Note:** This parameter applies to pay-as-you-go instances only.
InstanceId	String	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.
PayType	Integer	2	The type of the WAF instance: • **0**: No WAF instance has been purchased or activated in this region. • **1**: A subscription instance. • **2**: A pay-as-you-go instance.
Region	String	cn	The region where the WAF instance is located. • **cn**: mainland China • **cn-hongkong**: areas outside mainland China

Parameter	Type	Example	Description
RemainDay	Integer	0	The number of days before the trial period of the WAF instance expires. **Note:** This parameter applies to trial pay-as-you-go instances only.
Status	Integer	0	Indicates whether the WAF instance has expired. Valid values: • **0**: The instance has expired. • **1**: The instance has not expired and is working properly. **Note:** This parameter applies to subscription WAF instances only.
SubscriptionType	String	PayAsYouGo	The billing method of the WAF instance. Valid values: • **Subscription**: indicates subscription. • **PayAsYouGo**: indicates a pay-as-you-go instance.
Trial	Integer	0	Indicates whether this is a trial instance. Valid value: • **0**: false • **1**: true **Note:** This parameter applies to pay-as-you-go instances only.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

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

Sample success responses

`XML` format

```
<InstanceInfo>
   <Status>0</Status>
   <EndDate>1512921600</EndDate>
   <Region>cn</Region>
   <InDebt>1</InDebt>
   <Trial>0</Trial>
   <InstanceId>waf_elasticity-cn-0xldbqtm005</InstanceId>
   <RemainDay>0</RemainDay>
   <PayType>2</PayType>
</InstanceInfo>
<RequestId>276D7566-31C9-4192-9DD1-51B10DAC29D2</RequestId>
```

`JSON` format

```
{
 "InstanceInfo":{
  "Status":0,
  "EndDate":1512921600,
  "Region":"cn",
  "InDebt":1,
  "Trial":0,
  "InstanceId":"waf_elasticity-cn-0xldbqtm005",
  "RemainDay":0,
  "PayType":2
 },
 "RequestId":"276D7566-31C9-4192-9DD1-51B10DAC29D2"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.4.2 DescribeInstanceSpecInfo

You can call this operation to query the specification information of the WAF instance.

Note:

To call this operation, you do not need to specify **InstanceId** parameters

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

Element	Type	Required	Example	Description
Action	String	Yes	DescribeInstanceSpecInfo	The operation that you want to perform. Valid values: **DescribeInstanceSpecInfo**.
InstanceId	String	No	waf-cn-v0h1nej****	The ID of the WAF instance.
ResourceGroupId	String	No	rg-atstuj3rtop****	The ID of the resource group to which the WAF instance belongs. By default, no value is specified, which indicates that the WAF instance belongs to the default resource group.

Response parameters

Element	Type	Sample response	Description
ExpireTime	Long	1512921600	The timestamp (in seconds) indicating when the WAF instance expires.  **Note:** For a pay-as-you-go instance, the value returned indicates the time when the trial period ends.
InstanceId	String	waf_elasticity-cn-0xldbqt****	The ID of the WAF instance.

Element	Type	Sample response	Description
InstanceSpecInfos	Array		The specification information of the WAF instance, starting with **Code** and **Value** returns instance specification information as an array. Where, **Code** instance type item **Value** indicates the corresponding value.

Element	Type	Sample response	Description
Code	String	113	A configuration parameter of the WAF instance. The following instance specifications are returned based on the WAF instance version (**Code**) related items in: • **100** indicates whether HTTPS service protection is supported. • **101**: indicates the daily business traffic threshold. • **102**: indicates the HTTP flood protection threshold. • **103**: indicates the total number of supported domain names. • **104**: indicates whether wildcard domain names are supported. • **105**: indicates the number of supported custom precise access control rules. • **106** indicates the number of origin IP addresses. • **107**: indicates whether off-premises data centers are supported. • **108**: indicates whether custom Web access control is supported. • **109**: indicates whether non-standard ports are supported. • **110**: indicates whether the malicious IP blocking function is supported. • **111**: indicates whether data risk control is supported. • **112**: indicates the number of data risk control records that can be configured. • **113**: indicates the number of top-level domain that can be protected. • **114**: indicates the normal service bandwidth threshold.
			• **115**: indicates the number of bound domain names. • **116**: indicates whether an ECS IP address of another Alibaba Cloud

Element	Type	Sample response	Description
Value	String	1	The value of the configuration parameter.  **Note:** Boolean (whether...) Values of: **true** (Indicating Yes) | **false**(No).
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Element	Type	Sample response	Description
Version	String	version_elastic_bill	The version of the WAF instance. Valid values: • **version_pro_china**: indicates mainland China premium edition. • **version_business_china**: indicates Enterprise Edition in mainland China. • **version_enterprise_china**: indicates the flagship edition in mainland China. • **version_exclusive_china**: indicates the virtual exclusive Cluster Edition in mainland China. • **version_pro**: indicates the overseas pro edition. • **version_business**: indicates Enterprise Edition in international regions. • **version_enterprise**: indicates the international Ultimate Edition. • **version_exclusive**: indicates the virtual exclusive Cluster Edition in regions outside China. • **version_elastic_bill**: indicates the pay-as-you-go edition. The preceding list contains all the versions of WAF instances that an account of Alibaba Cloud International site can create. If the returned version is not listed, check whether you are using an International site account.

Examples

Sample request

```
http(s)://[Endpoint]/? Action=DescribeInstanceSpecInfo
```

```
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeInstanceSpecInfoResponse>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>150</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>151</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>0</Value>
        <Code>152</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>153</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>110</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>154</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>111</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>155</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>5</Value>
        <Code>112</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>156</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>1</Value>
        <Code>113</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>157</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>50</Value>
        <Code>114</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>0</Value>
        <Code>158</Code>
```

```
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>0</Value>
        <Code>115</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>159</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>116</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>117</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>0,1,3</Value>
        <Code>118</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>119</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>12</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>13</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>14</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>3</Value>
        <Code>160</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>nextwaf</Value>
        <Code>161</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>100</Value>
        <Code>162</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>100</Value>
        <Code>163</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>120</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>200</Value>
        <Code>164</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>121</Code>
```

```
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>165</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>0</Value>
        <Code>122</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>IP,Session</Value>
        <Code>166</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>123</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>167</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>124</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>1</Value>
        <Code>168</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>300</Value>
        <Code>125</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>169</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>126</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>4</Value>
        <Code>127</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>80,8080</Value>
        <Code>128</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>443,8443</Value>
        <Code>129</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>170</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>171</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>50</Value>
        <Code>172</Code>
```

```
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>173</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>130</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>5</Value>
        <Code>174</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>131</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>500</Value>
        <Code>175</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>5</Value>
        <Code>132</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>176</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>IP,URL,Referer,User-Agent,Params,URLPath</Value>
        <Code>133</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>177</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>0</Value>
        <Code>134</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>178</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>135</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>179</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>0</Value>
        <Code>136</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>137</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>138</Code>
```

```
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>180</Value>
        <Code>139</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>3</Value>
        <Code>140</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>141</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>4</Value>
        <Code>142</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>143</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>100</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>0</Value>
        <Code>144</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>2000</Value>
        <Code>101</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>145</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>20000</Value>
        <Code>102</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>146</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>10</Value>
        <Code>103</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>147</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>104</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>148</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>20</Value>
        <Code>105</Code>
```

```
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>149</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>20</Value>
        <Code>106</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>107</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>true</Value>
        <Code>108</Code>
    </InstanceSpecInfos>
    <InstanceSpecInfos>
        <Value>false</Value>
        <Code>109</Code>
    </InstanceSpecInfos>
    <RequestId>362778D1-E8D4-445D-A71D-F5ED47356125</RequestId>
    <InstanceId>waf-cn-v0h1nej****</InstanceId>
    <Version>version_3</Version>
    <ExpireTime>1591977600000</ExpireTime>
</DescribeInstanceSpecInfoResponse>
```

JSON format

```
{
   "InstanceSpecInfos": [
      {
         "Value": "false",
         "Code": "150"
      },
      {
         "Value": "false",
         "Code": "151"
      },
      {
         "Value": "0",
         "Code": "152"
      },
      {
         "Value": "false",
         "Code": "153"
      },
      {
         "Value": "true",
         "Code": "110"
      },
      {
         "Value": "true",
         "Code": "154"
      },
      {
         "Value": "false",
         "Code": "111"
      },
      {
         "Value": "true",
         "Code": "155"
      },
```

```
    {
      "Value": "5",
      "Code": "112"
    },
    {
      "Value": "true",
      "Code": "156"
    },
    {
      "Value": "1",
      "Code": "113"
    },
    {
      "Value": "false",
      "Code": "157"
    },
    {
      "Value": "50",
      "Code": "114"
    },
    {
      "Value": "0",
      "Code": "158"
    },
    {
      "Value": "0",
      "Code": "115"
    },
    {
      "Value": "true",
      "Code": "159"
    },
    {
      "Value": "true",
      "Code": "116"
    },
    {
      "Value": "false",
      "Code": "117"
    },
    {
      "Value": "0,1,3",
      "Code": "118"
    },
    {
      "Value": "true",
      "Code": "119"
    },
    {
      "Value": "true",
      "Code": "12"
    },
    {
      "Value": "true",
      "Code": "13"
    },
    {
      "Value": "false",
      "Code": "14"
    },
    {
      "Value": "3",
      "Code": "160"
    },
```

```
    {
      "Value": "nextwaf",
      "Code": "161"
    },
    {
      "Value": "100",
      "Code": "162"
    },
    {
      "Value": "100",
      "Code": "163"
    },
    {
      "Value": "true",
      "Code": "120"
    },
    {
      "Value": "200",
      "Code": "164"
    },
    {
      "Value": "false",
      "Code": "121"
    },
    {
      "Value": "false",
      "Code": "165"
    },
    {
      "Value": "0",
      "Code": "122"
    },
    {
      "Value": "IP,Session",
      "Code": "166"
    },
    {
      "Value": "false",
      "Code": "123"
    },
    {
      "Value": "false",
      "Code": "167"
    },
    {
      "Value": "true",
      "Code": "124"
    },
    {
      "Value": "1",
      "Code": "168"
    },
    {
      "Value": "300",
      "Code": "125"
    },
    {
      "Value": "true",
      "Code": "169"
    },
    {
      "Value": "false",
      "Code": "126"
    },
```

```
    {
      "Value": "4",
      "Code": "127"
    },
    {
      "Value": "80,8080",
      "Code": "128"
    },
    {
      "Value": "443,8443",
      "Code": "129"
    },
    {
      "Value": "false",
      "Code": "170"
    },
    {
      "Value": "false",
      "Code": "171"
    },
    {
      "Value": "50",
      "Code": "172"
    },
    {
      "Value": "false",
      "Code": "173"
    },
    {
      "Value": "true",
      "Code": "130"
    },
    {
      "Value": "5",
      "Code": "174"
    },
    {
      "Value": "true",
      "Code": "131"
    },
    {
      "Value": "500",
      "Code": "175"
    },
    {
      "Value": "5",
      "Code": "132"
    },
    {
      "Value": "false",
      "Code": "176"
    },
    {
      "Value": "IP,URL,Referer,User-Agent,Params,URLPath",
      "Code": "133"
    },
    {
      "Value": "false",
      "Code": "177"
    },
    {
      "Value": "0",
      "Code": "134"
    },
```

```
    {
      "Value": "false",
      "Code": "178"
    },
    {
      "Value": "false",
      "Code": "135"
    },
    {
      "Value": "false",
      "Code": "179"
    },
    {
      "Value": "0",
      "Code": "136"
    },
    {
      "Value": "false",
      "Code": "137"
    },
    {
      "Value": "true",
      "Code": "138"
    },
    {
      "Value": "180",
      "Code": "139"
    },
    {
      "Value": "3",
      "Code": "140"
    },
    {
      "Value": "true",
      "Code": "141"
    },
    {
      "Value": "4",
      "Code": "142"
    },
    {
      "Value": "false",
      "Code": "143"
    },
    {
      "Value": "true",
      "Code": "100"
    },
    {
      "Value": "0",
      "Code": "144"
    },
    {
      "Value": "2000",
      "Code": "101"
    },
    {
      "Value": "true",
      "Code": "145"
    },
    {
      "Value": "20000",
      "Code": "102"
    },
```

```
      {
        "Value": "true",
        "Code": "146"
      },
      {
        "Value": "10",
        "Code": "103"
      },
      {
        "Value": "true",
        "Code": "147"
      },
      {
        "Value": "true",
        "Code": "104"
      },
      {
        "Value": "false",
        "Code": "148"
      },
      {
        "Value": "20",
        "Code": "105"
      },
      {
        "Value": "true",
        "Code": "149"
      },
      {
        "Value": "20",
        "Code": "106"
      },
      {
        "Value": "true",
        "Code": "107"
      },
      {
        "Value": "true",
        "Code": "108"
      },
      {
        "Value": "false",
        "Code": "109"
      }
    ],
    "RequestId": "362778D1-E8D4-445D-A71D-F5ED47356125",
    "InstanceId": "waf-cn-v0h1nej****",
    "Version": "version_3",
    "ExpireTime": "1591977600000"
}
```


Error codes.

For a list of error codes, visit the API Error Center.

2.5 Domain configurations

2.5.1 DescribeDomainNames

You can call this operation to obtain a list of domains that have been added to a specified WAF instance.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeDomainNames	The operation that you want to perform. Set the value to **DescribeDomainNames**.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	Yes	rg-atstuj3rtoptyui	The ID of the resource group to which the queried domain belongs in Resource Management. By default, no value is specified, indicating that the domain belongs to the default resource group.

Response parameters

Parameter	Type	Example	Description
DomainNames	List	["1.example.com","2.example.com","3.example.com"]	A list of domains that have been added to the WAF instance.

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=DescribeDomainNames
&InstanceId=waf_elasticity-cn-0xldbqtm005
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DomainNames>1.example.com</DomainNames>
<DomainNames>2.example.com</DomainNames>
<DomainNames>3.example.com</DomainNames>
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

`JSON` format

```
{
 "DomainNames":["1.example.com","2.example.com","3.example.com"],
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Errors

For a list of error codes, visit the API Error Center.

2.5.2 DescribeDomain

You can call this operation to query the configuration information of a specified domain.

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	Boolean	No	DescribeDomain	The operation that you want to perform. Set the value to **DescribeDomain**.
Domain	String	No	www.example.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Domain	Struct		The configuration information of the specified domain.
SourceIps	String	["1.1.1.1", "2.2.2.2"]	The IP address or domain of the origin server to which the specified domain points.

Parameter	Type	Example	Description
HttpToUserIp	Integer	0	Indicates whether the HTTP back-to-origin feature is enabled. If this feature is enabled, the WAF instance can use HTTP to forward HTTPS requests to the origin server. By default, port 80 is used to forward the requests to the origin server. Valid values: • **0**: disabled (default) • **1**: yes
HttpsRedirect	Integer	0	Indicates whether the WAF instance redirects HTTP requests as HTTPS requests. Valid values: • **0**: no (default) • **1**: yes
Http2Port	String	[443]	The HTTP 2.0 port.
HttpPort	String	[80]	The HTTP port. **Note:** If a value is specified for this parameter, the HTTP protocol is enabled.
LoadBalancing	Integer	0	The load balancing algorithm that is used when WAF forwards the requests to the origin. Valid values: • **0**: IP hash • **1**: Round robin
Cname	String	xxxxxx.yundunwaf3.com	The CNAME record assigned by the WAF instance to the specified domain.

Parameter	Type	Example	Description
IsAccessProduct	Integer	0	Indicates whether a layer-7 proxy, such as Anti-DDoS Pro or CDN, has been configured for the specified domain to filter the incoming traffic before forwarding the traffic to WAF. Valid values: • **0**: no • **1**: true
HttpsPort	String	[443]	The HTTPS port. **Note:** If a value is specified for this parameter, the HTTPS protocol is enabled.
Version	Long	0	The system data identifier that is used to control optimistic locking.
LogHeaders	String	[{"k":"wafmark","v":"test"}]	The key-value pair that is used to mark the traffic that flows through WAF to the domain. Set the parameter in this format: [{"k":"_key_","v":"_value_"}]. Set _key_ to a custom request header field. Set _value_ to a field value. **Note:** If a request header contains the specified field, WAF overwrites the original field value with the specified value.

Parameter	Type	Example	Description
ClusterType	Integer	0	The type of the WAF cluster. Valid values: • **0**: shared cluster (default) • **1**: exclusive cluster
Connection Time	Integer	5	The connection timeout for WAF exclusive clusters. Unit: seconds.
ReadTime	Integer	120	The read timeout of a WAF exclusive cluster. Unit: seconds.
WriteTime	Integer	120	The timeout period for a WAF exclusive cluster write connection. Unit: seconds.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=DescribeDomain
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&<Common request parameters>
```

Sample success responses

XML format

```
<Domain>
    <HttpPort>80</HttpPort>
    <HttpToUserIp>0</HttpToUserIp>
    <WriteTime>120</WriteTime>
    <IsAccessProduct>0</IsAccessProduct>
    <Http2Port>443</Http2Port>
    <Version>0</Version>
    <HttpsRedirect>0</HttpsRedirect>
    <SourceIps>1.1.1.1</SourceIps>
    <SourceIps>2.2.2.2</SourceIps>
    <ConnectionTime>5</ConnectionTime>
    <Cname>xxxxxx.yundunwaf3.com</Cname>
    <LoadBalancing>0</LoadBalancing>
    <HttpsPort>443</HttpsPort>
    <ReadTime>120</ReadTime>
</Domain>
```

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
  "Domain":{
    "HttpPort":[80],
    "HttpToUserIp":0,
    "WriteTime":120,
    "IsAccessProduct":0,
    "Http2Port":[443],
    "Version":0,
    "HttpsRedirect":0,
    "SourceIps":["1.1.1.1","2.2.2.2"],
    "ConnectionTime":5,
    "Cname":"xxxxxx.yundunwaf3.com",
    "LoadBalancing":0,
    "HttpsPort":[443],
    "ReadTime":120
  },
  "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.5.3 CreateDomain

You can call this operation to add a domain to WAF.

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	CreateDomain	The operation that you want to perform. Set the value to **CreateDomain**.
Domain	String	Yes	www.example.com	The domain that you want to add to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
IsAccessProduct	Integer	Yes	0	Specifies whether to configure a Layer-7 proxy, such as Anti-DDoS Pro or CDN, to filter the inbound traffic before it is forwarded to WAF. Valid values: • **0**: false • **1**: true
SourceIps	String	Yes	["1.1.1.1", "2.2.2.2"]	The IP address or domain of the origin server to which the specified domain points.  **Note:** You can add a maximum of 20 origin IP addresses to implement load balancing or specify only one origin domain. Separate origin IP addresses with commas (,). You can specify either IP addresses or a domain.
LoadBalancing	Integer	No	0	The load balancing algorithm that is used to forward requests to the origin. Valid values: • **0**: IP hash • **1**: Round robin

Parameter	Type	Required	Example	Description
LogHeaders	String	No	[{"k":"wafmark","v":"test"}]	The key-value pair that is used to mark the traffic that flows through WAF to the domain. The style of the parameter value is[{"k":"_key_","v":"_value_"}]. Where, _Key_ represents the specified custom request header field,_Value_ indicates the value set for this field. WAF automatically marks the requests that pass through WAF by adding the specified field and value to the headers of these requests. **Note:** If a request header contains the specified field, WAF overwrites the original field value with the specified value.
HttpPort	String	No	[80]	The HTTP ports. Separate multiple ports with commas (,). **Note:** Set this parameter only if you want to use the HTTP protocol. You must set at least one of the **HttpPort** and **HttpsPort** parameters.

Parameter	Type	Required	Example	Description
HttpsPort	String	No	[443]	The HTTPS ports. Separate multiple HTTPS ports with commas (,). **Note:** Set this parameter only if you want to use the HTTPS protocol. You must set at least one of the **HttpPort** and **HttpsPort** parameters.
Http2Port	String	No	[443]	The HTTP 2.0 ports. Separate multiple ports with commas (,).
HttpToUserIp	Integer	No	0	Specifies whether to enable the HTTP back-to-origin feature. After this feature is enabled, the WAF instance can use HTTP to forward HTTPS requests to the origin server. By default, port 80 is used to forward the requests to the origin server. Valid values: • **0**: disables the feature (default) • **1**: enables the feature **Note:** If your website does not support HTTPS access, you can enable the HTTP back-to-origin feature to enable HTTPS access through WAF.

Parameter	Type	Required	Example	Description
HttpsRedirect	Integer	No	0	Specifies whether to redirect HTTP requests as HTTPS requests. Valid values: • **0**: no (default) • **1**: yes **Note:** This parameter is required only if the specified domain only accepts HTTPS requests. After you enable this feature, HTTP requests are redirected to HTTPS port 443.
ClusterType	Integer	No	0	The type of the WAF cluster. Valid values: • **0**: shared cluster (default) • **1**: exclusive cluster
ResourceGroupId	String	No	rg-atstuj3rtoptyui	The ID of the resource group to which the queried domain belongs in Resource Management. By default, no value is specified, indicating that the domain belongs to the default resource group.
ConnectionTime	Integer	No	5	The connection timeout for WAF exclusive clusters. Unit: seconds. **Note:** You can specify this parameter when you use exclusive clusters.

Parameter	Type	Required	Example	Description
ReadTime	Integer	No	120	The read timeout of a WAF exclusive cluster. Unit: seconds. **Note:** You can specify this parameter when you use exclusive clusters.
WriteTime	Integer	No	120	The timeout period for a WAF exclusive cluster write connection . Unit: seconds. **Note:** You can specify this parameter when you use exclusive clusters.

Response parameters

Parameter	Type	Example	Description
Cname	String	xxxxxx.yundunwaf3.com	The CNAME record assigned by the WAF instance to the specified domain.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=CreateDomain
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&IsAccessProduct=0
&SourceIps=["1.1.1.1", "2.2.2.2"]
&HttpPort=[80]
&<Common request parameters>
```

Sample success responses

XML format

```
<Cname>xxxxxx.yundunwaf3.com</Cname>
```

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
  "Cname":"xxxxxx.yundunwaf3.com",
  "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error code

For a list of error codes, visit the API Error Center.

2.5.4 ModifyDomain

You can call this operation to modify the configurations of a specific domain.

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	Boolean	No	ModifyDomain	The operation that you want to perform. Set the value to **ModifyDomain**.
Domain	String	No	www.example.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Parameter	Type	Required	Example	Description
IsAccessProduct	Integer	Yes	0	Specifies whether to configure a Layer-7 proxy, such as Anti-DDoS Pro or CDN, to filter the inbound traffic before it is forwarded to WAF. Valid values: • **0**: false • **1**: true
SourceIps	String	No	["1.1.1.1", "2.2.2.2"]	The IP address or domain of the origin server to which the specified domain points.  **Note:** You can add a maximum of 20 origin IP addresses to implement load balancing or specify only one origin domain. Separate origin IP addresses with commas (,). You can specify either IP addresses or a domain.
LoadBalancing	String	Optional	0	The load balancing algorithm that is used to forward requests to the origin. Valid values: • **0**: IP hash • **1**: Round robin

Parameter	Type	Required	Example	Description
HttpPort	String	Yes	[80]	The HTTP ports. Separate multiple ports with commas (,). **Note:** Set this parameter only if you want to use the HTTP protocol. You must set at least one of the **HttpPort** and **HttpsPort** parameters.
HttpsPort	String	Yes	[443]	The HTTPS ports. Separate multiple HTTPS ports with commas (,). **Note:** Set this parameter only if you want to use the HTTPS protocol. You must set at least one of the **HttpPort** and **HttpsPort** parameters.
Http2Port	String	Yes	[443]	The HTTP 2.0 ports. Separate multiple ports with commas (,).
HttpsRedirect	String	Optional	0	Specifies whether to redirect HTTP requests as HTTPS requests. Valid values: • **0**: no (default) • **1**: yes **Note:** This parameter is required only if the specified domain only accepts HTTPS requests. After you enable this feature, the HTTP requests are redirected to HTTPS port 443.

Parameter	Type	Required	Example	Description
HttpToUserIp	String	Optional	0	Specifies whether to enable the HTTP back-to-origin feature. After this feature is enabled, the WAF instance can use HTTP to forward HTTPS requests to the origin server. By default, port 80 is used to forward the requests to the origin server. Valid values: • **0**: disables the feature (default) • **1**: enables the feature **Note:** If your website does not support HTTPS access, you can enable the HTTP back-to-origin feature to enable HTTPS access through WAF.

Parameter	Type	Required	Example	Description
LogHeaders	String	Yes	[{"k":"wafmark","v":"test"}]	The key-value pair that is used to mark the traffic that flows through WAF to the domain. Set the parameter in this format: [{"k":"_key_","v":"_value_"}]. Set _key_ to a custom request header field. Set _value_ to a field value. WAF automatically marks the requests that pass through WAF by adding the specified field and value to the headers of these requests. **Note:** If a request header contains the specified field, WAF overwrites the original field value with the specified value.
ClusterType	String	Optional	0	The type of the WAF cluster. Valid values: • **0**: shared cluster (default) • **1**: exclusive cluster
Connection Time	String	Optional	5	The connection timeout for an exclusive cluster. Unit: seconds.
ReadTime	String	Optional	120	The timeout period for an exclusive cluster write connection. Unit: seconds.
WriteTime	String	Optional	120	The timeout period for a read connection of the exclusive cluster. Unit: seconds.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=ModifyDomain
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&IsAccessProduct=0
&SourceIps=["1.1.1.1", "2.2.2.2"]
&<Common request parameters>
```

Sample success responses

`XML` format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

`JSON` format

```
{
  "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.5.5 DeleteDomain

You can call this operation to remove a specified domain from the WAF instance.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteDomain	The operation that you want to perform. Set the value to **DeleteDomain**.
Domain	String	Yes	www.example.com	A domain that has been added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	No	rg-atstuj3rtoptyui	The ID of the resource group to which the specified domain belongs in Resource Management. By default, no value is specified, indicating that the domain that belongs to the default resource group is managed.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DeleteDomain
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
```

```
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes

For a list of error codes, visit the API Error Center.

2.5.6 DescribeCertificates

You can call this operation to query SSL certificates bound to a specified domain.

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	Boolean	No	DescribeCertificates	The operation that you want to perform. Set the value to DescribeCertificates.
Domain	String	No	www.example.com	A domain that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Certificates	Array		The certificate information of the specified domain.
CommonName	String	*.example.com	The domain of the certificate.
IsUsing	Boolean	false	Indicates whether the certificate used by the domain name is valid.
CertificateName	String	CertName	The name of the certificate.
CertificateId	Long	2329260	The ID of the certificate.
Sans	List	["*.example.com"]	A list of domains that are protected by WAF and bound to the certificate.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=DescribeCertificates
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&<Common request parameters>
```

Sample success responses

`XML` format

```
<Certificates>
   <Sans>*.example.com</Sans>
   <CertificateId>2329260</CertificateId>
   <CertificateName>CertName</CertificateName>
   <IsUsing>true</IsUsing>
   <CommonName>*.example.com</CommonName>
</Certificates>
<requestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</requestId>
```

`JSON` format

```
{
   "Certificates":[
```

```
      {
        "Sans":["*.example.com"],
        "CertificateId":2329260,
        "CertificateName":"CertName",
        "IsUsing":true,
        "CommonName":"*.example.com"
      }
    ],
    "requestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```


Error codes.

For a list of error codes, visit the API Error Center.

2.5.7 DescribeCertMatchStatus

You can call this operation to check whether the certificate of a specified domain matches with the private key.

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	DescribeCertMatchStatus	The operation that you want to perform. Set the value to **DescribeCertMatchStatus**.

Parameter	Type	Required	Example	Description
Certificate	String	Yes	-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== -----END CERTIFICATE-----	The content of the certificate.
Domain	String	Yes	www.example.com	A domain that has been added to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
PrivateKey	String	Yes	-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw== -----END RSA PRIVATE KEY-----	The content of the private key.

Parameter	Type	Required	Example	Description
ResourceGroupId	String	No	rg-atstuj3rtoptyui	The ID of the resource group to which the queried domain belongs in Resource Management. By default, no value is specified, indicating that a domain in the default resource group is queried.

Response parameters

Parameter	Type	Example	Description
MatchStatus	Boolean	false	Indicates whether the certificate matches with the private key.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeCertMatchStatus
&Certificate=-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9f
mxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8
PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/
MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv
4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== -----END CERTIFICATE-----
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&PrivateKey=-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn
2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/
W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f
6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04
RtKadOw== -----END RSA PRIVATE KEY-----
&<Common request parameters>
```

Sample success responses

XML format

```
<MatchStatus>false</MatchStatus>
```

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
 "MatchStatus":false
}
```

Error codes

For a list of error codes, visit the API Error Center.

2.5.8 CreateCertificate

You can call this operation to upload a certificate and a private key for a specified domain.

Note:
You can also call this operation to update the uploaded certificate and private key for a specified domain.

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	Boolean	No	CreateCertificate	The operation that you want to perform. Set the value to **CreateCertificate**.
CertificateName	String	No	CertName	The name of the certificate.
Domain	String	No	www.example.com	A domain that has been added to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
PrivateKey	String	No	-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw== -----END RSA PRIVATE KEY-----	The private key corresponding to the certificate.

Parameter	Type	Required	Example	Description
Certificate	String	Yes	-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== -----END CERTIFICATE-----	The content of the certificate.

Response parameters

Parameter	Type	Example	Description
CertificateId	Long	2329260	The certificate ID that is automatically generated by the system.

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=CreateCertificate
&CertificateName=CertName
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&PrivateKey=-----BEGIN RSA PRIVATE KEY----- DADTPZoOHd9WtZ3UKHJTRgNQmioPQn
2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/
W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f
6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04
RtKadOw== -----END RSA PRIVATE KEY-----
&Certificate=-----BEGIN CERTIFICATE----- 62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9f
mxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8
PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/
MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv
4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg== -----END CERTIFICATE-----
&<Common request parameters>
```

Sample success responses

`XML` format

```
<CertificateId>2329260</CertificateId>
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

`JSON` format

```
{
 "CertificateId":"2329260",
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.5.9 CreateCertificateByCertificateId

You can call this operation to create a certificate for a specified domain name based on the certificate ID.

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	Boolean	No	CreateCertificateByCertificateId	The operation that you want to perform. Valid values: **CreateCertificateByCertificateId**.
Domain	String	No	www.example.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
CertificateId	Long	No	3384669	The ID of the certificate.

Response parameters

Parameter	Type	Example	Description
CertificateId	Long	3384669	The ID of the certificate.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=CreateCertificateByCertificateId
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&CertificatedId=3384669
&<Common request parameters>
```

Sample success responses

XML format

```
<CertificateId>3384669</CertificateId>
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
  "CertificateId":"3384669",
  "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.5.10 DescribeDomainBasicConfigs

You can call this operation to query the protection settings in domain configuration records.

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	DescribeDomainBasicConfigs	The operation that you want to perform. Set the value to **DescribeDomainBasicConfigs**.

Parameter	Type	Required	Example	Description
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
DomainKey	String	No	example	A domain keyword. Specify a keyword to query the configuration records of domains that contain the keywords.  **Note:** By default, no value is specified, indicating that the configuration records of all domains added to WAF are queried.
PageNumber	Integer	No	1	The number of the page to return. Default value: 1
PageSize	Integer	No	10	The number of domain configuration records to return on each page. Default value: 10
ResourceGroupId	String	No	rg-atstuj3rtoptyui	The ID of the resource group to which the queried domains belong in Resource Management. By default, no value is specified, indicating that the domains that belong to the default resource group are queried.

Response parameters

Parameter	Type	Example	Description
DomainConfigs			The protection settings of the queried domains.
AclStatus	Integer	1	The status of the HTTP ACL policy feature. Valid values: • **0**: disabled • **1**: enabled
CcMode	Integer	0	The mode of HTTP flood protection. Valid values: • **0**: normal • **1**: emergency
CcStatus	Integer	1	The status of the HTTP flood protection feature. Valid values: • **0**: disabled • **1**: enabled
Domain	String	www.example.com	The domain name.
Owner	String	WAF	The source of a domain configuration record: • **Anti-Bot**: The domain configuration record was created in Anti-Bot Service. • **WAF**: The domain configuration record was created in WAF.
Status	Integer	1	The status of a domain configuration record. Valid values: • **0**: invalid or deleted • **1**: valid • **10**: creating • **11**: creation failed • **20**: deleting

Parameter	Type	Example	Description
Version	Long	0	The system data identifier that is used to control optimistic locking.
WafMode	Integer	0	The mode of Web application protection. Valid values: • **0**: prevention mode • **1**: detection mode
WafStatus	Integer	1	The status of Web application protection. Valid values: • **0**: disabled • **1**: enabled
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
TotalCount	Integer	1	The number of records returned.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDomainBasicConfigs
&InstanceId=waf_elasticity-cn-0xldbqtm005
&<Common request parameters>
```

Sample success responses

`XML` format

```
<TotalCount>1</TotalCount>
<DomainConfigs>
   <Owner>WAF</Owner>
   <AclStatus>1</AclStatus>
   <Version>0</Version>
   <CcStatus>1</CcStatus>
   <WafMode>0</WafMode>
   <WafStatus>1</WafStatus>
   <Domain>www.example.com</Domain>
   <CcMode>0</CcMode>
</DomainConfigs>
```

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
 "TotalCount":1,
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
 "DomainConfigs":[
  {
   "WafStatus":1,
   "Owner":"WAF",
   "AclStatus":1,
   "Domain":"www.example.com",
   "WafMode":0,
   "CcStatus":1,
   "CcMode":0,
   "Version":0
  }
 ]
}
```

Error codes

For a list of error codes, visit the API Error Center.

2.5.11 DescribeDomainAdvanceConfigs

You can call this operation to query the details in the configuration records of domains added to WAF.

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	Boolean	No	DescribeDomainAdvanceConfigs	The operation that you want to perform. Set the value to **DescribeDomainAdvanceConfigs**.
DomainList	String	No	1.example.com,2.example.com	Domains that have been added to WAF. You can enter multiple domains separated with commas (,).

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	Yes	rg-atstuj3rtoptyui	The ID of the resource group to which the queried domain belongs in Resource Management. By default, no value is specified, indicating that the domain belongs to the default resource group.

Response parameters

Parameter	Type	Example	Description
DomainConfigs	Array		The configuration information of domains.
Domain	String	1.example.com	The domain that you add in WAF.
Profile	Struct		The configuration information.
CertStatus	Integer	0	Indicates whether the domain certificate is uploaded and whether the HTTPS protocol is enabled. • **0**: The domain certificate is not uploaded and the HTTPS protocol is disabled. • **1**: The domain certificate is uploaded and the HTTPS protocol is enabled.

Parameter	Type	Example	Description
ClusterType	Integer	0	The type of the WAF cluster. Valid values: • **0**: shared cluster (default) • **1**: exclusive cluster
Cname	String	xxxxxx.yundunwaf3.com	The CNAME record that the WAF instance generates for the domain.
ExclusiveVipStatus	Integer	0	Indicates whether an exclusive WAF IP address is used. Valid values: • **0**: no • **1**: yes
GSLBStatus	Integer	0	Indicates whether intelligent load balancing is enabled. Valid values: • **0**: no • **1**: yes
Http2Port	String	[443]	The HTTP 2.0 port.
HttpPort	String	[80]	The HTTP port.
HttpsPort	String	[443]	The HTTPS port.
Ipv6Status	Integer	0	Indicates whether protection against malicious IPv6 traffic is enabled. Valid values: • **0**: disables protection • **1**: enables protection

Parameter	Type	Example	Description
ResolvedType	Integer	0	The IP address to which the CNAME record points. Valid values: • **-1**: The IP address of the origin server. • **0**: The IP address of the WAF instance. • **1**: The IP address of the exclusive cluster.
Rs	String	["1.1.1.1"]	The IP address of the origin server.
VipService Status	Integer	0	The service status of the IP address of the WAF instance or the exclusive WAF cluster. Valid values: • **0**: The IP address is normal. • **1**: The traffic to the IP address is being scrubbed. • **2**: The IP address is in the black hole.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=DescribeDomainAdvanceConfigs
&DomainList=1.example.com,2.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DomainConfigs>
  <Domain>1.example.com</Domain>
  <Profile>
    <HttpPort>80</HttpPort>
    <Rs>1.1.1.1</Rs>
    <VipServiceStatus>0</VipServiceStatus>
    <Http2Port>443</Http2Port>
    <CertStatus>1</CertStatus>
```

```
      <Ipv6Status>0</Ipv6Status>
      <ExclusiveVipStatus>0</ExclusiveVipStatus>
      <GSLBStatus>0</GSLBStatus>
      <Cname>xxxxxx.yundunwaf3.com</Cname>
      <ResolvedType>0</ResolvedType>
      <HttpsPort>443</HttpsPort>
    </Profile>
</DomainConfigs>
<RequestId>B4A6239E-835F-40FD-8B00-C50AE3CE40A7</RequestId>
```

JSON format

```
{
    "DomainConfigs":[
        {
            "Domain":"1.example.com",
            "Profile":{
                "HttpPort":[80],
                "Rs":["1.1.1.1"],
                "VipServiceStatus":0,
                "Http2Port":[443],
                "CertStatus":1,
                "Ipv6Status":0,
                "ExclusiveVipStatus":0,
                "GSLBStatus":0,
                "Cname":"xxxxxx.yundunwaf3.com",
                "ResolvedType":0,
                "HttpsPort":[443]
            }
        }
    ],
    "RequestId":"B4A6239E-835F-40FD-8B00-C50AE3CE40A7"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.5.12 ModifyLogRetrievalStatus

You can call this operation to enable or disable log retrieval for a specific domain.

Note:

The log search feature of WAF logs all the access requests to a domain only after log retrieval is enabled for the domain. WAF does not log access requests sent to a domain after log retrieval is disabled. After you enable log retrieval again, you cannot query access requests that occurred during the time period when log retrieval was disabled.

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	ModifyLogRetrievalStatus	The operation that you want to perform. Set the value to **ModifyLogRetrievalStatus**.
Domain	String	Yes	www.example.com	The domain that has been added to WAF.
Enabled	Integer	Yes	1	Specifies whether to enable log retrieval. Valid values: • **0**: disables log retrieval • **1**: enables log retrieval
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	No	rg-atstuj3rtoptyui	The ID of the resource group to which the queried domain belongs in Resource Management. By default, no value is specified, indicating that the domain belongs to the default resource group.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyLogRetrievalStatus
&Domain=www.example.com
&Enabled=1
&InstanceId=waf_elasticity-cn-0xldbqtm005
&<Common request parameters>
```

Sample success responses

JSON format

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

XML format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

Error codes

For a list of error codes, visit the API Error Center.

2.5.13 ModifyLogServiceStatus

You can call this operation to enable or disable log collection in the real-time log analysis feature for a specific domain.

Before you enable log collection, make sure that real-time log analysis has been activated for the WAF instance, and WAF has the permission to save logs to the exclusive Logstore.

For more information, see Real-time log analysis.

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	ModifyLogServiceStatus	The operation that you want to perform. Set the value to **ModifyLogServiceStatus**.

Parameter	Type	Required	Example	Description
Domain	String	Yes	www.example.com	The domain that has been added to WAF.
Enabled	Integer	Yes	1	Specifies whether to enable log collection. Valid values: • **0**: disables log collection • **1**: enables log collection
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	No	rg-atstuj3rtoptyui	The ID of the resource group to which the queried domain belongs in Resource Management. By default, no value is specified, indicating that the domain belongs to the default resource group.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyLogServiceStatus
&Domain=www.example.com
&Enabled=1
&InstanceId=waf_elasticity-cn-0xldbqtm005
&<Common request parameters>
```

Sample success responses

JSON format

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

XML format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

Error codes

For a list of error codes, visit the API Error Center.

2.6 Protection configuration

2.6.1 ModifyDomainIpv6Status

You can call this operation to enable or disable protection for a specified domain against malicious IPv6 traffic.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	ModifyDomainIpv6Status	The operation that you want to perform. Set the value to **ModifyDomainIpv6Status**.
Domain	String	No	www.example.com	The domain that has been added to WAF.
Enabled	String	No	0	Specifies whether to enable protection against malicious IPv6 traffic. Valid values: • **0**: disables protection • **1**: enables protection

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf-cn-mp9153****	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=ModifyDomainIpv6Status
&Domain=www.example.com
&Enabled=0
&InstanceId=waf-cn-mp9153****
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Errors

For a list of error codes, visit the API Error Center.

2.6.2 DescribeProtectionModuleStatus

You can call this operation to query the DescribeProtectionModuleStatus status of each protection module, including Web intrusion prevention, data security, advanced protection, Bot management, and access control or throttling.

You can set the **DefenseType** parameter to specify the protection module. For more information about the values of this parameter, see the description of **DefenseType** in the following section.

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

Element	Type	Required	Example	Description
Action	String	Yes	DescribeProtectionModuleStatus	The operation that you want to perform. Set the value to **DescribeProtectionModuleStatus**.

Element	Type	Required	Example	Description
DefenseType	String	Yes	waf	The protection module. Valid values: • **waf**: the RegEx protection engine • **dld**: the big data deep learning engine • **tamperproof**: tamper protection • **antihijack**: web page anti-hijacking • **dlp**: data leakage prevention • **normalized**: positive security model • **bot_crawler**: valid crawlers • **bot_intelligence**: Bot Threat Intelligence • **antifraud**: data risk control • **bot_algorithm**: intelligent algorithm • **bot_wxbb**: App Protection • **bot_wxbb_pkg**: version protection in App protection • **cc**: HTTP flood protection • **ac_blacklist**: the IP blacklist. • **ac_highfreq**: block high-frequency Web attacks in the scanning protection module • **ac_dirscan**: directory traversal protection • **ac_scantools**: scan tools in the scan protection module are blocked. • **ac_collaborative**: collaborative defense • **ac_custom**: custom protection policies
Domain	String	Yes	www.example.com	The domain name that has been added to WAF.

Element	Type	Required	Example	Description
InstanceId	String	Yes	waf_elasticity-cn-0xl****	The ID of the WAF instance.  **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Response parameters

Element	Type	Sample response	Description
ModuleStatus	Integer	1	Indicates whether the module is enabled. Valid values: • **0**: indicates that log backups are disabled. • **1**: indicates enabled.
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample request

```
http(s)://[Endpoint]/? Action=DescribeProtectionModuleStatus
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xl****
&DefenseType=waf
&<Common request parameters>
```

Sample success responses

XML format

```
<ModifyProtectionRuleCacheStatusResponse>
    <ModuleStatus>1</ModuleStatus>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
</ModifyProtectionRuleCacheStatusResponse>
```

JSON format

```
{
  "ModuleStatus": 1,
  "RequestId": "D7861F61-5B61-46CE-A47C-6B19160D5EB0"
```

```
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.6.3 ModifyProtectionModuleStatus

You can call this operation to enable or disable the protection of a specified WAF feature, such as web intrusion prevention, data security, advanced protection, Bot management, and access control or throttling.

You can set the **DefenseType** parameter to specify the protection module. For more information about the values of this parameter, see the description of **DefenseType** in the following section.

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	Boolean	No	ModifyProtectionModuleStatus	The operation that you want to perform. Set the value to **ModifyProtectionModuleStatus**.

Parameter	Type	Required	Example	Description
DefenseType	String	No	waf	The protection module. Valid values: • **waf**: the RegEx protection engine • **dld**: the big data deep learning engine • **tamperproof**: tamper protection • **antihijack**: web page anti-hijacking • **dlp**: data leakage prevention • **normalized**: positive security model • **bot_crawler**: valid crawlers • **bot_intelligence**: Bot Threat Intelligence • **antifraud**: data risk control • **bot_algorithm**: intelligent algorithm • **bot_wxbb**: App Protection • **bot_wxbb_pkg**: version protection in App protection **Note:** After you enable the version protection function, call CreateProtectionModuleRule to create version protection rules that specify the permitted valid versions. • **cc**: HTTP flood protection • **ac_blacklist**: the IP blacklist. • **ac_highfreq**: block high-frequency Web attacks in the scanning protection module • **ac_dirscan**: directory traversal protection • **ac_scantools**: scan tools in the scan protection module are blocked. • **ac_collaborative**: collaborative defense

Parameter	Type	Required	Example	Description
Domain	String	No	www.example.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ModuleStatus	Integer	Yes	1	The status of the specified protection module. Valid values: • **0**: disables the feature • **1**: enables protection

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=ModifyProtectionModuleStatus
&DefenseType=waf
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&ModuleStatus=1
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
  "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
```

```
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.6.4 DescribeProtectionModuleMode

You can call this operation to query the protection mode of a specific protection module, such as web application protection, HTTP flood protection, and the big data deep learning engine.

You can set the **DefenseType** parameter to specify the protection module. For more information about the values of this parameter, see the description of **DefenseType** in the following section.

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	Boolean	No	DescribeProtectionModuleMode	The operation that you want to perform. Set the value to **DescribeProtectionModuleMode**.
DefenseType	String	No	waf	The protection module. Valid values: • **waf**: the RegEx protection engine • **dld**: the big data deep learning engine • **cc**: HTTP flood protection • **antifraud**: data risk control • **normalized**: positive security model
Domain	String	No	www.example.com	The domain name that has been added to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
ResourceGroupId	String	Yes	rg-atstuj3rtoptyui	The ID of the resource group to which the queried domain belongs in Resource Management. By default, no value is specified, indicating that the domain belongs to the default resource group.

Response parameters

Parameter	Type	Example	Description
Mode	Integer	1	The protection mode of the specified protection module. Valid values: **Note:** The value of the **Mode** parameter varies depending on the value of the **DefenseType** parameter. • The RegEx protection engine (DefenseType is set to **waf**) - **0**: prevention mode - **1**: detection mode • The big data deep learning engine (DefenseType is set to **dld**) - **0**: detection mode - **1**: prevention mode • HTTP flood protection (DefenseType is set to **cc**) - **0**: prevention mode - **1**: protection-emergency mode • Data risk control (DefenseType is set to **antifraud**) - **0**: detection mode - **1**: prevention mode - **2**: strict interception mode • Positive security model (DefenseType is set to **normalized**) - **0**: detection mode - **1**: prevention mode
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=DescribeProtectionModuleMode
&DefenseType=waf
```

```
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&<Common request parameters>
```

Sample success responses

`XML` format

```
<Mode>1</Mode>
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

`JSON` format

```
{
 "Mode":1,
   "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.6.5 ModifyProtectionModuleMode

You can call this operation to change the protection mode of a specific protection module, including the RegEx protection engine, big data deep learning engine, HTTP flood protection feature, data risk control feature, and positive security model.

You can set the **DefenseType** parameter to specify the protection module. For more information about the values of this parameter, see the description of **DefenseType** in the following section.

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	ModifyProtectionModuleMode	The operation that you want to perform. Set the value to **ModifyProtectionModuleMode**.

Parameter	Type	Required	Example	Description
DefenseType	String	Yes	waf	The protection module. Valid values: • **waf**: the RegEx protection engine. • **dld**: the big data deep learning engine. • **cc**: HTTP flood protection. • **antifraud**: data risk control. • **normalized**: the positive security model
Domain	String	Yes	www.example.com	The domain that has been added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Parameter	Type	Required	Example	Description
Mode	Integer	Yes	0	The protection mode of the specified protection module. Valid values: **Note:** The value of the **Mode** parameter varies depending on the value of the **DefenseType** parameter. • The RegEx protection engine (DefenseType is set to **waf**) - **0**: prevention mode - **1**: detection mode • The big data deep learning engine (DefenseType is set to **dld**) - **0**: detection mode - **1**: prevention mode • HTTP flood protection (DefenseType is set to **cc**) - **0**: protection mode - **1**: protection-emergency mode • Data risk control (DefenseType is set to **antifraud**) - **0**: detection mode - **1**: prevention mode - **2**: strict interception mode • Positive security model (DefenseType is set to **normalized**) - **1**: prevention mode - **0**: detection mode

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyProtectionModuleMode
&DefenseType=waf
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Mode=0
& <Common request parameters>
```

Sample success responses

`XML` format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

`JSON` format

```
{
  "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes

For a list of error codes, visit the API Error Center.

2.6.6 DescribeProtectionModuleRules

You can call this operation to query the configuration records of DescribeProtectionModuleRules in a specific WAF feature, such as Web intrusion prevention, data security, Bot management, access control or throttling, and website whitelist.

You can set the **DefenseType** parameter to specify the protection module. For more information about the values of this parameter, see the description of **DefenseType** in the following section.

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	Boolean	No	DescribeProtectionModuleRules	The operation that you want to perform. Set the value to **DescribeProtectionModuleRules**.
DefenseType	String	No	ac_highfreq	Specify the protection module. Valid values: • **waf-codec**: configures RegEx protection engine decoding settings. • **tamperproof**: tamper protection. • **dlp**: data leakage prevention. • **ng_account**: account security rule configuration • **bot_crawler**: configuration of valid crawler rules • **bot_intelligence**: Bot Threat Intelligence rule configuration • **antifraud**: data risk control. • **antifraud_js**: data risk control JavaScript. • **bot_algorithm**: Configure Smart algorithm rules • **bot_wxbb_pkg**: version protection rules for App protection • **bot_wxbb**: Path protection rules for App protection • **ac_blacklist**: the IP blacklist. • **ac_highfreq**: IP blocking based on the request rate. • **block_dirscan**: directory traversal. • **ac_custom**: custom protection policies. • **whitelist**: the whitelist.

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
PageSize	String	Optional	10	The number of entries to return on each page.
PageNumber	String	Optional	1	The number of the page to return. Pages start from page 1. Default value: 1
Domain	String	Yes	www.example.com	The domain that has been added to WAF.  **Note:** Only when querying the project security module rules (that is **DefenseType** the parameter value is **account** you must specify the domain name configuration when querying other functional modules.

Parameter	Type	Required	Example	Description
Query	String	Yes	e2ZpbHRlcjp7InJ1bGVJZCI6NDI3NTV9LG9yZGVyQnk6ImdtdF9tb2RpZmllZCIsZGVzYzp0cnVlfQ==	Configure the filtering and sorting of rules, in JSON format strings, including the following parameters: **Note:** **Query** the parameter must be base64-encoded. Construct a JSON string and convert it to the base64-encoded format based on the following parameter description. • **filter**: Optional. The filter conditions in a JSON string. Describe the filter conditions in a JSON string that contains the following parameters: - **nameId**: Optional. This parameter queries rules whose IDs are the same as the value of this parameter, or names contain the parameter value. Data type: string. - **scene**: Optional. This parameter specifies the protection module. Set the value to the same as that of the **DefenseType** parameter. Data type: string. - **enabled**: Optional. This parameter specifies whether the rule is enabled. Data type: Boolean. Valid values: ■ **false**: No ■ **true**: Yes - **status**: Optional. This parameter specifies the rule status. The description of this parameter is the same as that of the **enabled** parameter. Data type:

Parameter	Type	Required	Example	Description
Lang	String	Yes	zh	The language attribute of the rule name. Valid values: • **zh**: Chinese name • **En**: English name • **Ja**: Japanese name

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Rules	Array		The configurations of the rules.
Content	String	{"count":60,"interval":60,"ttl":300}	The content of the rule. It is a JSON string that contains multiple parameters. **Note:** According to the specified protection function module configuration (**DefenseType**), the specific parameters involved vary. For more information, see Content parameter description.
RuleId	Long	42755	The ID of the rule.
Status	Long	1	Indicates the rule status. Valid values: • **0**: disabled • **1**: enabled
Time	Long	1570700044	The time when the rule was created. The timestamp is accurate to the second.

Parameter	Type	Example	Description
Version	Long	2	The system data identifier that is used to control optimistic locking.
TotalCount	Integer	1	The total number of entries returned.

Content

- The JSON string that describes the decoding settings of the RegEx protection engine (DefenseType is set to **waf-codec**) contains the following parameters:
  - **codecList**: Required. The specified decoding settings. Data type: string.
  - **Sample response**

```
{
  "codecList":["url","base64"]
}
```

- To modify a tamper protection rule, set DefenseType to **tamperproof** and construct a JSON string that includes the following parameters:
  - **uri**: Required. The URL that needs protection. Data type: string.
  - **name**: Required. The name of the rule. Data type: string.
  - **status**: Optional. The protection status of the rule. Data type: integer.
    - **0**: disabled (default).
    - **1**: enabled.
  - **Sample request**

```
{
  "name":"example",
  "uri":"http://www.example.com/example",
  "Status":1
}
```

- To modify a data leakage prevention rule, set DefenseType to **dlp** and construct a JSON string that includes the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **conditions**: Required. The matching condition, which is described in a JSON string. You can specify up to two conditions that have the AND logical relation to apply the

conditions at the same time. Data type: array. The array must include the following parameters:

- **key**: The matching items.
  - **0**: Sets the matching item to URLs.
  - **10**: indicates sensitive information.
  - **11**: indicates the response code.
- **operation**: The matching logic. This value is set to **1** by default, which specifies the INCLUDES logical operator.
- **value**: The matching condition values, which are formulated in a JSON string. You can specify multiple values. The JSON string must include the following parameters:
  - **v**: only applies to scenarios where the matching condition (**key**) is set to URLs (**0**) or HTTP status codes (**11**).
    - URL: when`"key":0` the parameter value is the URL address.
    - Response Code: when`"key":11` valid values for the parameter include**400**,**401** ,**402**,**403**,**404**,**405-499**,**500**,**501**,**502**,**503**,**504**,**505-599**.
  - **k**: only applies to scenarios where the matching item (**key**) is set to sensitive information (**10**). Valid values:
    - **100**: masks resident ID card numbers.
    - **101**: masks credit card numbers.
    - **102**: masks phone numbers.
    - **103**: masks the default sensitive words.

- **action**: The matching action.
  - **3**: sets the matching action to warn.
  - **10**: filters sensitive information. This action only applies to scenarios where sensitive information is contained (`"key":10`) to find matching conditions.
  - **11**: indicates that the system returns to the built-in intercept page, this action only applies to response codes (`"key":11`) to find matching conditions.
- **Sample request**

```
 {
   "name":"example",
   "conditions":[{"key":11,"operation":1,"value":[{"v":401}]},{"key":"0","operation":1,"
value":[{"v":"www.example.com"}]}],
```

```
  "action":3
}
```

- Configure account security rules (**ng_account**) corresponding to the JSON string contains the following parameters:
  - **domain**: Required. The domain that is protected. Data type: string.
  - **Method**: The request method to be moderated. Valid values: POST, GET, PUT, and DELETE. Data Type: String. You can set multiple request methods. Separate multiple request methods with commas (,).
  - **url_path**: Required. The URL to the operation that runs detection tasks. The URL must start with a slash (/). Data type: string.
  - **account_left**: Required. The parameter that specifies the account. Data type: string.
  - **password_left**: Optional. The password of the account. Data type: string.
  - **Action**: Required. The protection action. Valid values:
    - **Monitor**: indicates an alert.
    - **Block**: indicates interception.
  - **Sample request**

```
{
   "domain":"www.example.com",
   "method":"GET,POST",
   "url_path":"/example",
   "account_left":"aaa",
   "action":"monitor"
}
```

- Configure valid crawler rules (**bot_crawler**) corresponding to the JSON string contains the following parameters:
  - **Status**: Required. Data type: integer. Valid values:
    - 0: Disabled
    - 1: enabled
  - **Version**: Required. The version of the rule. Data type: integer.
  - **Content**: Required. The details of the rule, in JSON format. Data type: string. This parameter includes the following parameters:
    - **name**: Required. The name of the rule. Data type: string.
    - **Conditions**: Optional. The Path Protection Condition. Data type: array. In the valid crawler rule configuration, it is fixed to empty, indicating the full path.
    - **expressions**: Required. The regular expression that represents the matching conditions of all rules in a readable way. Data type: array.
    - **bypassTags**: Required. The module to be ignored. Data type: string. Set it in the configuration of valid crawler rules. **antibot**, indicating the Bot management module.
    - **Tags**: Required. The protection module to which the rule belongs. Data type: array. Set it in the configuration of valid crawler rules. ["antibot"], indicating the Bot management module.
  - **RuleId**: Required. The ID of the rule. Data type: integer.
  - **Time**: Required. The time when the rule is last modified, in seconds. Data type: string.
  - **Sample request**

```
{
   "Status":0,
   "Version":1,
   "Content":{
      "name":"Baidu Spider whitelist",
      "conditions":[],
      "expressions":["remote_addr inl 'ioc.210d077a-cf34-49ad-a9b3-0aa48095c5
95' && uri =^ '/'"],
      "bypassTags":"antibot",
      "tags":["antibot"]
   },
  "RuleId":20384,
  "Time":1585818161
  }
```

```
```

- Bot Threat Intelligence configurations (**bot_intelligence**) corresponding to the JSON string contains the following parameters:
  - **Status**: Required. Data type: integer. Valid values:
    - **0**: disabled
    - **1**: enabled
  - **Version**: Required. The version of the rule. Data type: Integer.
  - **Content**: Required. The details of the rule, in JSON format. Data type: string. It includes the following parameters:
    - **name**: Required. The name of the rule. Data type: string.
    - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
      - **monitor**: monitors requests
      - **captcha**: requires CAPTCHA verification
      - **captcha_strict**: requires more strict CAPTCHA verification
      - **JS**: indicates JavaScript validation.
      - **block**: blocks requests
    - **urlList**: Required. The protected paths. You can specify a maximum of ten protected paths. Data type: array. The parameter is represented as a JSON string, which includes the following parameters:
      - **Mode**: Required. The matching method. This parameter must be the same as the path keyword (**URL**) parameter in combination with the specified protected path. Optional values: **EQ**(Precise matching), **prefix-match**(Prefix matching), **regex**(Regular expression matching).
      - **URL**: Required. The path keyword, which must start with a forward slash (/). Data type: string.
    - **keyType**: Required. The type of the intelligence database, including the IP address Library (**IP**), fingerprint Library (**UA**) two types.
  - **RuleId**: Required. The ID of the rule. Data type: integer.
  - **Time**: Required. The time when the rule is last modified, in seconds. Data type: string.
  - **Sample request**

```
{
```

```
    "Status":1,
    "Version":1,
    "Content":{
      "name":"IDC IP Address Library-Tencent Cloud",
      "action":"captcha_strict",
      "urlList":[{"mode":"prefix-match","url":"/indexa"}, {"mode":"regex","url":"/"},{"
mode":"eq","url":"/"}],
      "keyType":"ip"
    },
    "RuleId":922777,
    "Time":1585907112
  }
```

- To modify a data risk control request, set DefenseType to **antifraud** and construct a JSON string that includes the following parameters:
  - **uri**: Required. The request URL. Data type: string.
  - **Sample request**

```
{
  "uri": "http://1.example.com/example"
}
```

- The JSON string that describes the data risk control JavaScript insertion feature (DefenseType is set to **antifraud_js**) contains the following parameters:
  - **uri**: Required. The URL of the web page into which you want to insert the data risk control JavaScript. The system inserts data risk control JavaScript into all the pages under the specified URL directory.
  - **Sample request**

```
{
  "uri": "/example/example"
}
```

- Bot management intelligent algorithm rule configuration (**bot_algorithm**) corresponding to the JSON string contains the following parameters:
  - **Status**: Required. Data type: integer. Valid values:
    - 0: Disabled
    - 1: enabled
  - **Version**: Required. The version of the rule. Data type: integer.
  - **Content**: Required. The details of the rule, in JSON format. Data type: string. The parameter includes the following parameters:
    - **name**: Required. The name of the rule. Data type: string.
    - **timeInterval**: Required. The detection period. Valid values: 30, 60, 120, 300, and 600. Unit: Seconds. Data type: integer.
    - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
      - **Monitor**: indicates observation.
      - **CAPTCHA**: indicates the slider.
      - **JS**: indicates JavaScript validation.
      - **Block**: indicates the block. When blocking is selected as the disposal action, the blocking duration (**blocktime**) parameter.
    - **blocktime**: Optional. The blocking duration. Unit: Minutes. Value range: 1 to 600.
    - **algorithmName**: Required. The name of the algorithm. Valid values:
      - **RR**: indicates the Crawler identification algorithm for special resources.
      - **PR**: indicates a targeted path Crawler identification algorithm.
      - **DPR**: indicates the round-robin Crawler identification algorithm.
      - **SR**: indicates the dynamic IP Crawler identification algorithm.
      - **IND**: indicates the proxy Crawler identification algorithm.
      - **Periodicity**: indicates the periodic crawler recognition algorithm.
    - **config**: Required. The algorithm configuration, in JSON format. Data Type: String. The specific sub-parameters in the algorithm configuration and the selected algorithm name (**algorithmName**) related.
      - Crawler identification algorithm for special resources (**RR**) the corresponding configuration information shall contain the following sub-parameters:

- **resourceType**: The type of the requested resource. Valid values:
  - **1**: represents a dynamic resource type.
  - **2**: represents a static resource type.
  - **-1**: indicates custom resource types. If you select a custom Resource Group, **extensions** the parameter that specifies the resource suffix in string format. Separate multiple file extensions with commas (,), for example, `css ,jpg,xls`.
- **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests are detected. Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.
- **minRatio**: Required. The risk determination condition. A risk is determined when the proportion of requests sent by an IP address exceeds the threshold. Valid values: 0.01 to 1.

- Directed path Crawler identification algorithm (**PR**) the corresponding configuration information shall contain the following sub-parameters:
  - **keyPathConfiguration**: The request path. You can specify a maximum of 10 Paths. This parameter is required only when a Crawler identification algorithm is used. Data type: array. The parameters must be in a JSON string. The following parameters must be included:
    - **Method**: Required. The request method. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, **OPTIONS**.
    - **URL**: Required. The request path keyword, which must start with a forward slash (/). Data type: string.
    - **matchType**: Required. The matching method. This parameter must be the same as the request path keyword (**URL** parameter in combination with the specified request path. Optional values: **all**(Precise matching), **prefix** (Prefix matching), **regex**(Regular expression matching).
  - **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests

are detected. Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.

- **minRatio**: Required. The risk determination condition, that is, the threshold of the percentage of accesses to the specified path in IP access requests (applicable to the Crawler identification algorithm for specific specific paths). If the threshold is exceeded, a risk is determined. Valid values: 0.01 to 1.

- Parameter polling Crawler identification algorithm (**DPR**) the corresponding configuration information shall contain the following sub-parameters:
  - **Method**: Required. The request method. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, **OPTIONS**.
  - **urlPattern**: Required. The path of the key parameter, which must start with a forward slash (/). Data Type: String. Key parameters are indicated by braces ({}). When multiple braces ({}) are set, these parameters are joined as key parameters. For example, `/company/{}/{}/{}/user.php? uid={}` .
  - **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests are detected. Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.
  - **minRatio**: Required. The risk determination condition. If the value of a key parameter exceeds the threshold, the request is considered as a risk. A value of 0.01 to 1 indicates a risk.
- Dynamic IP Crawler identification algorithm (**SR**) the corresponding configuration information shall contain the following sub-parameters:
  - **maxRequestCountPerSrSession**: Required. It specifies the minimum number of requests in each session. If the number of requests in each session is smaller than the value of this parameter, a session is abnormal. Valid values: 1 to 8.
  - **minSrSessionCountPerIp**: Required. The risky condition. The value is the threshold for the number of abnormal sessions in an IP access request. If the

number of abnormal sessions exceeds this threshold, a risk is detected. Valid values: 5 to 300.

- Proxy Crawler identification algorithm (**IND**) the corresponding configuration information shall contain the following sub-parameters:
  - **minIpCount**: Required. The condition for determining the number of IP addresses associated with the Wi-Fi connection of a malicious device. If the threshold is exceeded, a risk is detected. Valid values: 5 to 500.
  - **keyPathConfiguration**: The detection path information. You can specify up to 10 paths. Data type: array. The parameters must be in a JSON string. The following parameters must be included:
    - **Method**: Required. The request method. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, **OPTIONS**.
    - **URL**: Required. The keyword of the detection path, which must start with a forward slash (/). Data Type: String.
    - **matchType**: Required. The matching method. This parameter must be the same as the keyword of the detection path (**URL** parameter in combination with the specified request path. Optional values: **all**(Precise matching), **prefix**(Prefix matching), **regex**(Regular expression matching).
- Periodic Crawler identification algorithm (**Periodicity**) the corresponding configuration information shall contain the following sub-parameters:
  - **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests

are detected. Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.

  - **level**: Required. The risk level of the Accessed IP address. It indicates the visibility of the periodic features of the IP address. Data type: Integer. Valid values:
    - **0**: indicates obvious
    - **1**: Medium
    - **2**: indicates weak.

- **RuleId**: Required. The ID of the rule. Data type: Integer.
- **Time**: Required. The time when the rule is last modified, in seconds. Data type: string.
- **Sample request**

```
{
    "Status":1,
    "Version":1,
    "Content":{
      "name":"Dynamic IP",
      "timeInterval":60,
      "action":"warn",
      "algorithmName":"IND",
      "config":{"minIpCount":5,"keyPathConfiguration":[{"method":"GET","
matchType":"prefix","url":"/index"}]}
    },
    "RuleId":940180,
    "Time":1585832957
}
```

- Version protection rule configuration for App protection (**bot_wxbb_pkg**) corresponding to the JSON string contains the following parameters:
  - **Version**: Required. The version of the rule. Data type: integer.
  - **Content**: Required. the details of the rule, in JSON format. Data of the String type includes the following parameters:
    - **name**: Required. The name of the rule. Data type: string.
    - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
      - **Test**: indicates observation.
      - **Close**: indicates the block.
    - **nameList**: Required. The version information. You can specify up to five rules. Data type: array. The code is represented as a JSON string, which includes the following parameters:
      - **Name**: Required. The name of the valid package. Data type: string.
      - **signList**: Required. The signature of the corresponding package. You can specify a maximum of 15 signatures. Separate multiple signatures with commas (,). Data type: array.
  - **RuleId**: Required. The ID of the rule. Data type: integer.
  - **Time**: Required. The time when the rule is last modified, in seconds. Data type: string.
  - **Sample request**

```
{
  "Version":0,
  "Content":{
    "nameList":[{"signList":["xxxxxx","xxxxx","xxxx","xx"],"name":"apk-xxxx"}],
    "name":"test",
    "action":"close"
  },
  "RuleId":271,
  "Time":1585836143
}
```

- Configure the path protection rule for App protection **bot_wxbb**) corresponding to the JSON string contains the following parameters:
  - **Version**: Required. The version of the rule. Data type: integer.
  - **Content**: Required. The details of the rule, in JSON format. Data of the String type includes the following parameters:
    - **name**: Required. The name of the rule. Data type: string.
    - **uri**: Required. The path, which must start with a forward slash (/). Data Type: String.
    - **matchType**: Required. The matching method. Data type: string. Optional values: **all**(Precise matching), **prefix**(Prefix matching), **regex**(Regular expression matching).
    - **Arg**: Required. The parameter value. Data type: string. Together with the **matchType** parameter, it specifies protected path configuration.
    - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
      - **Test**: indicates observation.
      - **Close**: indicates the block.
    - **wxbbVmpFieldType**: Optional. The type of the user-defined field. Data type: Integer. If no user-defined field is set in the rule, this parameter is not returned. Set the value to:
      - **0**: indicates the header.
      - **1**: represents the parameter.
      - **2**: indicates a cookie.
    - **wxbbVmpFieldValue**: Optional. The value of the user-defined field. Data type: string. If no user-defined field is set in the rule, this parameter is not returned.
    - **blockInvalidSign**: Required. The action to be taken against an invalid signature. Data type: Boolean.
    - **blockProxy**: Required. The action to perform on the proxy. Data type: Boolean.
    - **blockSimulator**: Required. The action to be processed by the simulator. Data type: Boolean.
  - **RuleId**: Required. The ID of the rule. Data type: Integer.
  - **Time**: Required. The time when the rule is last modified, in seconds. Data type: String.

- **Sample request**

```
{
  "Version":6,
  "Content":{
    "blockInvalidSign":true,
    "wxbbVmpFieldValue":"test",
    "blockSimulator":true,
    "matchType":"all",
    "arg":"test",
    "name":"test",
    "action":"close",
    "blockProxy":true,
    "uri":"/index",
    "wxbbVmpFieldType":1
  },
  "RuleId":2585,
  "Time":1586241849
}
```

- The JSON string that describes the IP blacklist rule (DefenseType is set to**ac_blacklist**) contains the following parameters:
  - **empty**: Required. This parameter indicates whether the blacklist is empty. Data type: Boolean.
  - **remoteAddr**: Required. This parameter represents the IP addresses in the blacklist. Data type: Array.
  - **Area**: Required. the region blocking rule. Data type: String. It must be a JSON String. These parameters include countryCodes, regionCodes, and whether to allow (not). The blocked countries and regions are returned by using annotations. We recommend that you go to the console to view the blocked countries and regions.
  - **Sample request**

```
{
  "empty":false,
  "remoteAddr":["1.1.1.1","12.11.1.2"]
}
```

- To modify the rule that automatically blocks IP addresses initiating attacks, set DefenseType to **ac_highfreq**, and construct a JSON string that contains the following parameters:
  - **Interval** Required. The time range to be detected, in seconds. Valid values:[5,1800].
  - **TTL**: Required. The duration of blocked IP addresses. Unit: Seconds. Value range: 60 to 86400.
  - **count**: Required. The maximum number of requests allowed from an IP address. If the number of requests initiated from an IP address during the specified time period exceeds this limit, the IP address is blocked. Data type: integer. Value range: 2-50000.
  - **Sample request**

```
{
  "interval":60,
  "ttl":300,
  "count":60
}
```

- To modify a directory traversal protection rule, set DefenseType to **block_dirscan** and construct a JSON string that includes the following parameters:
  - **Interval**: Required. The time range to be detected, in seconds. Valid values:[5,1800].
  - **ttl**: Required. The time period (in seconds) during which an IP address is blocked. Data type: Integer.
  - **Count**: Required. The number of visits. Valid values:[2,50000].
  - **Weight**: Required. The threshold of HTTP status codes 404 (as a percentage). Valid values:(0,1].
  - **uriNum**: Required. The threshold of the number of directories to be scanned. Valid values:[2,50000].
  - **Sample request**

```
{
  "interval":10,
  "ttl":1800,
  "count":50,
  "weight":0.7,
  "uriNum":20
}
```

- Custom protection policies rule configuration (**ac_custom**), its corresponding JSON string **scene** to set ACL access control rules and HTTP flood protection rules.
  - To modify an ACL rule, set **scene** to **custom_acl**, and construct a JSON string that includes the following parameters.
    - **name**: Required. The name of the rule. Data type: string.
    - **scene**: Required. The type of the protection policy. Data type: string. If you need to modify an ACL rule, set the value to **custom_acl**.
    - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
      - **monitor**: monitors requests
      - **captcha**: requires CAPTCHA verification
      - **captcha_strict**: requires more strict CAPTCHA verification
      - **js**: requires JavaScript verification
      - **block**: blocks the request.
    - **conditions**: Required. The matching conditions. Data type: array. The conditions are described in a JSON string that contains the following parameters:
      - **Key**: the matching field. Valid values: **URL**, **IP**, **Referer**, **user-Agent**, **Params**, **Cookie**, **content-Type**, **content-Length**, **x-Forwarded-For**, **post-Body**, **http-Method**, **Header**, **URLPath**.
      - **opCode**: The logical operator. Valid values:
        - **0**: does not include
        - **1**: includes
        - **2**: does not exist
        - **10**: does not equal
        - **11**: equals
        - **20**: length smaller than
        - **21**: length equals
        - **22**: length greater than
        - **30**: value smaller than
        - **31**: value equals
        - **32**: value greater than

- **40**: does not belong to
- **41**: belongs to

- **values**: The matching content. Set the content as required, in String format.
- **contain**: The logical operator. Valid values are the same as those of the **opCode** parameter.
- **opValue**: The description of the abbreviated logical operator. For more information, see the description of **opCode**.
- **pattern**: The description of the abbreviated logical operator. Valid values are the same as those of the **opValue** parameter.

- **expressions**: Required. The regular expression that represents the matching conditions of all rules in a readable way. Data type: array.

- **Sample request**

```
    {
      "name":"test2",
      "action":"monitor",
      "conditions":[{"contain":1,"values":"login","pattern":"contain","opCode":1,"
opValue":"contain","key":"URL"}],
      "expressions":["request_uri contains 'login' "],
      "scene":"custom_acl"
    }
```

- Set HTTP flood protection rules (**scene** the parameter value is **custom_cc**), the corresponding JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **scene**: Required. The type of the protection policy. Data type: string. If you need to modify a protection rule against HTTP flood attacks, set the value to **custom_cc**.
  - **conditions**: Required. The matching conditions. Data type: array. The conditions are described in a JSON string that contains the following parameters:
    - **Key**: the matching field. Valid values: **URL**, **IP**, **Referer**, **user-Agent**, **Params**, **Cookie**, **content-Type**, **content-Length**, **x-Forwarded-For**, **post-Body**, **http-Method**, **Header**, **URLPath**.
    - **opCode**: The logical operator. Valid values:
      - **0**: does not include
      - **1**: includes
      - **2**: does not exist
      - **10**: does not equal
      - **11**: equals
      - **20**: length smaller than
      - **21**: length equals
      - **22**: length greater than
      - **30**: value smaller than
      - **31**: value equals
      - **32**: value greater than
      - **40**: does not belong to
      - **41**: belongs to
    - **values**: The matching content. Set the content as required, in String format.
    - **contain**: The logical operator. Valid values are the same as those of the **opCode** parameter.
    - **opValue**: The description of the abbreviated logical operator. For more information, see the description of **opCode**.
    - **pattern**: The description of the abbreviated logical operator. Valid values are the same as those of the **opValue** parameter.

- **expressions**: Required. The regular expression that represents the matching conditions of all rules in a readable way. Data type: array.
- **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
  - **monitor**: monitors requests
  - **captcha**: requires CAPTCHA verification
  - **captcha_strict**: requires more strict CAPTCHA verification
  - **js**: requires JavaScript verification
  - **block**: block requests
- **ratelimit**: Required. The maximum request rate from an object. Data type: JSON. Describe the rate in a JSON string that includes the following parameters:
  - **target**: Required. The type of the object whose request rate is calculated. Data type: string. Valid values:
    - **remote_addr**: IP addresses.
    - **cookie.acw_tc**: sessions.
    - **queryarg**: custom parameters. If you choose to use custom parameters, specify the name of the object in the **subkey** parameter.
    - **cookie**: custom cookies. If you choose to use custom cookies, specify the cookie content in the **subkey** parameter.
    - **header**: custom headers. If you choose to use custom headers, specify the header content in the **subkey** parameter.
  - **subkey**: Optional. When **target** is set to **cookie**, **header**, or **queryarg**, you must specify the required information in the **subkey** parameter. Data type: string.
  - **interval**: Required. The time period (in seconds) during which the number of requests from the specified object is calculated. This parameter must be used together with the **threshold** parameter. Data type: integer.
  - **threshold**: Required. During the specified time period, the maximum number of requests that are allowed from an individual object. Data type: integer.
  - **status**: Optional. The maximum number of an HTTP status code. Data type: string. It is described in a JSON string that contains the following parameters:
    - **code**: Required. The specified HTTP status code. Data type: integer.

- **Count**: Optional. It indicates the occurrence threshold. If the number of occurrences exceeds the threshold, a protection rule is hit. Valid values:[1, 999999999]. You can select either **Count** or **ratio** parameter.
- **Ratio**: Optional. The threshold (in percentage) of the response code. If the occurrence ratio of a specified response code exceeds this threshold, the rule is hit. Valid values:[1,100]. You can select either **Count** or **ratio** parameter.

- **scope**: Required. This parameter specifies where the settings take effect. Data type: string. Valid values:
  - **rule**: objects that match the specified conditions.
  - **domain**: domains where the rule is applied.
- **TTL**: Required. The validity period of the action. Unit: Seconds. Data type: integer. Valid values:[60,86400].
- **Sample request**

```
    {
      "name":"anti-HTTP flood attacks",
      "conditions":[{"contain":1,"values":"login","pattern":"contain","opCode
":1,"opValue":"contain","key":"URL"}],
      "expressions":["request_uri contains 'login' "],
      "action":"block",
      "scene":"custom_cc",
      "ratelimit":{
        "target": "remote_addr",
        "interval": 300,
        "threshold": 2000,
        "status": {
          "code": 404,
          "count": 200
        },
        "scope": "rule",
        "ttl": 1800
      }
    }
```

- To modify a whitelist rule, set DefenseType to **whitelist**, and construct a JSON string that includes the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **tags**: Required. The protection modules that can be skipped. You can specify multiple modules. Valid values:
    - **waf**: the website whitelist
    - **cc**: system HTTP flood protection
    - **customrule**: custom rules
    - **blacklist**: the IP blacklist
    - **antiscan**: anti-scan protection
    - **regular**: web application protection
    - **deeplearning**: deep learning
    - **antifraud**: data risk control
    - **dlp**: data leakage prevention
    - **tamperproof**: tamper protection
    - **bot_intelligence**: indicates bot threat intelligence.
    - **bot_algorithm**: indicates an intelligent algorithm.
    - **bot_wxbb**: indicates App protection.
  - **bypassTags**: Required. The list of protection modules that skip detection. Data type: string.
  - **conditions**: Required. The matching conditions. Data type: array. The conditions are described in a JSON string that contains the following parameters:
    - **Key**: the matching field. Valid values: **URL**, **IP**, **Referer**, **user-Agent**, **Params**, **Cookie**, **content-Type**, **content-Length**, **x-Forwarded-For**, **post-Body**, **http-Method**, **Header**, **URLPath**.
    - **opCode**: The logical operator. Valid values:
      - **0**: does not include
      - **1**: includes
      - **2**: does not exist
      - **10**: does not equal
      - **11**: equals
      - **20**: length smaller than

- **21**: length equals
- **22**: length greater than
- **30**: value smaller than
- **31**: value equals
- **32**: value greater than
- **40**: does not belong to
- **41**: belongs to

- **values**: The matching content. Set the content as required, in String format.
- **contain**: The logical operator. Valid values are the same as those of the **opCode** parameter.
- **opValue**: The description of the abbreviated logical operator. For more information, see the description of **opCode**.
- **pattern**: The description of the abbreviated logical operator. Valid values are the same as those of the **opValue** parameter.

- **expressions**: Required. The regular expression that represents the matching conditions of all rules in a readable way. Data type: array.
- **Sample request**

```
{
    "name": "test",
    "tags": ["cc","customrule"],
    "bypassTags":"antifraud,dlp,tamperproof",
    "conditions":[{"contain":1,"values":"login","pattern":"contain","opCode":1,"
opValue":"contain","key":"URL"}],
    "expressions":["request_uri contains 'login' "]
}
```

Samples

Sample request

```
http(s)://[Endpoint]/? Action=DescribeProtectionModuleRules
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Domain=www.example.com
&DefenseType=ac_highfreq
&<Common request parameters>
```

Sample success responses

XML format

```
<TotalCount>1</TotalCount>
<Rules>
  <Version>2</Version>
```

```
    <Status>1</Status>
    <Content>
      <count>60</count>
      <interval>60</interval>
      <ttl>300</ttl>
    </Content>
    <RuleId>42755</RuleId>
    <Time>1570700044</Time>
</Rules>
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
    "TotalCount":1,
    "Rules":[
      {
        "Version":2,
        "Status":1,
        "Content":{"count":60,"interval":60,"ttl":300},
        "RuleId":42755,
        "Time":1570700044
      }
    ],
    "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.6.7 CreateProtectionModuleRule

You can call this operation to create rules in a specified WAF feature, such as web intrusion prevention, data security, advanced protection, Bot management, and access control and throttling.

You can set the **DefenseType** parameter to specify the protection module. For more information about the values of this parameter, see the description of **DefenseType** in the following section.

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	Boolean	No	CreateProtectionModuleRule	The operation that you want to perform. Set the value to **CreateProtectionModuleRule**.
Domain	String	No	www.example.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
Rule	String	No	{"action":"monitor","name":"test","scene":"custom_acl","conditions":[{"opCode":1,"key":"URL","values":"/example"}]}	The content of the rule. It is a JSON string that contains multiple parameters.  **Note:** According to the specified protection function module configuration (**DefenseType**), the specific parameters involved vary. For more information, see Rule parameters.

Parameter	Type	Required	Example	Description
DefenseType	String	Yes	ac_custom	Specify the protection module. Valid values: • **waf-codec**: configures RegEx protection engine decoding settings. • **tamperproof**: tamper protection. • **dlp**: data leakage prevention. • **ng_account**: account security rule configuration • **antifraud**: data risk control. • **antifraud_js**: data risk control JavaScript. • **bot_algorithm**: intelligent algorithm rules for Bot management • **bot_wxbb_pkg**: version protection rules for App protection • **bot_wxbb**: path protection rules for App protection • **ac_custom**: custom protection policies. • **whitelist**: whitelist

Rule parameters

- To configure the decoding settings of the RegEx protection engine, set DefenseType to **waf-codec** and construct a JSON string that includes the following parameters:
  - **codecList**: Required. The decoding settings. Data type: string. You can view the valid values of this parameter in the WAF console.
  - **Sample request**

```
{
  "codecList":["url","base64"]
}
```

- To modify a tamper protection rule, set DefenseType to **tamperproof** and construct a JSON string that includes the following parameters:
  - **uri**: Required. The URL that needs protection. Data type: string.
  - **name**: Required. The name of the rule. Data type: string.
  - **Sample request**

```
{
  "name":"example",
  "uri":"http://www.example.com/example"
}
```

- To modify a data leakage prevention rule, set DefenseType to **dlp** and construct a JSON string that includes the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **conditions**: Required. The matching condition, which is described in a JSON string. You can specify up to two conditions that have the AND logical relation to apply the conditions at the same time. Data type: array. The array must include the following parameters:
    - **key**: The matching items.
      - **0**: Sets the matching item to URLs.
      - **10**: indicates sensitive information.
      - **11**: indicates the response code.

Note:

> You cannot set HTTP status codes (**11**) and sensitive information (**10**) as the matching conditions in the **conditions** parameter at the same time.

- **operation**: The matching logic. This value is set to **1** by default, which specifies the INCLUDES logical operator.
- **value**: The matching condition values, which are formulated in a JSON string. You can specify multiple values. The JSON string must include the following parameters:
  - **v**: only applies to scenarios where the matching condition (**key**) is set to URLs (**0**) or HTTP status codes (**11**).
    - URL: when`"key":0` the parameter value is the URL address.
    - Response Code: when`"key":11` valid values for the parameter include**400**,**401**,**402**,**403**,**404**,**405-499**,**500**,**501**,**502**,**503**,**504**,**505-599**.
  - **k**: only applies to scenarios where the matching item (**key**) is set to sensitive information (**10**). Valid values:
    - **100**: masks resident ID card numbers.
    - **101**: masks credit card numbers.
    - **102**: masks phone numbers.
    - **103**: masks the default sensitive words.
- **action**: The matching action.
  - **3**: sets the matching action to warn.
  - **10**: filters sensitive information. This action only applies to scenarios where sensitive information is contained (`"key":10`) to find matching conditions.
  - **11**: indicates that the system returns to the built-in intercept page, this action only applies to response codes (`"key":11`) to find matching conditions.
- **Sample request**

```
{
  "name":"example",
  "conditions":[{"key":11,"operation":1,"value":[{"v":401}]},{"key":"0","operation":1,"
value":[{"v":"www.example.com"}]}],
  "action":3
}
```

- Configure account security rules (**ng_account**) corresponding to the JSON string contains the following parameters:
  - **url_path**: Required. The URL to the operation that runs detection tasks. The URL must start with a slash (/). Data type: string.
  - **Method**: The request method to be moderated. Valid values: POST, GET, PUT, and DELETE. Data Type: String. You can set multiple request methods. Separate multiple request methods with commas (,).
  - **account_left**: Required. The parameter that specifies the account. Data type: string.
  - **password_left**: Optional. The password of the account. Data type: string.
  - **Action**: Required. The protection action. Valid values:
    - **Monitor**: indicates an alert.
    - **Block**: indicates interception.
  - **Sample request**

```
{
   "url_path":"/example",
   "method":"POST,GET,PUT,DELETE",
   "account_left":"aaa",
   "password_left:" 123 ",
   "action":"monitor"
}
```

- To modify a data risk control request, set DefenseType to **antifraud** and construct a JSON string that includes the following parameters:
  - **uri**: Required. The request URL. Data type: string.
  - **Sample request**

```
{
   "uri": "http://1.example.com/example"
}
```

- To modify the data risk control JavaScript that is inserted into a web page, set DefenseType to **antifraud_js** and construct a JSON string that includes the following parameters:
  - **uri**: Required. The URL of the web page into which you want to insert the data risk control JavaScript. The system inserts data risk control JavaScript into all the pages under the specified URL directory. Data type: string.
  - **Sample request**

```
{
  "uri": "/example/example"
}
```

- Bot management intelligent algorithm rule configuration (**bot_algorithm**) corresponding to the JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **algorithmName**: (required) the name of the algorithm. Valid values:
    - **RR**: indicates the Crawler identification algorithm for special resources.
    - **PR**: indicates a targeted path Crawler identification algorithm.
    - **DPR**: represents the round-robin Crawler identification algorithm.
    - **SR**: indicates the dynamic IP Crawler identification algorithm.
    - **IND**: represents the proxy Crawler identification algorithm.
    - **Periodicity**: indicates the periodic crawler recognition algorithm.
  - **timeInterval**: Required. The detection period. Valid values: 30, 60, 120, 300, and 600. Unit: Seconds. Data type: integer.
  - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
    - **Monitor**: indicates observation.
    - **CAPTCHA**: indicates the slider.
    - **JS**: indicates JavaScript validation.
    - **Block**: indicates the block. When blocking is selected as the disposal action, the blocking duration (**blocktime**) parameter.
  - **blocktime**: Optional. The blocking duration. Unit: Minutes. Value range: 1 to 600.
  - **config**: Required. the algorithm configuration, in JSON format. Data type: string. The specific sub-parameters in the algorithm configuration and the selected algorithm name (**algorithmName**) related.
    - Crawler identification algorithm for special resources (**RR**) the corresponding configuration information shall contain the following sub-parameters:
      - **resourceType**: The type of the requested resource. Valid values: integer.
        - **1**: represents a dynamic resource type.
        - **2**: represents a static resource type.
        - **-1**: indicates custom resource types. If you select a custom Resource Group, enter the **extensions** parameter that specifies the resource suffix in string

format. Separate multiple file extensions with commas (,), for example, `css`, `jpg,xls`.

- **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests are detected. Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.
- **minRatio**: Required. The criteria for determining the risk, that is, the proportion of requests sent by an IP address to the specified resource (this corresponds to the crawler detection algorithm for special resources.) the proportion of requests sent by IP addresses to the specified path. This value exceeds the threshold. Valid values: 0.01 to 1.

- Directed path Crawler identification algorithm (**PR**) the corresponding configuration information shall contain the following sub-parameters:
  - **keyPathConfiguration**: Required. The request path. You can specify a maximum of 10 Paths. This parameter is required only when a Crawler identification algorithm is used. Data type: array.The parameters must be in a JSON string. The following parameters must be included:
    - **Method**: Required. The request method. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, **OPTIONS**.
    - **URL**: Required. The request path keyword, which must start with a forward slash (/). Data Type: String.
    - **matchType**: Required. The matching method. This parameter must be the same as the request path keyword (**URL** parameter in combination with the specified request path. Optional values: **all**(Precise matching), **prefix**(Prefix matching), **regex**(Regular expression matching).
  - **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests are detected. Data type: Integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.
  - **minRatio**: Required. The criteria for determining the risk, that is, the proportion of requests sent by an IP address to the specified resource (this corresponds to the crawler detection algorithm for special resources.) the proportion of

requests sent by IP addresses to the specified path. This value exceeds the threshold. Valid values: 0.01 to 1.

- Parameter polling Crawler identification algorithm (**DPR**) the corresponding configuration information shall contain the following sub-parameters:
  - **Method**: Required. The request method. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, **OPTIONS**.
  - **urlPattern**: Required. The path of the key parameter, which must start with a forward slash (/). Data type: string. Key parameters are indicated by braces ({}). When multiple braces ({}) are set, these parameters are joined as key parameters. For example, `/company/{}/{}/{}/user.php? uid={}` .
  - **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests are detected. Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.
  - **minRatio**: Required. The risk determination condition. If the value of a key parameter exceeds the threshold, the request is considered as a risk. A value of 0.01 to 1 indicates a risk.
- Dynamic IP Crawler identification algorithm (**SR**) the corresponding configuration information shall contain the following sub-parameters:
  - **maxRequestCountPerSrSession**: Required. It specifies the minimum number of requests in each session. If the number of requests in each session is smaller than the value of this parameter, a session is abnormal. Valid values: 1 to 8.
  - **minSrSessionCountPerIp**: Required. The risky condition. The value is the threshold for the number of abnormal sessions in an IP access request. If the

number of abnormal sessions exceeds this threshold, a risk is detected. Valid values: 5 to 300.

- Proxy Crawler identification algorithm (**IND**) the corresponding configuration information shall contain the following sub-parameters:
  - **minIpCount**: Required. The condition for determining the number of IP addresses associated with the Wi-Fi connection of a malicious device. If the threshold is exceeded, a risk is detected. Valid values: 5 to 500.
  - **keyPathConfiguration**: The detection path information. You can specify up to 10 paths. Data type: array. The parameters must be in a JSON string. The following parameters must be included:
    - **Method**: Required. The request method. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, **OPTIONS**.
    - **URL**: Required. The keyword of the detection path, which must start with a forward slash (/). Data type: string.
    - **matchType**: Required. The matching method. This parameter must be the same as the keyword of the detection path (**URL** parameter in combination with the specified request path. Optional values: **all**(Precise matching), **prefix**(Prefix matching), **regex**(Regular expression matching).
- Periodic Crawler identification algorithm (**Periodicity**) the corresponding configuration information shall contain the following sub-parameters:
  - **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests are detected. Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.
  - **level**: Required. The risk level of the Accessed IP address. It indicates the visibility of the periodic features of the IP address. Data type: Integer. Valid values:
    - **0**: indicates obvious
    - **1**: Medium
    - **2**: indicates weak.

- **Sample request**

```
{
  "name":"proxy Crawler identification",
  "algorithmName":"IND",
```

```
    "timeInterval":"60",
    "action":"warn",
    "config":{
      "minIpCount":5,
      "keyPathConfiguration":[{"url":"/index","method":"GET","matchType":"prefix"}]
    }
  }
```

- Version protection rule configuration for App protection (**bot_wxbb_pkg**) corresponding to the JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
    - **Test**: indicates observation.
    - **Close**: indicates the block.
  - **nameList**: Required. The version information. You can specify up to five rules. Data type: array. The parameter is represented as a JSON string, which includes the following parameters:
    - **Name**: Required. The name of the valid package. Data type: string.
    - **signList**: Required. The maximum number of package signatures. You can specify up to 15. Separate multiple signatures with commas (,). Data type: array.
  - **Sample request**

```
{
  "name":"test",
  "action":"close",
  "nameList":[{
    "name":"apk-xxxx",
    "signList":["xxxxxx","xxxxx","xxxx","xx"]
  }]
}
```

- Configure the path protection rule for App protection **bot_wxbb**) corresponding to the JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **uri**: Required. The path, which must start with a forward slash (/). Data type: string.
  - **matchType**: Required. The matching method. Data type: string. Optional values: **all** (Precise matching), **prefix**(Prefix matching), **regex**(Regular expression matching).
  - **Arg**: Required. The parameter value. Data type: String. Together with the **matchType** parameter specify protected path configuration.
  - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
    - **Test**: indicates observation.
    - **Close**: indicates the block.
  - **hasTag**: Required. Data type: Boolean. You must specify whether to sign the fields.
    - **true**: indicates yes. When you select fields that require custom signing, you must set the **wxbbVmpFieldType** and **wxbbVmpFieldValue** parameters to specify the type and value of the field that you want to sign.
    - **false**: indicates no.
  - **wxbbVmpFieldType**: Optional. The type of the user-defined field. Data type: integer. When the **hasTag** parameter value is **true**, you must specify the parameter. Set the value to:
    - **0**: indicates the header.
    - **1**: represents the parameter.
    - **2**: indicates a cookie.
  - **wxbbVmpFieldValue**: Optional. The value of the user-defined field. Data type: string. When the **hasTag** parameter value is **true**, you must specify the parameter.
  - **blockInvalidSign**: Required. The action to be taken against the invalid signature. Data type: integer. Static value: **1**. The default protection policies of the path protection rule.
  - **blockProxy**: Optional. The processing method of the proxy. Data type: integer. Static value: **1**. This parameter is not required if you do not need to perform the action on the proxy behavior.

- **blockSimulator**: Optional. It indicates whether to perform the action on the simulator. Static value:**1**. This parameter is not required if you do not need to perform the action on the simulator behavior.
- **Sample request**

```
{
  "name":"test",
  "uri":"/index",
  "matchType":"all",
  "arg":"test",
  "action":"close",
  "hasTag":true,
  "wxbbVmpFieldType":2,
  "wxbbVmpFieldValue":"test",
  "blockInvalidSign":1,
  "blockProxy":1
}
```

- To modify a custom protection policy, set DefenseType to **ac_custom**, and set the **scene** parameter in the JSON string to modify an ACL or HTTP flood protection rule.
  - To modify an ACL rule, set **scene** to **custom_acl**, and construct a JSON string that includes the following parameters.
    - **name**: Required. The name of the rule. Data type: string.
    - **scene**: Required. The type of the protection policy. Data type: string. If you need to modify an ACL rule, set the value to **custom_acl**.
    - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
      - **monitor**: monitors requests
      - **captcha**: requires CAPTCHA verification
      - **captcha_strict**: requires more strict CAPTCHA verification
      - **js**: requires JavaScript verification
      - **block**: blocks requests
    - **Conditions**: Required. The matching conditions. You can specify up to five matching conditions. Data type: Array. Describe the rate in a JSON string that includes the following parameters:
      - **Key**: the matching field. Valid values: **URL**, **IP**, **Referer**, **user-Agent**, **Params**, **Cookie**, **content-Type**, **content-Length**, **x-Forwarded-For**, **post-Body**, **http-Method**, **Header**, **URLPath**.
      - **opCode**: The logical operator. Valid values:
        - **0**: does not include
        - **1**: includes
        - **2**: does not exist
        - **10**: does not equal
        - **11**: equals
        - **20**: length smaller than
        - **21**: length equals
        - **22**: length greater than
        - **30**: value smaller than
        - **31**: value equals

- **32**: value greater than
- **40**: does not belong to
- **41**: belongs to

- **values**: The matching content. Set the content as required, in String format.

> **Note:**
> The logical operator in the matching condition (**opCode**) and the values of the matching content (**values**) must be set based on the specified matching field (**key**). For more information about matching condition configurations, see matching Condition fields.

- **Sample request**

```
{
  "action":"monitor",
  "name":"test",
  "scene":"custom_acl",
  "conditions":[{"opCode":1,"key":"URL","values":"/example"}]
}
```

- Set HTTP flood protection rules (**scene** the parameter value is **custom_cc**), the corresponding JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **scene**: Required. The type of the protection policy. Data type: string. If you need to modify a protection rule against HTTP flood attacks, set the value to **custom_cc**.
  - **Conditions**: Required. The matching conditions. You can specify up to five matching conditions. Data type: array. Describe the rate in a JSON string that includes the following parameters:
    - **Key**: the matching field. Valid values: **URL**, **IP**, **Referer**, **user-Agent**, **Params**, **Cookie**, **content-Type**, **content-Length**, **x-Forwarded-For**, **post-Body**, **http-Method**, **Header**, **URLPath**.
    - **opCode**: The logical operator. Valid values:
      - **0**: does not include
      - **1**: includes
      - **2**: does not exist
      - **10**: does not equal
      - **11**: equals
      - **20**: length smaller than
      - **21**: length equals
      - **22**: length greater than
      - **30**: value smaller than
      - **31**: value equals
      - **32**: value greater than
      - **40**: does not belong to
      - **41**: belongs to
    - **values**: The matching content. Set the content as required, in String format.

      Note:

The logical operator in the matching condition (**opCode**) and the values of the matching content (**values**) must be set based on the specified matching field (**key**).

- **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
  - **monitor**: monitors requests
  - **captcha**: requires CAPTCHA verification
  - **captcha_strict**: requires more strict CAPTCHA verification
  - **js**: requires JavaScript verification
  - **block**: block requests
- **ratelimit**: Required. The maximum request rate from an object. Data type: JSON. Describe the rate in a JSON string that includes the following parameters:
  - **target**: Required. The type of the object whose request rate is calculated. Data type: string. Valid values:
    - **remote_addr**: IP addresses.
    - **cookie.acw_tc**: sessions.
    - **queryarg**: custom parameters. If you choose to use custom parameters, specify the name of the object in the **subkey** parameter.
    - **cookie**: custom cookies. If you choose to use custom cookies, specify the cookie content in the **subkey** parameter.
    - **header**: custom headers. If you choose to use custom headers, specify the header content in the **subkey** parameter.
  - **subkey**: Optional. When **target** is set to **cookie**, **header**, or **queryarg**, you must specify the required information in the **subkey** parameter. Data type: string.
  - **interval**: Required. The time period (in seconds) during which the number of requests from the specified object is calculated. This parameter must be used together with the **threshold** parameter. Data type: integer.
  - **threshold**: Required. During the specified time period, the maximum number of requests that are allowed from an individual object. Data type: integer.
  - **status**: Optional. The maximum number of an HTTP status code. Data type: string. It is described in a JSON string that contains the following parameters:
    - **code**: Required. The specified HTTP status code. Data type: integer.

- **Count**: Optional. It indicates the occurrence threshold. If the number of occurrences exceeds the threshold, a protection rule is hit. Valid values:[1, 999999999].**Count** parameters and **ratio** you can select either parameter.
- **Ratio**: Optional. The threshold (in percentage) of the response code. If the occurrence ratio of a specified response code exceeds this threshold, the rule is hit. Valid values:[1,100].**Count** parameters and **ratio** you can select either parameter.

- **scope**: Required. This parameter specifies where the settings take effect. Data type: string. Valid values:
  - **rule**: objects that match the specified conditions.
  - **domain**: domains where the rule is applied.
- **TTL**: Required. The validity period of the action. Unit: Seconds. Data type: Integer. Valid values:[60,86400].

- **Sample request**

```
{
  "name":"HTTP flood protection",
  "conditions":[{"opCode":1,"key":"URL","values":"/example"}],
  "action":"block",
  "scene":"custom_cc",
  "ratelimit":{
    "target": "remote_addr",
    "interval": 300,
    "threshold": 2000,
    "status": {
      "code": 404,
      "count": 200
    },
    "scope": "rule",
    "ttl": 1800
  }
}
```

- Website whitelist rule configuration (**whitelist**) corresponding to the JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **tags**: Required. The protection modules that can be skipped. You can specify multiple modules. Valid values:
    - **waf**: the website whitelist
    - **cc**: system HTTP flood protection
    - **customrule**: custom rules
    - **blacklist**: the IP blacklist
    - **antiscan**: anti-scan protection
    - **regular**: web application protection
    - **deeplearning**: deep learning
    - **antifraud**: data risk control
    - **dlp**: data leakage prevention
    - **tamperproof**: tamper protection
    - **bot_intelligence**: indicates bot threat intelligence.
    - **bot_algorithm**: indicates an intelligent algorithm.
    - **bot_wxbb**: indicates App protection.
  - **Conditions**: Required. The matching conditions. You can specify up to five matching conditions. Data type: array. Describe the rate in a JSON string that includes the following parameters:
    - **Key**: the matching field. Valid values: **URL**, **IP**, **Referer**, **user-Agent**, **Params**, **Cookie**, **content-Type**, **content-Length**, **x-Forwarded-For**, **post-Body**, **http-Method**, **Header**, **URLPath**.
    - **opCode**: The logical operator. Valid values:
      - **0**: does not include
      - **1**: includes
      - **2**: does not exist
      - **10**: does not equal
      - **11**: equals
      - **20**: length smaller than
      - **21**: length equals

- **22**: length greater than
- **30**: value smaller than
- **31**: value equals
- **32**: value greater than
- **40**: does not belong to
- **41**: belongs to

- **values**: The matching content. Set the content as required, in String format.

> **Note:**
> The logical operator in the matching condition (**opCode**) and the values of the matching content (**values**) must be set based on the specified matching field (**key**).

- **Sample request**

```
{
   "name": "test",
   "tags": ["cc","customrule"],
   "conditions":[{"opCode":1,"key":"URL","values":"/example"}],
}
```

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=CreateProtectionModuleRule
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&DefenseType=ac_custom
&Rule= {"action":"monitor","name":"test","scene":"custom_acl","conditions":[{"opCode":1,"
key":"URL","values":"/example"}]}
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
  "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.6.8 ModifyProtectionModuleRule

You can call this operation to modify the rules of a Web Application Firewall (WAF) protection module, such as web intrusion prevention, data security, advanced protection, anti-Bot, access control and throttling, and whitelist.

You can set the **DefenseType** parameter to specify the protection module. For more information about the values of this parameter, see the description of **DefenseType** in the following section.

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	Boolean	No	ModifyProtectionModuleRule	The operation that you want to perform. Set the value to **ModifyProtectionModuleRule**.

Parameter	Type	Required	Example	Description
DefenseType	String	No	ac_custom	Specify the protection module. Valid values: • **tamperproof**: tamper protection. • **dlp**: data leakage prevention. • **ng_account**: account security rule configuration • **bot_intelligence**: Bot Threat Intelligence configuration • **antifraud**: data risk control • **antifraud_js**: data risk control JavaScript • **bot_algorithm**: intelligent algorithm rules for Bot management • **bot_wxbb_pkg**: version protection rules for App protection • **bot_wxbb**: path protection rules for App protection • **ac_blacklist**: IP blacklist • **ac_highfreq**: IP blocking based on the request rate • **block_dirscan**: directory traversal • **ac_custom**: custom protection policies • **whitelist**: whitelist
Domain	String	No	www.example.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.

Parameter	Type	Required	Example	Description
LockVersion	Long	Yes	env	The version of the configuration to be modified.
Rule	String	No	{"action":"monitor","name":"test","scene":"custom_acl","conditions":[{"opCode":1,"key":"URL","values":"/example"}]}	The content of the rule. It is a JSON string that contains multiple parameters. **Note:** According to the specified protection function module configuration (**DefenseType**), the specific parameters involved vary. For more information, see Rule parameters.
RuleId	Long	Yes	369998	The ID of the rule.

Rule parameters

- To modify a tamper protection rule, set DefenseType to **tamperproof** and construct a JSON string that includes the following parameters:
  - **uri**: Required. The URL that needs protection. Data type: string.
  - **name**: Required. The name of the rule. Data type: string.
  - **status**: Optional. The protection status of the rule. Data type: integer.
    - **0**: disabled (default).
    - **1**: enabled.
  - **Sample request**

```
{
  "name":"example",
  "uri":"http://www.example.com/example",
  "Status":1
}
```

- To modify a data leakage prevention rule, set DefenseType to **dlp** and construct a JSON string that includes the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **conditions**: Required. The matching condition, which is described in a JSON string. You can specify up to two conditions that have the AND logical relation to apply the conditions at the same time. Data type: array. The array must include the following parameters:
    - **key**: The matching items.
      - **0**: Sets the matching item to URLs.
      - **10**: indicates sensitive information.
      - **11**: indicates the response code.

        Note:

You cannot set HTTP status codes (**11**) and sensitive information (**10**) as the matching conditions in the **conditions** parameter at the same time.

- **operation**: The matching logic. This value is set to **1** by default, which specifies the INCLUDES logical operator.
- **value**: The matching condition values, which are formulated in a JSON string. You can specify multiple values. The JSON string must include the following parameters:
  - **v**: only applies to scenarios where the matching condition (**key**) is set to URLs (**0**) or HTTP status codes (**11**).
    - URL: when`"key":0` the parameter value is the URL address.
    - Response Code: when`"key":11` valid values for the parameter include**400**,**401**,**402**,**403**,**404**,**405-499**,**500**,**501**,**502**,**503**,**504**,**505-599**.
  - **k**: only applies to scenarios where the matching item (**key**) is set to sensitive information (**10**). Valid values:
    - **100**: masks resident ID card numbers.
    - **101**: masks credit card numbers.
    - **102**: masks phone numbers.
    - **103**: masks the default sensitive words.
- **action**: The matching action.
  - **3**: sets the matching action to warn.
  - **10**: filters sensitive information. This action only applies to scenarios where sensitive information is contained (`"key":10`) to find matching conditions.
  - **11**: indicates that the system returns to the built-in intercept page, this action only applies to response codes (`"key":11`) to find matching conditions.
- **Sample request**

```
 {
  "name":"example",
  "conditions":[{"key":11,"operation":1,"value":[{"v":401}]},{"key":"0","operation":1,"
value":[{"v":"www.example.com"}]}],
  "action":3
 }
```

- Configure account security rules (**ng_account**) corresponding to the JSON string contains the following parameters:
  - **url_path**: Required. The URL to the operation that runs detection tasks. The URL must start with a slash (/). Data type: string.
  - **Method**: The request method to be moderated. Valid values: POST, GET, PUT, and DELETE. Data Type: String. You can set multiple request methods. Separate multiple request methods with commas (,).
  - **account_left**: Required. The parameter that specifies the account. Data type: string.
  - **password_left**: Optional. The password of the account. Data type: string.
  - **Action**: (required) The protection action. Valid values:
    - **Monitor**: indicates an alert.
    - **Block**: indicates interception.
  - **Sample request**

```
{
   "url_path":"/example",
   "method":"POST,GET,PUT,DELETE",
   "account_left":"aaa",
   "password_left:" 123 ",
   "action":"monitor"
}
```

- Bot Threat Intelligence configurations (**bot_intelligence**) corresponding to the JSON string contains the following parameters:
  - **Name**: Required. The rule name. It must be consistent with the rule ID (**RuleId**) parameter. Data type: string.
  - **urlList**: Required. The protected paths. You can specify a maximum of ten protected paths. Data type: array. The code is represented as a JSON string, which includes the following parameters:
    - **Mode**: Required. The matching method. This parameter must be the same as the path keyword (**URL**) parameter in combination with the specified protected path.

Optional values: **EQ**(Precise matching), **prefix-match**(Prefix matching), **regex** (Regular expression matching).

- **URL**: Required. The path keyword, which must start with a forward slash (/). Data Type: string.

- **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
  - **monitor**: monitors requests
  - **captcha**: requires CAPTCHA verification
  - **captcha_strict**: indicates the strict slider.
  - **JS**: indicates JavaScript validation.
  - **block**: blocks requests
- **Status**: Required. The status of the instance. Valid values: integer.
  - **0**: disables the rule.
  - **1**: enables the rule.
- **Sample request**

```
{
  "urlList":[
    {"mode":"prefix-match","url":"/indexa"},
    {"mode":"regex","url":"/"},
    {"mode":"eq","url":"/"}],
  "name":"IDC IP Address Library-Tencent Cloud",
  "action":"captcha_strict",
  "Status":1
}
```

- Bot management intelligent algorithm rule configuration (**bot_algorithm**) corresponding to the JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **algorithmName**: Required. The name of the algorithm. Valid values:
    - **RR**: indicates the crawler identification algorithm for special resources.
    - **PR**: indicates the targeted path Crawler identification algorithm.
    - **DPR**: indicates the round-robin Crawler identification algorithm.
    - **SR**: indicates the dynamic IP Crawler identification algorithm.
    - **IND**: indicates the proxy Crawler identification algorithm.
    - **Periodicity**: indicates the periodic crawler recognition algorithm.
  - **timeInterval**: Required. The detection period. Valid values: 30, 60, 120, 300, and 600. Unit: Seconds. Data type: integer.
  - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
    - **Monitor**: indicates observation.
    - **CAPTCHA**: indicates the slider.
    - **JS**: indicates JavaScript validation.
    - **Block**: indicates the block. When blocking is selected as the disposal action, the blocking duration (**blocktime**) parameter.
  - **blocktime**: Optional. The blocking duration. Unit: Minutes. Value range: 1 to 600.
  - **config**: Required. The algorithm configuration, in JSON format. Data type: string. The specific sub-parameters in the algorithm configuration and the selected algorithm name (**algorithmName**) related.
    - Crawler identification algorithm for special resources (**RR**) the corresponding configuration information shall contain the following sub-parameters:
      - **resourceType**: The type of the requested resource. Data type: integer. Valid values:
        - **1**: represents a dynamic resource type.
        - **2**: represents a static resource type.

- **-1**: indicates custom resource types. If you select a custom Resource Group, **extensions** the parameter that specifies the resource suffix in string format. Separate multiple file extensions with commas (,), for example, `css,jpg,xls`.
- **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests are detected. Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.
- **minRatio**: Required. The risk determination condition. A risk is determined when the proportion of requests sent by an IP address exceeds the threshold. Valid values: 0.01 to 1.

- Directed path Crawler identification algorithm (**PR**) the corresponding configuration information shall contain the following sub-parameters:
  - **keyPathConfiguration**: The request path. You can specify a maximum of 10 Paths. This parameter is required only when a Crawler identification algorithm is used. Data type: array. The parameters must be in a JSON string. The following parameters must be included:
    - **Method**: Required. The request method. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, **OPTIONS**.
    - **URL**: Required. The request path keyword, which must start with a forward slash (/). Data type: string.
    - **matchType**: Required. The matching method. This parameter must be the same as the request path keyword (**URL** parameter in combination with the specified request path. Valid values: **all**(Precise matching), **prefix**(Prefix matching), **regex**(Regular expression matching).
  - **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests are detected.

Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.

- **minRatio**: Required. The risk determination condition. A risk is determined when the proportion of requests sent from an IP address to the specified path exceeds the threshold. Valid values: 0.01 to 1.

- Parameter polling Crawler identification algorithm (**DPR**) the corresponding configuration information shall contain the following sub-parameters:
  - **Method**: Required. The request method. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, **OPTIONS**.
  - **urlPattern**: Required. The path of the key parameter, which must start with a forward slash (/). Data type: string. Key parameters are indicated by braces ({}). When multiple braces ({}) are set, these parameters are joined as key parameters. For example, `/company/{}/{}/{}/user.php? uid={}` .
  - **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests are detected. Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.
  - **minRatio**: Required. The risk determination condition. If the value of a key parameter exceeds the threshold, the request is considered as a risk. A value of 0.01 to 1 indicates a risk. (required)
- Dynamic IP Crawler identification algorithm (**SR**) the corresponding configuration information shall contain the following sub-parameters:
  - **maxRequestCountPerSrSession**: Required. It specifies the minimum number of requests in each session. If the number of requests in each session is smaller than the value of this parameter, a session is abnormal. Valid values: 1 to 8.
  - **minSrSessionCountPerIp**: Required. The risky condition. The value is the threshold for the number of abnormal sessions in an IP access request. If the

number of abnormal sessions exceeds this threshold, a risk is detected. Valid values: 5 to 300.

- Proxy Crawler identification algorithm (**IND**) the corresponding configuration information shall contain the following sub-parameters:
  - **minIpCount**: Required. The condition for determining the number of IP addresses associated with the Wi-Fi connection of a malicious device. If the threshold is exceeded, a risk is detected. Valid values: 5 to 500.
  - **keyPathConfiguration**: The detection path information. You can specify up to 10 paths. Data type: array. The parameters must be in a JSON string. The following parameters must be included:
    - **Method**: Required. The request method. Valid values: **POST**, **GET**, **PUT**, **DELETE**, **HEAD**, **OPTIONS**.
    - **URL**: Required. The keyword of the detection path, which must start with a forward slash (/). Data type: string.
    - **matchType**: Required. The matching method. This parameter must be the same as the keyword of the detection path (**URL** parameter in combination with the specified request path. Valid values: **all**(Precise matching), **prefix** (Prefix matching), **regex**(Regular expression matching).
- Periodic Crawler identification algorithm (**Periodicity**) the corresponding configuration information shall contain the following sub-parameters:
  - **minRequestCountPerIp**: Required. The IP address range in the detection period. Only IP addresses that have a specified number of access requests are detected. Data type: integer. This parameter specifies the minimum number of requests. Valid values: 5 to 10000.
  - **level**: Required. The risk level of the Accessed IP address. It indicates the visibility of the periodic features of the IP address. Data type: Integer. Valid values:
    - **0**: indicates obvious
    - **1**: Medium
    - **2**: indicates weak.

- **Sample request**

```
{
  "name":"proxy Crawler identification",
  "algorithmName":"IND",
```

```
    "timeInterval":"60",
    "action":"warn",
    "config":{
      "minIpCount":5,
      "keyPathConfiguration":[{"url":"/index","method":"GET","matchType":"prefix"}]
    }
  }
```

- Version protection rule configuration for App protection (**bot_wxbb_pkg**) corresponding to the JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
    - **Test**: indicates observation.
    - **Close**: indicates the block.
  - **nameList**: Required. The version information. You can specify up to five rules. Data type: array. The parameter is represented as a JSON string, which includes the following parameters:
    - **Name**: Required. The name of the valid package. Data type: string.
    - **signList**: Required. The maximum number of package signatures. You can specify up to 15. Separate multiple signatures with commas (,). Data type: array.
  - **Sample request**

```
{
  "name":"test",
  "action":"close",
  "nameList":[{
    "name":"apk-xxxx",
    "signList":["xxxxxx","xxxxx","xxxx","xx"]
  }]
}
```

- Configure the path protection rule for App protection **bot_wxbb**) corresponding to the JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **uri**: Required. The path, which must start with a forward slash (/). Data type: string.
  - **matchType**: Required. The matching method. Data type: string. Valid values: **all** (Precise matching), **prefix**(Prefix matching), **regex**(Regular expression matching).
  - **Arg**: Required. The parameter value defines the specified protected path configuration with the **matchType** parameter. Data type: string.
  - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
    - **Test**: Indicates the observation.
    - **Close**: Indicates the block.
  - **hasTag**: Required. Data type: boolean. You must specify whether to sign the fields.
    - **true**: indicates yes. When you select fields that require custom signing, you must pass in **wxbbVmpFieldType** and **wxbbVmpFieldValue** the parameters specify the type and value of the field that you want to sign.
    - **false**: indicates no.
  - **wxbbVmpFieldType**: Optional. The type of the user-defined field. Data type: Integer. When the **hasTag** parameter value is **true** you must specify the parameter. Valid values:
    - **0**: indicates the header.
    - **1**: represents the parameter.
    - **2**: indicates a cookie.
  - **wxbbVmpFieldValue**: Optional. The value of the user-defined field. Data type: string. When the **hasTag** parameter value is **true**, you must specify the parameter.
  - **blockInvalidSign**: Required. The action to be taken against the invalid signature. Data type: integer. Static value: **1**. The default protection policies of the path protection rule.
  - **blockProxy**: Required. The processing method of the proxy. Data type: integer. Static value: **1**. This parameter is not required if you do not need to perform the action on the proxy behavior.

- **blockSimulator**: Required. Indicates whether to perform the action on the simulator. Data type: integer. Static value: **1**. This parameter is not required if you do not need to perform the action on the simulator behavior.
- **Sample request**

```
{
  "name":"test",
  "uri":"/index",
  "matchType":"all",
  "arg":"test",
  "action":"close",
  "hasTag":true,
  "wxbbVmpFieldType":2,
  "wxbbVmpFieldValue":"test",
  "blockInvalidSign":1,
  "blockProxy":1
}
```

- To modify a data risk control request, set DefenseType to **antifraud** and construct a JSON string that includes the following parameters:
  - **uri**: Required. The request URL. Data type: string.
  - **Sample request**

```
{
  "uri": "http://1.example.com/example"
}
```

- To modify the data risk control JavaScript that is inserted into a web page, set DefenseType to **antifraud_js** and construct a JSON string that includes the following parameters:
  - **uri**: Required. The URL of the web page into which you want to insert the data risk control JavaScript. The system inserts data risk control JavaScript into all the pages under the specified URL directory. Data type: string.
  - **Sample request**

```
{
  "uri": "/example/example"
}
```

- To modify an IP blacklist rule, set DefenseType to **ac_blacklist**, and construct a JSON string that contains the following parameters:

  > **Note:**
  > You cannot call API operations to block regions. Use this feature in the console.

  - **remoteAddr**: Required. The IP addresses in the blacklist. You can specify IP addresses and CIDR blocks. Separate IP addresses with commas (,). You can add up to 200 IP addresses to the blacklist. Data type: array. If no value is specified, it indicates that the blacklist is empty.
  - **Sample request**

    ```
    {
      "remoteAddr":["1.1.1.1","12.11.1.2"]
    }
    ```

- To modify the rule that automatically blocks IP addresses initiating attacks, set DefenseType to **ac_highfreq**, and construct a JSON string that contains the following parameters:

  - **Interval**: Required. The time range to be detected, in seconds. Data type: integer. Valid values:[5,1800].
  - **TTL**: Required. The duration of blocked IP addresses. Unit: Seconds. Data type: integer. Valid values:[60,86400].
  - **count**: Required. The maximum number of requests allowed from an IP address. If the number of requests initiated from an IP address during the specified time period exceeds this limit, the IP address is blocked. Data type: integer. Valid values: [2,50000].
  - **Sample request**

    ```
    {
      "interval":60,
      "ttl":300,
      "count":60
    }
    ```

- To modify a directory traversal protection rule, set DefenseType to **block_dirscan** and construct a JSON string that includes the following parameters:
  - **Interval**: Required. The time range to be detected, in seconds. Valid values:[5,1800].
  - **TTL**: Required. The duration of blocked IP addresses. Unit: Seconds. Valid values:[60, 86400].
  - **Count**: Required. The number of visits. Valid values:[2,50000].
  - **Weight**: Required. The threshold of HTTP status codes 404 (as a percentage). Valid values:(0,1].
  - **uriNum**: Required. The threshold of the number of directories to be scanned. Valid values:[2,50000].
  - **Sample request**

```
{
    "interval":10,
    "ttl":1800,
    "count":50,
    "weight":0.7,
    "uriNum":20
}
```

- To modify a custom protection policy, set DefenseType to **ac_custom**, and set the **scene** parameter in the JSON string to modify an ACL or HTTP flood protection rule.
  - To modify an ACL rule, set **scene** to **custom_acl**, and construct a JSON string that includes the following parameters.
    - **name**: Required. The name of the rule. Data type: string.
    - **scene**: Required. The type of the protection policy. Data type: string. If you need to modify an ACL rule, set the value to **custom_acl**.
    - **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
      - **monitor**: monitors requests
      - **captcha**: requires CAPTCHA verification
      - **captcha_strict**: requires more strict CAPTCHA verification
      - **js**: requires JavaScript verification
      - **block**: blocks requests
    - **Conditions**: Required. The matching conditions. You can specify up to five matching conditions. Data type: array. Describe the rate in a JSON string that includes the following parameters:
      - **Key**: the matching field. Valid values: **URL**, **IP**, **Referer**, **user-Agent**, **Params**, **Cookie**, **content-Type**, **content-Length**, **x-Forwarded-For**, **post-Body**, **http-Method**, **Header**, **URLPath**.
      - **opCode**: The logical operator. Valid values:
        - **0**: does not include
        - **1**: includes
        - **2**: does not exist
        - **10**: does not equal
        - **11**: equals
        - **20**: length smaller than
        - **21**: length equals
        - **22**: length greater than
        - **30**: value smaller than
        - **31**: value equals

- **32**: value greater than
- **40**: does not belong to
- **41**: belongs to

- **values**: The matching content. Set the content as required, in String format.

> **Note:**
> The logical operator in the matching condition (**opCode**) and the values of the matching content (**values**) must be set based on the specified matching field (**key**). For more information about matching condition configurations, see matching Condition fields.

- **Sample request**

```
{
  "action":"monitor",
  "name":"test",
  "scene":"custom_acl",
  "conditions":[{"opCode":1,"key":"URL","values":"/example"}]
}
```

- Set HTTP flood protection rules (**scene** the parameter value is **custom_cc**), the corresponding JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **scene**: Required. The type of the protection policy. Data type: string. If you need to modify a protection rule against HTTP flood attacks, set the value to **custom_cc**.
  - **Conditions**: Required. The matching conditions. You can specify up to five matching conditions. Data type: array. Describe the rate in a JSON string that includes the following parameters:
    - **Key**: the matching field. Valid values: **URL**, **IP**, **Referer**, **user-Agent**, **Params**, **Cookie**, **content-Type**, **content-Length**, **x-Forwarded-For**, **post-Body**, **http-Method**, **Header**, **URLPath**.
    - **opCode**: The logical operator. Valid values:
      - **0**: does not include
      - **1**: includes
      - **2**: does not exist
      - **10**: does not equal
      - **11**: equals
      - **20**: length smaller than
      - **21**: length equals
      - **22**: length greater than
      - **30**: value smaller than
      - **31**: value equals
      - **32**: value greater than
      - **40**: does not belong to
      - **41**: belongs to
    - **values**: The matching content. Set the content as required, in String format.

      Note:

The logical operator in the matching condition (**opCode**) and the values of the matching content (**values**) must be set based on the specified matching field (**key**).

- **action**: Required. The action performed after the rule is matched. Data type: string. Valid values:
  - **monitor**: monitors requests
  - **captcha**: requires CAPTCHA verification
  - **captcha_strict**: requires more strict CAPTCHA verification
  - **js**: requires JavaScript verification
  - **block**: block requests
- **ratelimit**: Required. The maximum request rate from an object. Data type: JSON. Describe the rate in a JSON string that includes the following parameters:
  - **target**: Required. The type of the object whose request rate is calculated. Data type: string. Valid values:
    - **remote_addr**: IP addresses.
    - **cookie.acw_tc**: sessions.
    - **queryarg**: custom parameters. If you choose to use custom parameters, specify the name of the object in the **subkey** parameter.
    - **cookie**: custom cookies. If you choose to use custom cookies, specify the cookie content in the **subkey** parameter.
    - **header**: custom headers. If you choose to use custom headers, specify the header content in the **subkey** parameter.
  - **subkey**: Optional. When **target** is set to **cookie**, **header**, or **queryarg**, you must specify the required information in the **subkey** parameter. Data type: string.
  - **interval**: Required. The time period (in seconds) during which the number of requests from the specified object is calculated. This parameter must be used together with the **threshold** parameter. Data type: integer.
  - **threshold**: Required. During the specified time period, the maximum number of requests that are allowed from an individual object. Data type: integer.
  - **status**: Optional. The maximum number of an HTTP status code. Data type: string. It is described in a JSON string that contains the following parameters:
    - **code**: Required. The specified HTTP status code. Data type: integer.

- **Count**: Optional. It indicates the occurrence threshold. If the number of occurrences exceeds the threshold, a protection rule is hit. Valid values:[1, 999999999].**Count** parameters and **ratio** you can select either parameter.
- **Ratio**: Optional. The threshold (in percentage) of the response code. If the occurrence ratio of a specified response code exceeds this threshold, the rule is hit. Valid values:[1,100]. You can select either**Count** and **ratio** parameters.

- **scope**: Required. This parameter specifies where the settings take effect. Data type: string. Valid values:
  - **rule**: objects that match the specified conditions.
  - **domain**: domains where the rule is applied.
- **ttl**: Required. The effective time period (in seconds) of the action. Data type: integer. Valid values: 60, 86400.

- **Sample request**

```
{
    "name":"HTTP flood protection",
    "conditions":[{"opCode":1,"key":"URL","values":"/example"}],
    "action":"block",
    "scene":"custom_cc",
    "ratelimit":{
      "target": "remote_addr",
      "interval": 300,
      "threshold": 2000,
      "status": {
        "code": 404,
        "count": 200
      },
      "scope": "rule",
      "ttl": 1800
    }
}
```

- Website whitelist rule configuration (**whitelist**) corresponding to the JSON string contains the following parameters:
  - **name**: Required. The name of the rule. Data type: string.
  - **tags**: Required. The protection modules that can be skipped. You can specify multiple modules. Valid values:
    - **waf**: the website whitelist
    - **cc**: system HTTP flood protection
    - **customrule**: custom rules
    - **blacklist**: the IP blacklist
    - **antiscan**: anti-scan protection
    - **regular**: web application protection
    - **deeplearning**: deep learning
    - **antifraud**: data risk control
    - **dlp**: data leakage prevention
    - **tamperproof**: tamper protection
    - **bot_intelligence**: indicates bot threat intelligence.
    - **bot_algorithm**: indicates an intelligent algorithm.
    - **bot_wxbb**: indicates App protection.
  - **Conditions**: Required. The matching conditions. You can specify up to five matching conditions. Data type: array. Describe the rate in a JSON string that includes the following parameters:
    - **Key**: the matching field. Valid values: **URL**, **IP**, **Referer**, **user-Agent**, **Params**, **Cookie**, **content-Type**, **content-Length**, **x-Forwarded-For**, **post-Body**, **http-Method**, **Header**, **URLPath**.
    - **opCode**: The logical operator. Valid values:
      - **0**: does not include
      - **1**: includes
      - **2**: does not exist
      - **10**: does not equal
      - **11**: equals
      - **20**: length smaller than
      - **21**: length equals

- **22**: length greater than
- **30**: value smaller than
- **31**: value equals
- **32**: value greater than
- **40**: does not belong to
- **41**: belongs to

- **values**: The matching content. Set the content as required, in String format.

> **Note:**
> The logical operator in the matching condition (**opCode**) and the values of the matching content (**values**) must be set based on the specified matching field (**key**).

- **Sample request**

```
{
   "name": "test",
   "tags": ["cc","customrule"],
   "conditions":[{"opCode":1,"key":"URL","values":"/example"}],
}
```

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=ModifyProtectionModuleRule
&DefenseType=ac_custom
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&LockVersion=2
&Rule={"action":"monitor","name":"test","scene":"custom_acl","conditions":[{"opCode":1,"
key":"URL","values":"/example"}]}
&RuleId=369998
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

JSON format

```
{
  "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.6.9 ModifyProtectionRuleStatus

Call the ModifyProtectionRuleStatus API to enable or disable the WAF protection features for the specified domain, including website tamper-proofing, legitimate crawler defense, crawler threat intelligence, custom protection policies, and website whitelist.

You can set the **DefenseType** parameter to specify the protection module. For more information about the values of this parameter, see the description of **DefenseType** in the following section.

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	Boolean	No	ModifyProtectionRuleStatus	The operation that you want to perform. Set the value to **ModifyProtectionRuleStatus**.

Parameter	Type	Required	Example	Description
DefenseType	String	No	tamperproof	The protection module. Valid values: • **tamperproof**: tamper protection • **bot_crawler**: whitelist of legitimate search engines in legitimate crawlers • **bot_intelligence**: Bot Threat Intelligence • **ac_custom**: custom protection policies • **Whitelist**: website whitelist
Domain	String	No	www.example.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
LockVersion	Long	Yes	env	The version of the configuration record to be modified.
RuleId	Long	Yes	42755	The ID of the rule. **Note:** You can call the DescribeProtectionModuleRules operation to query the ID of a rule.
RuleStatus	Integer	Yes	1	The status of the rule. Set this parameter to: • **0**: disables the rule. • **1**: enables the rule.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Samples

Sample request

```
http(s)://[Endpoint]/? Action=ModifyProtectionRuleStatus
&DefenseType=tamperproof
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&LockVersion=2
&RuleId=42755
&RuleStatus=1
&<Common request parameters>
```

Sample success responses

`XML` format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

`JSON` format

```
{
  "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

2.6.10 DescribeDomainRuleGroup

You can call this operation to query the ID of the rule group configured in the RegEx protection engine for a specified domain.

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	DescribeDomainRuleGroup	The operation that you want to perform. Set the value to **DescribeDomainRuleGroup**.
Domain	String	Yes	1.example.com	The domain that has been added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of a WAF instance.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
RuleGroupId	Long	1012	The ID of the rule group configured in the RegEx protection engine. The system provides the following default rule groups: • **1011**: strict rules • **1012**: normal rules • **1013**: loose rules **Note:** If a custom rule group is configured for the specified domain, the ID of this custom group is returned.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=DescribeDomainRuleGroup
&Domain=1.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&<Common request parameters>
```

Sample success responses

`XML` format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
<RuleGroupId>1012</RuleGroupId>
```

`JSON` format

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
   "RuleGroupId":"1012"
}
```

Error codes

For a list of error codes, visit the API Error Center.

2.6.11 SetDomainRuleGroup

You can call this operation to select a default rule group or customize a rule group used by the RegEx protection engine for specified domains. The system provides three default rule groups.

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
Domains	String	Yes	["1.example.com","2.example.com"]	The domains that have been added to WAF. **Note:** You can specify multiple domain names.

Parameter	Type	Required	Example	Description
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call the DescribeInstanceInfo operation to query the ID of a WAF instance.
RuleGroupId	Long	Yes	1012	The ID of the protection rule group. The system provides the following default rule groups: • **1011**: strict rules • **1012**: normal rules • **1013**: loose rules  **Note:** You can also enter the ID of a custom rule group. The ID is displayed on the Customize Rule Groups page in the WAF console.
WafVersion	Long	No	1	The system data identifier that is used to control optimistic locking.
ResourceGroupId	String	No	rg-atstuj3rtoptyui	The ID of the resource group to which the queried domains belong in Resource Management. By default, no value is specified, indicating that the domains belong to the default resource group.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=SetDomainRuleGroup
&Domains=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&RuleGroupId=1012
&<Common request parameters>
```

Sample success responses

`XML` format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

`JSON` format

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes

For a list of error codes, visit the API Error Center.

2.6.12 ModifyProtectionRuleCacheStatus

You can call this operation to update cached pages protected by a specific tamper protection rule.

Note:
Currently, WAF instances deployed in regions outside mainland China do not support tamper protection.

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	ModifyProtectionRuleCacheStatus	The operation that you want to perform. Set the value to **ModifyProtectionRuleCacheStatus**.
DefenseType	String	Yes	tamperproof	Specifies the protection module. Set the value to **tamperproof**.
Domain	String	Yes	www.example.com	The domain that has been added to WAF.
InstanceId	String	Yes	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call the DescribeInstanceInfo operation to query the ID of the WAF instance.
RuleId	Long	Yes	42755	The ID of the protection rule. **Note:** You can call the DescribeProtectionModuleRules operation to query the ID of a protection rule.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/? Action=ModifyProtectionRuleCacheStatus
&DefenseType=tamperproof
```

```
&Domain=www.example.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&RuleId=42755
&<Common request parameters>
```

Sample success responses

`XML` format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
```

`JSON` format

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes

For a list of error codes, visit the API Error Center.

3 Legacy engine

3.1 API overview

This topic describes the API operations provided by Web Application Firewall (WAF).

instance information

Name	Description
DescribeRegions	You can call this operation to query the regions supported by WAF.
DescribePayInfo	You can call this operation to query the information of the WAF instance in a specified region.
DescribeWafSourceIpSegment	Queries DescribeWafSourceIpSegment CIDR blocks of the WAF instance.

Domain configurations

Name	Description
DescribeDomainNames	You can call this operation to obtain a list of domains that have been added to a specified WAF instance.
DescribeDomainConfig	You can call this operation to query the forwarding configurations of a specified domain name.
DescribeDomainConfigStatus	You can call this operation to query whether the forwarding configuration of a specified domain name takes effect.
CreateDomainConfig	Adds CreateDomainConfig domain name configuration information.
ModifyDomainConfig	You can call this operation to modify the configuration of a specified domain name.
DeleteDomainConfig	You can call this operation to delete the configurations of a specified domain name.
CreateCertAndKey	You can call this operation to upload CreateCertAndKey and private key information for a specified domain configurat ion record.

Configure Web attack protection

Name	Description
ModifyWafSwitch	Call the ModifyWafSwitch API to enable or disable Web attack protection.

Configure access control list

Name	Description
CreateAclRule	Adds an HTTP-based ACL rule for a specified domain.
DeleteAclRule	Deletes a specified ACL rule.
ModifyAclRule	Modifies a specified ACL rule.
DescribeAclRules	You can call this operation to query the list of precise access control rules for a specified domain name.

Asynchronous task information

Name	Description
DescribeAsyncTaskStatus	You can call this operation to query the DescribeAs yncTaskStatus of a WAF task.

3.2 Request method

To send a Web Application Firewall (WAF) API request, you must send an HTTP GET request to the WAF 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

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

The request syntax is as follows:

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

In the request:

- **Endpoint**: The endpoint of the WAF API is wafopenapi.cn-hangzhou.aliyuncs.com.
- **Action**: The operation that you want to perform. For example, to obtain a list of the domains added to WAF, you must set the Action parameter to **DescribeDomainNames**.

- **Version**: The version of the API to be used. The current WAF API version is 2018-01-17.
- **Parameters**: The request parameters for the operation. Separate multiple parameters with ampersands (&).

  Request parameters include both common parameters and operation-specific parameters. Common parameters include the API version and authentication information. For more information, see Common parameters.

The following example demonstrates how to call the **DescribeDomainNames** operation to obtain a list of the domains added to WAF.

Note:
To improve readability, the API request is displayed in the following format:

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Format=xml
&Version=2018-01-17
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2012-06-01T12:00:00Z
...
```

API authorization

To ensure the security of your account, we recommend that you call the WAF API as a RAM user. To call the WAF API as a RAM user, you must create an account for the RAM user and grant the account required permissions.

Signature method

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

WAF 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=
CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-
4e0ad82fd6cf
```

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

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2018-01-17
&SignatureVersion=1.0
```

Perform the following operations to calculate the signature:

1. Use the request parameters to create a string-to-sign:

   ```
   GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeDomainNames&Region%3Dcn
   &InstanceId%3Dwaf_elasticity-cn-0xldbqtm005&Format%3DXML&SignatureMethod
   %3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&
   SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version
   %3D2018-01-17
   ```

2. Calculate the HMAC value of the string-to-sign.

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

   ```
   CT9X0VtwR86fNWSnsc6v8YGOjuE=
   ```

3. Add the signature to the request parameters:

   ```
   https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
   &Region=cn
   &InstanceId=waf_elasticity-cn-0xldbqtm005
   &TimeStamp=2016-02-23T12:46:24Z
   &Format=XML
   &AccessKeyId=testid
   &SignatureMethod=HMAC-SHA1
   &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
   &Version=2018-01-17
   &SignatureVersion=1.0
   ```

```
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

3.3 Common parameters

Common request parameters

Common request parameters must be included in all WAF API requests.

Table 3-1: Common request parameters

Parameter	Type	Require	Description
Region	String	Yes	The ID of the region to which the WAF instance belongs. Set the value to: • CN: indicates mainland China. • cn-hongkong: indicates the overseas region.
InstanceId	String	Yes	The ID of the WAF instance. **Note:** You can call **DescribePayInfo** to view your WAF instance ID.
Format	String	No	The format in which to return the response. Valid values: • JSON (default) • XML
Version	String	Yes	The version number of the API, in the format of YYYY-MM-DD. Set the value to: 2018-01-17
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud
Signature	String	Yes	The signature string in the API request.
SignatureMethod	String	Yes	The encryption method of the signature string. Set the value to HMAC-SHA1

Parameter	Type	Require	Description
Timestamp	String	Yes	The UTC time when the request is signed. Specify the time in the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format. The time must be in UTC. For example, 20:00:00 on January 10, 2013 in China Standard Time (UTC +8) is written as 2013-01-10T12:00:00Z.
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 multiple requests.
ResourceOwnerAccount	String	No	The account that owns the resource to be accessed by the current request.

Sample requests

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&Region=cn
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Timestamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&SignatureMethod=Hmac-SHA1
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2018-01-17
&SignatureVersion=1.0
&Signature=Signature
```

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. Response data can be returned in either the JSON or XML format. You can specify the response format when you are making the request. The default response format is XML.

Every response returns a unique **RequestId** (request ID) regardless of whether the call is successful.

- XML format

```
<?xml xml version="1.0" encoding="utf-8"? >
```

```
<!--Result Root Node-->
<Operation Name+Response>
  <!-Return Request Tag-->
  <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
  <!-Return Result Data-->
</Operation Name+Response>
```

- JSON format

```
{
  "RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
  /*Return Result Data*/
  }
```

3.4 Call examples

When you call a WAF API, an HTTP GET request is sent to the WAF API end point. You must add the Web Application Firewall in the request based on the API operation description. After the call, the system returns a response.

The following Python Sample code demonstrates how to add common parameters and interface request parameters, how to use request parameters to construct a canonicalized query string, how to construct a StringToSign string, and how to obtain an OpenAPI server address. The system sends an HTTP request by using the Get method to obtain the response .

Download the Python Sample code

Note:

To use the following examples, you need to replace common request parameters and request parameters in request parameters examples.

Define common parameters

```
#! /usr/bin/env python
# -*- coding: utf-8 -*-
import hashlib
import urllib
import requests
import hmac
import random
import datetime
import sys

class OpenAPI(object):
   def __init__(self, signature_version='1.0', api_url=None, ak=None, sk=None, api_version
=None):
      assert api_url is not None
      assert ak is not None
      assert sk is not None
      assert api_version is not None
```

```
        self.signature_once = 0
        self.signature_method = 'HMAC-SHA1'
        self.signature_version = signature_version
        self.api_version = api_version
        self.format = 'json'
        self.signature_method = 'HMAC-SHA1'
        self.api_url = api_url
        self.access_key = ak
        self.access_secret = sk

    def __gen_common_params(self, req_type, api_version, access_key, access_secret,
http_params):
        while 1:
            rand_int = random.randint(10, 999999999)
            if rand_int! =self.signature_once:
                self.signature_once = rand_int
                break

        # Indicates whether the current step contains the AccessKey parameter.
        if access_key == None:
            return None

        http_params.append(('AccessKeyId', access_key))
        http_params.append(('Format', self.format))
        http_params.append(('Version', api_version))
        timestamp = datetime.datetime.utcnow().strftime("%Y-%m-%dT%H:%M:%SZ")
        http_params.append(('Timestamp', timestamp))
        http_params.append(('SignatureMethod', self.signature_method))
        http_params.append(('SignatureVersion', self.signature_version))
        http_params.append(('SignatureNonce', str(self.signature_once)))
        # Signature
        http_params = self.sign(req_type, http_params, access_secret)
        return urllib.urlencode(http_params)

    def get(self, http_params=[], host=None, execute=True):
        data = self.__gen_common_params('GET', self.api_version, self.access_key, self.
access_secret, http_params)
        api_url = self.api_url

        if data == None:
            url = "%s" % (api_url)
        else:
            url = "%s/? " % api_url + data
        print ("URL: %s"%url)
        if execute is False:
            return url
        ret = {}
        try:
            if host is not None:
                response = requests.get(url,headers={'Host':host}, verify=False)
            else:
                response = requests.get(url, verify=False)
            ret['code'] = response.status_code
            ret['data'] = response.text
        except Exception as e:
            ret['data'] = str(e)

        return ret

    def __get_data(self, http_params):
        params = self.__gen_common_params('POST', self.api_version, self.access_key, self.
access_secret, http_params)
        if params == []:
```

```
            data = None
        else:
            data = params.replace("+", "%20")
            data = data.replace("*", "%2A")
            data = data.replace("%7E", "~")
        return data

    def post(self, http_params=[], out_fd=sys.stdout):
        data = self.__get_data(self.api_version, self.access_key, self.access_secret,
http_params)
        api_url = self.api_url
        out_fd.write(u"[%s] --> (POST):%s\n%s\n" % (datetime.datetime.now(), api_url, data
))
        ret = requests.post(api_url, data, verify=False)
        print (ret.text)
        return ret

    def sign(self, http_method, http_params, secret):
        list_params = sorted(http_params, key=lambda d: d[0])
        # print list_params
        url_encode_str = urllib.urlencode(list_params)
        # print url_encode_str
        url_encode_str = url_encode_str.replace("+", "%20")
        url_encode_str = url_encode_str.replace("*", "%2A")
        url_encode_str = url_encode_str.replace("%7E", "~")
        string_to_sign = http_method + "&%2F&" + urllib.quote(url_encode_str)
        # print string_to_sign
        hmac_key = str(secret + "&")
        sign_value = str(hmac.new(hmac_key, string_to_sign, hashlib.sha1).digest().encode
('base64').rstrip())
        http_params.append(('Signature', sign_value))
        return http_params
```

Generate an API call request

Note:

The following code example is used to call the **ModifyWafSwitch** example: enable Web application protection through the API.

```
from open_api import OpenAPI

class Waf(OpenAPI):
    def __init__(self, api_url, ak, sk, api_version, instance_id, region):

        super(Waf, self).__init__(api_url=api_url, ak=ak, sk=sk, api_version=api_version)
        self.instance_id = instance_id
        self.region = region

    def ModifyWafSwitch(self,domain, instance_id=None, region='cn', service_on=1,
execute=True):
        if instance_id is None:
            instance_id = self.instance_id
        if region is None:
            region = self.region

        params = [
            ('Action', 'ModifyWafSwitch'),
            ('InstanceId', instance_id),
            ('Domain', domain),
            ('Region',region),
```

```
            ('ServiceOn', service_on)
        ]

        print (params)

        return self.get(http_params=params,execute=execute)

if __name__ == "__main__":
    api_url = "https://wafopenapi.cn-hangzhou.aliyuncs.com"
    # Enter the accesskey ID of your account
    ak = ""
    # Enter the AccessKeyScecret information of your account.
    sk = ""
    # Enter the ID of your WAF instance. You can obtain the instance ID by calling the
GetPayInfo operation.
    instance_id = ""
    # Enter the region information of your WAF instance.
    region = ""
    api_version = "2018-01-17"

    t = Waf(api_url=api_url, ak=ak, sk=sk, api_version=api_version, instance_id=instance_id
, region=region)
    print (t.ModifyWafSwitch(domain="", service_on=1))
```

Send an HTTP GET request

You can use the preceding code to obtain an HTTP request and send the HTTP GET request to the WAF API endpoint.

Sample requests

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=ModifyWafSwitch&Domain=
www.aliyun.com&ServiceOn=1&Region=cn&InstanceId=waf_elasticity-cn-0xldbqtm005&
TimeStamp=2018-08-23T12:46:24Z&Format=JSON&AccessKeyId=testid&SignatureMethod
=HMAC-SHA1&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&Version=2018-
01-17&SignatureVersion=1.0&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

Get response results

Finally, a response is received from the WAF API server.

Sample responses

```
{
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
 "Result":{
   "Status":2,
   "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 }
}
```

3.5 Instance information

3.5.1 DescribePayInfo

You can call this operation to query the information of the WAF instance in a specified region.

> **Note:**
> You do not need to specify the **InstanceId** common request parameters.

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	Boolean	No	DescribePayInfo	The operation that you want to perform. Valid values: **DescribePayInfo**.
InstanceSource	String	Yes	waf-cloud	The source of the instance. Default value: **waf-cloud**.
Region	String	Yes	cn	The ID of the region. Valid values: • **cn**: mainland China (default) • **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	Cost	The ID of the request.
Result			The returned result.
EndDate	Long	1512921600	The time when an instance expires. **Note:** For a pay-as-you-go instance, the trial period ends.

Parameter	Type	Example	Description
InDebt	Integer	1	Whether the current instance is overdue: • **0**: The instance has overdue payments. • **1**: indicates normal. **Note:** This parameter takes effect for pay-as-you-go WAF instances.
InstanceId	String	waf_elasticity-cn-0xldbqtm005	The ID of the instance whose type or storage space is modified.
PayType	Integer	env	The type of the WAF instance: • **0**: indicates that the ECS instance is not purchased or activated. • **1**: A subscription instance. • **2**: A pay-as-you-go instance.
Region	String	cn	Region: • **CN**: indicates mainland China. • **cn-hongkong**: indicates the overseas region.
RemainDay	Integer	0	The number of days before the trial period of the WAF instance expires. **Note:** This parameter is only valid for pay-as-you-go WAF instances.

Parameter	Type	Example	Description
Status	Integer	0	The status of the WAF instance. Valid values: • **0**: indicates that the API has expired. • **1**: indicates normal. **Note:** This parameter is only valid for WAF subscription instances.
Trial	Integer	0	Indicates whether this is a trial instance. Valid value: • **0**: false • **1**: true **Note:** This parameter is only valid for pay-as-you-go WAF instances.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribePayInfo
&Region=cn
&Common request parameters
```

Sample success responses

`XML` format

```
<DescribePayInfoResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Result>
        <Status>1</Status>
        <Trial>0</Trial>
        <InstanceId>waf_elasticity-cn-0xldbqtm005</InstanceId>
        <InDebt>1</InDebt>
        <Region>cn</Region>
        <RemainDay>0</RemainDay>
        <PayType>2</PayType>
        <EndDate>1512921600</EndDate>
    </Result>
```

```
</DescribePayInfoResponse>
```

JSON format

```
{
 "Result":{
  "Status":1,
  "EndDate":1512921600,
  "Region":"cn",
  "InDebt":1,
  "Trial":0,
  "InstanceId":"waf_elasticity-cn-0xldbqtm005",
  "RemainDay":0,
  "PayType":2
 },
 "RequestId":"276D7566-31C9-4192-9DD1-51B10DAC29D2"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.5.2 DescribeRegions

You can call this operation to query the regions supported by WAF.

Note:

You do not need to specify the **Region** and **InstanceId** these two public request parameters.

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	Boolean	No	DescribeRegions	The operation that you want to perform. Set the value to **DescribeRegions**.

Response parameters

Parameter	Type	Example	Description
Regions			The list of regions.

Parameter	Type	Example	Description
Region			The list of regions.
Display	String	ture	Indicates whether the WAF service is available in the specified region. • **true**: indicates yes. • **false**: indicates no.
Region	String	cn	The region ID.
RequestId	String	Cost	The ID of the request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeRegions
&Common request parameters
```

Sample success responses

XML format

```
<DescribeRegionsResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Regions>
        <Region>
            <Region>cn</Region>
            <Display>true</Display>
        </Region>
        <Region>
            <Region>cn-hongkong</Region>
            <Display>true</Display>
        </Region>
    </Regions>
</DescribeRegionsResponse>
```

JSON format

```
{
 "RequestId":"276D7566-31C9-4192-9DD1-51B10DAC29D2",
 "Regions":{
  "Region":[
   {
    "region":"cn",
    "display":"true"
   },
   {
    "region":"cn-hongkong",
    "display":"true"
```

```
    }
   ]
  }
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.5.3 DescribeWafSourceIpSegment

Queries DescribeWafSourceIpSegment CIDR blocks of the WAF instance.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeWafSourceIpSegment	The operation that you want to perform. Valid values: **DescribeWafSourceIpSegment**.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
Ips	String	121.43.18.0/24, 120.25.115.0/24, 101.200.106.0/24	The CIDR blocks used by WAF. Separate the CIDR blocks with commas (,).
RequestId	String	9087 ADDC-9047 -4D02-82A7- 33021B58083C	The ID of the request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeWafSourceIpSegment
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Region=cn
& <Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeWafSourceIpSegmentResponse>
    <Ips>121.43.18.0/24,120.25.115.0/24,101.200.106.0/24</Ips>
    <RequestId>9087ADDC-9047-4D02-82A7-33021B58083C</RequestId>
</DescribeWafSourceIpSegmentResponse>
```

`JSON` format

```
{
 "RequestId":"9087ADDC-9047-4D02-82A7-33021B58083C",
 "Ips":"121.43.18.0/24,120.25.115.0/24,101.200.106.0/24"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.6 Domain configuration

3.6.1 DescribeDomainNames

You can call this operation to obtain a list of domains that have been added to a specified WAF instance.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeDomainNames	The operation that you want to perform. Set the value to **DescribeDomainNames**.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: outside mainland China

Response parameters

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

Parameter	Type	Example	Description
Result		rstest.cdn.com	The returned result. The structure is described as follows: • **DomainNames** A list of domain names that have been added. It is a string array.
DomainNames			The returned result. The structure is described as follows: • **DomainNames** A list of domain names that have been added. It is a string array.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/?Action=DescribeDomainNames
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Common request parameters
```

Sample success responses

XML format

```
<DescribeDomainNamesResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Result>
        <DomainNames>rstest.cdn.com</DomainNames>
        <DomainNames>rstest1.cdn.com</DomainNames>
        <DomainNames>rstest2.cdn.com</DomainNames>
        <DomainNames>rstest3.cdn.com</DomainNames>
    </Result>
</DescribeDomainNamesResponse>
```

JSON format

```
{
 "Result":{
  "DomainNames":[
   "rstest.cdn.com",
   "rstest1.cdn.com",
   "rstest2.cdn.com",
   "rstest3.cdn.com"
  ]
 },
 "RequestId":"56B40D30-4960-4F19-B7D5-2B1F0EE6CB70"
```

```
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.6.2 DescribeDomainConfig

You can call this operation to query the forwarding configurations of a specified domain name.

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	Boolean	No	DescribeDomainConfig	The operation that you want to perform. Valid values: **DescribeDomainConfig**.
Domain	String	No	rstest.cdn.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	Cost	The ID of the request.
Result			The returned result.
DomainConfig			Domain name configuration structure.
Cname	String	xxxxxxxxxxxxxx.fakewaf.com	The WAF CNAME address.
ProtocolType	Integer	env	Protocol type: • **0**: indicates that HTTP is supported. • **1**: indicates that HTTPS is supported. • **2**: indicates that both HTTP and HTTPS are supported.
SourceIps	String	1.1.1.1	The IP address of the origin server.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712180229702.Y6re3d	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeDomainConfig
&Domain=www.aliyun.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&Common request parameters
```

Sample success responses

XML format

```
<DescribeDomainConfigResponse>
    <RequestId>56B40D30-4960-4F19-B7D5-2B1F0EE6CB70</RequestId>
    <Result>
        <Status>2</Status>
        <DomainConfig>
            <ProtocolType>2</ProtocolType>
            <SourceIps>x.x.x.x</SourceIps>
            <SourceIps>x.x.x.x</SourceIps>
            <Cname>xxxxxxxxxxxxxx.fakewaf.com</Cname>
        </DomainConfig>
        <WafTaskId>aliyun.waf.20180712180229702.Y6re3d</WafTaskId>
    </Result>
</DescribeDomainConfigResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712180229702.Y6re3d",
  "DomainConfig":{
   "Cname":"xxxxxxxxxxxxx.fakewaf.com",
   "ProtocolType":2,
   "SourceIps":[
    "x.x.x.x",
    "x.x.x.x"
   ]
  }
 },
 "RequestId":"56B40D30-4960-4F19-B7D5-2B1F0EE6CB70"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.6.3 DescribeDomainConfigStatus

You can call this operation to query whether the forwarding configuration of a specified domain name takes effect.

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	Boolean	No	DescribeDomainConfigStatus	The operation that you want to perform. Valid values: **DescribeDomainConfigStatus**.
Domain	String	No	rstest.cdn.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
DomainConfig			Domain name forwarding configuration structure.

Parameter	Type	Example	Description
ConfigStatus	String	1	Domain name forwarding configuration effective Status: • **0**: indicates that it does not take effect. • **1**: indicates that the alert has taken effect. • **-1**: indicates that the detection has not been completed.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.2018071221 4032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeDomainConfigStatus
&Domain=www.aliyun.com
&Common request parameters
```

Sample success responses

XML format

```
<RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
<Result>
   <Status>2</Status>
   <DomainConfig>
      <ConfigStatus>1</ConfigStatus>
   </DomainConfig>
   <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
</Result>
```

JSON format

```
{
```

```
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a",
  "DomainConfig":{
   "ConfigStatus":1
  }
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```


Error codes.

For a list of error codes, visit the API Error Center.

3.6.4 CreateDomainConfig

Adds CreateDomainConfig domain name configuration information.

To ensure Web application security when you add your domain name to WAF, perform the following steps:

1. Call CreateDomainConfig to add domain name configuration information.

2. Based on the information in the returned result **WafTaskId** value, call DescribeAsyncTaskStatus to view the execution progress of the configuration task for adding a domain name. When the task is completed, the domain name configuration information is added.

3. Call DescribeDomainConfigStatus to check whether the domain name configuration takes effect.

> **Note:**
> In the returned result, you can switch the business traffic to the WAF instance only after the configurations take effect.

4. Call DescribeDomainConfig to view the WAF CNAME address.

5. In the domain name DNS resolution service provider, modify the parsing records of the domain name, switch the business traffic to WAF.

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	Boolean	No	CreateDomainConfig	The operation that you want to perform. Valid values: **CreateDomainConfig**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
IsAccessProduct	Integer	Yes	0	Indicates whether a layer -7 proxy, such as anti-DDoS pro or CDN, has been configured for the domain name in front of the WAF instance. Valid values: • **0**: indicates none. • **1**: indicates yes.
Protocols	String	No	["http"]	The access protocol supported by the domain name. Valid values: • **HTTP**: indicates that HTTP is supported. • **HTTPS**: indicates that HTTPS is supported. • **http,https**: supports both HTTP and HTTPS.
SourceIps	String	Yes	["1.1.1.1"]	The origin IP address. Multiple IP addresses can be specified. Array type. Example values: ["1.1.1.1"].

Parameter	Type	Required	Example	Description
HttpPort	String	Yes	[80]	The HTTP ports. When multiple HTTP ports are specified, separate them with commas (,). Example value: [80]. **Note:** This parameter is required if the Protocols parameter is set to http. Default value: **80**. **HttpPort** and **HttpsPort** fill in at least one of the two request parameters.
HttpsPort	String	Yes	[443]	The HTTPS ports. When multiple HTTPS ports are specified, separate them with commas (,). Example value: [443]. **Note:** This parameter is required if the Protocols parameter is set to https. Default value: **443**. **HttpPort** and **HttpsPort** fill in at least one of the two request parameters.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China
LoadBalancing	String	Optional	0	The back-to-source SLB policy. Valid values: • **0**: represents IP Hash mode. • **1**: Round robin

Parameter	Type	Required	Example	Description
HttpToUserIp	String	Optional	0	Indicates whether to enable HTTP-based back-to-origin for HTTPS requests. Valid values: • **0**: Disabled (default) • **1**: indicates enabled **Note:** If your website does not support HTTPS back-to-origin, enable the HTTP back-to-origin feature (port 80 is selected by default) to enable HTTPS access through WAF.
HttpsRedirect	String	Optional	0	Specifies whether to redirect HTTP requests as HTTPS requests. Valid values: • **0**: Disabled (default) • **1**: indicates enabled **Note:** You need to specify this request parameter only if the Protocols parameter is set to https. After you enable this feature, HTTP requests are redirected to HTTPS port 443.
RsType	String	Optional	0	The origin address type of the domain name. Valid values: • **0**: indicates a back-to-origin IP address. • **1**Indicates the back-to-origin domain name.
ResourceGroupId	String	Yes	rs1234	The ID of the resource group.

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result	Struct		The returned result.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.
Status	Integer	2	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=CreateDomainConfig
&Domain=www.aliyun.com
&SourceIps=["x.x.x.x","x.x.x.x"]
&Protocols=["http","https"]
&HttpPort=[80]
&HttpsPort=[443]
&RsType=0
&IsAccessProduct=0
&LoadBalancing=0
&HttpsRedirect=1
&HttpToUserIp=0
&Common request parameters
```

Sample success responses

`XML` format

```
<CreateDomainConfigResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
```

```
</CreateDomainConfigResponse>
```

JSON format

```
{
  "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
  "Result":{
    "Status":2,
    "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
  }
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.6.5 ModifyDomainConfig

You can call this operation to modify the configuration of a specified domain name.

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	Boolean	No	ModifyDomainConfig	The operation that you want to perform. Valid values: **ModifyDomainConfig**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.

Parameter	Type	Required	Example	Description
IsAccessProduct	Integer	Yes	0	Indicates whether a layer -7 proxy, such as anti-DDoS pro or CDN, has been configured for the domain name in front of the WAF instance. Valid values: • **0**: indicates none. • **1**: indicates yes.
Protocols	String	No	["http"]	The access protocol supported by the domain name. Valid values: • **HTTP**: indicates that HTTP is supported. • **HTTPS**: indicates that HTTPS is supported. • **http,https**: supports both HTTP and HTTPS.
HttpPort	String	Yes	[80]	The HTTP ports. When multiple HTTP ports are specified, separate them with commas (,). Example value: [80]. **Note:** This parameter is required if the Protocols parameter is set to http. Default value: **80**. **HttpPort** and **HttpsPort** fill in at least one of the two request parameters.

Parameter	Type	Required	Example	Description
HttpToUserIp	String	Optional	0	Indicates whether to enable HTTP-based back-to-origin for HTTPS requests. Valid values: • **0**: Disabled (default) • **1**: indicates enabled **Note:** If your website does not support HTTPS back-to-origin, enable the HTTP back-to-origin feature (port 80 is selected by default) to enable HTTPS access through WAF.
HttpsPort	String	Yes	[443]	The HTTPS ports. When multiple HTTPS ports are specified, separate them with commas (,). Example value: [443]. **Note:** This parameter is required if the Protocols parameter is set to https. Default value: **443**. **HttpPort** and **HttpsPort** fill in at least one of the two request parameters.
HttpsRedirect	String	Optional	1	The Https status. Set the value to: • **1:** Log backup is enabled. • **0**: Off (default)
LoadBalancing	String	Optional	0	The load balancing method. Valid values: • **0**:IP hash • **1**: Polling

Parameter	Type	Required	Example	Description
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China
SourceIps	String	Yes	["1.1.1.1"]	The origin IP address. Multiple IP addresses can be specified. Example: ["1.1.1.1"].

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=ModifyDomainConfig
&Domain=www.aliyun.com
&SourceIps=["x.x.x.x","x.x.x.x"]
&Protocols=["http","https"]
&HttpPort=[80]
```

```
&HttpsPort=[443]
&IsAccessProduct=0
&HttpsRedirect=1
&HttpToUserIp=0
&Common request parameters
```

Sample success responses

XML format

```
<ModifyDomainConfigResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</ModifyDomainConfigResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.6.6 DeleteDomainConfig

You can call this operation to delete the configurations of a specified domain name.

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	Boolean	No	DeleteDomainConfig	The operation that you want to perform. Valid values: **DeleteDomainConfig**.

Parameter	Type	Required	Example	Description
Domain	String	No	rstest.cdn.com	The domain name that has been added to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxl9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DeleteDomainConfig
&Domain=www.aliyun.com
&Common request parameters
```

Sample success responses

XML format

```
<DeleteDomainConfigResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</DeleteDomainConfigResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.6.7 CreateCertAndKey

You can call this operation to upload CreateCertAndKey and private key information for a specified domain configuration record.

Note:
You can also call this operation to update the uploaded certificate and private key for a specified domain.

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	Boolean	No	CreateCert AndKey	The operation that you want to perform. Valid values: **CreateCert AndKey**.
Cert	String	No	----- BEGIN CERTIFICATE ----------END CERTIFICATE -----	The content of the certificate.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.
HttpsCertName	String	No	www.aliyun.com	The name of the certificate.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
Key	String	No	----- BEGIN RSA PRIVATE KEY ----------END RSA PRIVATE KEY -----	Private key
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DeleteDomainConfig
&Domain=www.aliyun.com
&Cert="-----BEGIN CERTIFICATE----------END CERTIFICATE-----"
&Key="-----BEGIN RSA PRIVATE KEY----------END RSA PRIVATE KEY-----"
&HttpsCertName=www.aliyun.com
&Common request parameters
```

Sample success responses

`XML` format

```
<CreateCertAndKeyResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</CreateCertAndKeyResponse>
```

`JSON` format

```
{
 "Result":{
  "Status":2,
```

```
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Errors

For a list of error codes, visit the API Error Center.

3.7 Configure web attack protection

3.7.1 ModifyWafSwitch

Call the ModifyWafSwitch API to enable or disable Web attack protection.

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	Boolean	No	ModifyWafSwitch	The operation that you want to perform. Valid values: **ModifyWafSwitch**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
ServiceOn	Integer	Yes	1	The Web attack protection switch. Valid values: • **0**: indicates closing. • **1**: indicates enabled.

Parameter	Type	Required	Example	Description
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=ModifyWafSwitch
&Domain=www.aliyun.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&ServiceOn=1
&Common request parameters
```

Sample success responses

XML format

```
<ModifyWafSwitchResponse>
```

```
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</ModifyWafSwitchResponse>
```

JSON format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Errors

For a list of error codes, visit the API Error Center.

3.8 Configure access control list

3.8.1 DescribeAclRules

You can call this operation to query the list of precise access control rules for a specified domain name.

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	Boolean	No	DescribeAclRules	The operation that you want to perform. Valid values: **DescribeAclRules**.
CurrentPage	Integer	Yes	1	The number of the page to return. For example, to query the returned results on the first page, enter **1**.

Parameter	Type	Required	Example	Description
Domain	String	No	www.aliyun.com	The domain that you want to add to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
PageSize	Integer	Yes	10	The number of entries returned per page.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
AclRules			The list of HTTP-based ACL rules. Each ACL rule is described as a sub-parameter of AclRule. The AclRule sub-parameter is a JSON string.
AclRule			The list of HTTP-based ACL rules. Each ACL rule is described as a sub-parameter of AclRule. The AclRule sub-parameter is a JSON string.

Parameter	Type	Example	Description
Action	Integer	1	The matching action of the rule. Valid values: • **0**: indicates blocking, that is, the access request is blocked if the matching condition of the rule is met. • **1**: allows the access request to pass, that is, the access request that meets the matching condition of the rule. • **2**: indicates an alert. That is, when the matched condition of the rule is matched, the access request is allowed, but the request is recorded and an alert is generated.
Conditions			The structure of rule matching conditions.
condition			The structure of rule matching conditions.

Parameter	Type	Example	Description
Contain	String	1	Logical operator: • **0**: indicates that the rule is not included. • **1**: indicates include. • **2**: indicates that it does not exist. • **10**: indicates a value that is not equal to the passed value. • **11**: indicates equal to. • **20**: indicates that the length is less than the specified value. • **21**: indicates a character with a length equal to the value of • **22**: indicates that the length is greater than. • **30**: indicates that the value is less than. • **31**: indicates that the value is equal to. • **32**: indicates a value greater than.
Key	String	url	The matching field. Valid values: IP , URL, Referer, User-Agent, Params, Cookie, Content-Type, X-Forwarded-For, Content-Length, Post-Body, Http-Method, and Header. **Note:** Note: WAF instances of different versions support different fields. You can view the supported fields in the Web Application Firewall console.
Value	String	login.	The matching content.
ContinueBlockGeo	Integer	1	Indicates whether to continue region blocking. Valid values: • **0**: false • **1**: true

Parameter	Type	Example	Description
ContinueCc	Integer	1	Indicates whether to proceed with the HTTP flood detection. Valid values: • **0**: false • **1**: true
ContinueDataRiskControl	Integer	1	Indicates whether to continue data risk control protection. Valid values: • **0**: false • **1**: true
ContinueSA	Integer	1	Indicates whether to perform the smart protection engine rule check. Valid values: • **0**: false • **1**: true
ContinueSdk	Integer	1	Indicates whether to continue SDK protection. Valid values: • **0**: no • **1**: true
ContinueWaf	Integer	1	Indicates whether to proceed with the Web attack protection rule detection. Valid values: • **0**: false • **1**: true
Id	Long	1111	The ID of the ACL rule.
IsDefault	Integer	1	Indicates whether the rule is a default rule. Valid values: • **0**: false • **1**: true
Name	String	test	The name of the rule.

Parameter	Type	Example	Description
Order	Integer	1	The order of the rules. **Note:** Note: the greater the value, the higher the priority of the rule.
Total	Interger	1	The total number of rules.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeAclRules
&Domain=www.aliyun.com
&CurrentPage=1
&PageSize=50
&Common request parameters
```

Sample success responses

`XML` format

```
<DescribeAclRulesResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <AclRules>
            <AclRule>
                <IsDefault>1</IsDefault>
                <Order>0</Order>
                <ContinueBlockGeo>1</ContinueBlockGeo>
                <Action>1</Action>
                <ContinueWaf>1</ContinueWaf>
                <ContinueSdk>0</ContinueSdk>
                <Id>16572</Id>
                <ContinueCc>1</ContinueCc>
                <Conditions>
                    <condition>
                        <key>URL</key>
                        <contain>1</contain>
                        <value>asfas</value>
                    </condition>
                </Conditions>
                <Name>default</Name>
                <ContinueDataRiskControl>1</ContinueDataRiskControl>
                <ContinueSA>1</ContinueSA>
            </AclRule>
        </AclRules>
        <Total>1</Total>
    </Result>
```

```
</DescribeAclRulesResponse>
```

JSON format

```
{
 "Result":{
  "AclRules":{
   "AclRule":[
    {
     "Name":"default",
     "Conditions":{
      "condition":[
       {
        "contain":1,
        "value":"asfas",
        "key":"URL"
       }
      ]
     },
     "ContinueDataRiskControl":1,
     "Action":1,
     "ContinueSdk":0,
     "ContinueWaf":1,
     "IsDefault":1,
     "Order":0,
     "Id":16572,
     "ContinueCc":1,
     "ContinueSA":1,
     "ContinueBlockGeo":1
    }
   ]
  },
  "Total":1
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.8.2 CreateAclRule

Adds an HTTP-based ACL rule for a specified domain.

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	Boolean	No	CreateAclRule	The operation that you want to perform. Valid values: **CreateAclRule**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call DescribePayInfo to view your WAF instance ID.

Parameter	Type	Required	Example	Description
Rules	String	No	{"conditions":[{"key":"URL","contain":1,"value":"asfas"}],"continueComponent":{"post_action_cc":1,"post_action_waf":1,"post_action_sa":1,"post_action_block_geo":"0","post_action_data_risk_control":"1"},"action":"1","name":"lei123"}	The details of the HTTP-based ACL rule, in JSON format. The following table describes the structure. • **Id**: Optional. The ID of the rule. The value is of the Long type. • **Name**: the name of the rule. This parameter is required and of String type. • **Action** the matching action of the rule. This parameter is required and of Integer type. Valid values: - **0**: indicates blocking, that is, the access request is blocked if the matching condition of the rule is met. - **1**: allows the access request to pass, that is, the access request that meets the matching condition of the rule. - **2**: indicates an alert. That is, when the matched condition of the rule is matched, the access request is allowed, but the request is recorded and an alert is generated. • **ContinueComponent**: Optional. The String type. This parameter specifies whether to run other WAF protection policies in JSON format. The following table describes the structure. - **post_action_cc**(Optional) The Integer type. Specifies whether to proceed with the HTTP flood detection. Valid values: ■ **0**: false ■ **1**: true - **post_action_waf**(Optional)

Parameter	Type	Required	Example	Description
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Specifies the mapping between a field and logical operators.

Field	Logical operator
IP	Belongs to, does not belong to
Referer	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
User-Agent	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
Param	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
Cookie	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist
Content-Type	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
X-Forwarded-For	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist

Field	Logical operator
Content-Length	Value less than, value equal to, and value greater than
Post-Body	Contains, does not contain, equals, is not equal to
Http-Method	Equal to, not equal to
Header	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The GUID generated by Alibaba Cloud for the request.
Result			The returned result.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.2018071221 4032277.qmxI9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=CreateAclRule
&Domain=www.aliyun.com
&ServiceOn=1
&Rules={...}
```

```
&Common request parameters
```

Sample success responses

`XML` format

```
<CreateAclRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</CreateAclRuleResponse>
```

`JSON` format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.8.3 ModifyAclRule

Modifies a specified ACL rule.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	ModifyAclRule	The operation that you want to perform. Valid values: **ModifyAclRule**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call DescribePayInfo to view your WAF instance ID.

Parameter	Type	Required	Example	Description
Rules	String	No	{"conditions":[{"key":"URL","contain":1,"value":"asfas"}],"continueComponent":{"post_action_cc":1,"post_action_waf":1,"post_action_sa":1,"post_action_block_geo":"0","post_action_data_risk_control":"1"},"action":"1","name":"lei123","id":65899}	The details of the HTTP-based ACL rule, in JSON format. The following table describes the structure. • **Id** the ID of the rule. Required. The ID is of the Long type. • **Name**: the name of the rule. This parameter is required and of String type. • **Action** the matching action of the rule. This parameter is required and of Integer type. Valid values: - **0**: indicates blocking, that is, the access request is blocked if the matching condition of the rule is met. - **1**: allows the access request to pass, that is, the access request that meets the matching condition of the rule. - **2**: indicates an alert. That is, when the matched condition of the rule is matched, the access request is allowed, but the request is recorded and an alert is generated. • **ContinueComponent**: Optional. The String type. This parameter specifies whether to run other WAF protection policies in JSON format. The following table describes the structure. - **post_action_cc**(Optional) The Integer type. Specifies whether to proceed with the HTTP flood detection. Valid values: ■ **0**: false ■ **1**: true - **post_action_waf**(Optional)

Parameter	Type	Required	Example	Description
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Specifies the mapping between a field and logical operators.

Field	Logical operator
IP	Belongs to, does not belong to
Referer	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
User-Agent	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
Param	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
Cookie	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist
Content-Type	Contains, does not contain, is equal to, is not equal to, is less than, length is equal to, and length is greater than
X-Forwarded-For	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist

Field	Logical operator
Content-Length	Value less than, value equal to, and value greater than
Post-Body	Contains, does not contain, equals, is not equal to
Http-Method	Equal to, not equal to
Header	Contains, does not contain, is equal to, is not equal to, is less than, has a length of, is greater than, and does not exist

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result	Struct		The returned result.
WafTaskId	String	aliyun.waf.2018071221 4032277.qmxl9a	The ID of the WAF request.
Status	Integer	2	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=ModifyAclRule
&Domain=www.aliyun.com
&ServiceOn=1
&Rules={...}
```

```
&Common request parameters
```

Sample success responses

`XML` format

```
<ModifyAclRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</ModifyAclRuleResponse>
```

`JSON` format

```
{
   "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0",
   "Result":{
      "Status":2,
      "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
   }
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.8.4 DeleteAclRule

Deletes a specified ACL rule.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DeleteAclRule	The operation that you want to perform. Valid values: **DeleteAclRule**.
Domain	String	No	rstest.cdn.com	The domain that you want to add to WAF.

Parameter	Type	Required	Example	Description
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance.  **Note:** You can call DescribePayInfo to view your WAF instance ID.
RuleId	Long	Yes	65899	The ID of the HTTP-based ACL rule.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	D7861F61-5B61-46CE-A47C-6B19160D5EB0	The ID of the request.
Result			The returned result.
Status	Integer	env	Request execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.
WafTaskId	String	aliyun.waf.20180712214032277.qmxl9a	The ID of the WAF request.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DeleteAclRule
&Domain=www.aliyun.com
&InstanceId=waf_elasticity-cn-0xldbqtm005
&RuleId=65899
&Common request parameters
```

Sample success responses

`XML` format

```
<DeleteAclRuleResponse>
    <RequestId>D7861F61-5B61-46CE-A47C-6B19160D5EB0</RequestId>
    <Result>
        <Status>2</Status>
        <WafTaskId>aliyun.waf.20180712214032277.qmxI9a</WafTaskId>
    </Result>
</DeleteAclRuleResponse>
```

`JSON` format

```
{
 "Result":{
  "Status":2,
  "WafTaskId":"aliyun.waf.20180712214032277.qmxI9a"
 },
 "RequestId":"D7861F61-5B61-46CE-A47C-6B19160D5EB0"
}
```

Error codes.

For a list of error codes, visit the API Error Center.

3.9 Asynchronous task information

View the WAF API task status.

3.9.1 DescribeAsyncTaskStatus

You can call this operation to query the DescribeAsyncTaskStatus of a WAF task.

Debugging

OpenAPI Explorer automatically calculates the signature value. For your convenience, we recommend that you call this operation in OpenAPI Explorer. OpenAPI Explorer dynamically generates the sample code of the operation for different SDKs.

Request parameters

Parameter	Type	Required	Example	Description
Action	Boolean	No	DescribeAsyncTaskStatus	The operation that you want to perform. Valid values: **DescribeAsyncTaskStatus**.
InstanceId	String	No	waf_elasticity-cn-0xldbqtm005	The ID of the WAF instance. **Note:** You can call DescribePayInfo to view your WAF instance ID.
WafRequestId	String	No	aliyun.waf.20180719140433783.SvaZeY	The ID of the WAF task.
Region	String	Yes	cn	The ID of the region to which the WAF instance belongs. Set the value to: • **cn**: mainland China (default) • **cn-hongkong**: areas outside mainland China

Response parameters

Parameter	Type	Example	Description
RequestId	String	12EF3845-CCEB-4B84-AE60-2B49B2FF1EE5	The ID of the request.
Result			Responses
AsyncTaskStatus	String	env	Asynchronous task execution status: • **0**: indicates that the request is pending execution. • **1**: indicates that the request is being executed. • **2**: indicates that the request has been completed.

Parameter	Type	Example	Description
Data	String	xx	The business data returned by asynchronous tasks.
ErrCode	String	400	Error code. **Note:** This parameter is only returned when an error occurs during request execution.
ErrMsg	String	xx	The description of the error message. **Note:** This parameter is only returned when an error occurs during request execution.
Progress	Integer	90	The progress of the asynchronous task. Unit: percentage.

Samples

Sample request

```
https://wafopenapi.cn-hangzhou.aliyuncs.com/? Action=DescribeAsyncTaskStatus
&InstanceId=waf_elasticity-cn-0xldbqtm005
&WafRequestId=aliyun.waf.20180719140433783.SvaZeY
&Common request parameters
```

Sample success responses

XML format

```
<DescribeAsyncTaskStatusResponse>
    <RequestId>12EF3845-CCEB-4B84-AE60-2B49B2FF1EE5</RequestId>
    <Result>
        <DomainConfig>
            <Progress>100</Progress>
            <AsyncTaskStatus>2</AsyncTaskStatus>
        </DomainConfig>
    </Result>
</DescribeAsyncTaskStatusResponse>
```

JSON format

```
{
```

```
 "Result":{
  "DomainConfig":{
   "AsyncTaskStatus":2,
   "Progress":100
  }
 },
 "RequestId":"12EF3845-CCEB-4B84-AE60-2B49B2FF1EE5"
}
```


Errors

For a list of error codes, visit the API Error Center.

4 Error codes

The following table lists all the error codes that the system may return when you call a WAF API.

Error code	Error message	Description
RequestError	The system is unavailable. Please try again later.	The error message returned because an internal error occurred. Try again later.
ComboError	No package information is available.	The error message returned because no package information is available. Possible reasons include invalid UID or WAF instance ID.
DomainCountError	The number of domain names exceeds the limit. You can upgrade the domain package.	The error message returned because the number of domains has reached the upper limit.
HttpsSupportError	HTTPS is not supported.	The error message returned because HTTPS requests are not supported.
OuterCloudSupportError	Servers outside Alibaba is not supported.	The error message returned because external servers are not supported.
DomainSourceIpCountError	The number of origin fetch addresses exceeds the limit.	The error message returned because the number of origin IP addresses has reached the upper limit.
DomainNotRegisterError	The specified domain name is not ICP filed.	The error message returned because the specified domain does not have an ICP license.
ExtensiveDomainSupportError	Wildcard domains is not supported.	The error message returned because wildcard domains are not supported.

Error code	Error message	Description
DomainHasAdded	The domain has been configured.	The error message returned because the specified domain has already been added to WAF.
SourceIpNotYoursError	You are not the owner of this origin fetch address.	The error message returned because the specified origin IP address does not belong to the current account.
HttpsCertFormatError	The certificate file is malformed.	The error message returned because the SSL certificate format is invalid.
HttpsPrivateKeyFormatError	The private key of the certificate is malformed.	The error message returned because the format of the SSL certificate private key is invalid.
ErrorInSourceIps	The origin fetch address includes disallowed IP addresses or domains.	The error message returned because some IP addresses or domains cannot be added as origins.
DomainNotExist	The specified domain does not exist.	The error message returned because the specified domain does not exist.
IsNonStandardPort	Non-standard ports are not supported.	The error message returned because WAF does not support non-standard ports.
InvalidDomainError	The domain is invalid.	The error message returned because the specified domain is invalid.
InvalidMainDomainError	The number of primary domains exceeds the limit. You can upgrade the domain package.	The error message returned because the number of top-level domains has reached the upper limit.
NotSupportMainDomain Error	The primary domain is not supported.	The error message returned because the specified top-level domain is invalid.

Error code	Error message	Description
CertAndKeyNotMatch	The certificate file and private key do not match.	The error message returned because the specified certificate and private key do not match.
SourceIpSupportsVirtualIpError	This is an instance dedicated for shared virtual host. Only an IP of a virtual host can be added.	The error message returned because only the IP address of a Web Hosting instance can be added.
DomainAutoAccessError	The auto access of domain is being configured.	The error message returned because a domain is being automatically added to WAF.
DomainHttpPortError	An invalid HTTP port is specified.	The error message returned because HTTP ports are not supported.
DomainHttpsPortError	An invalid HTTPS port is specified.	The error message returned because HTTPS ports are not supported.
PortCountError	The number of ports exceeds the limit.	The error message returned because the number of ports has reached the upper limit.
DomainBlackError	The domain has been listed in the blacklist.	The error message returned because the specified domain has been added to the blacklist.
AclRuleCountError	The number of access control rules exceeds the limit.	The error message returned because the number of HTTP ACL rules has reached the upper limit.
AclRuleSeniorError	You don't have permission to use senior access control rule.	The error message returned because the number of advanced HTTP ACL rules has reached the upper limit.
AclRuleDuplicateError	The access control rule name is invalid or a rule with the same name already exists.	The error message returned because the specified HTTP ACL rule name is invalid.
AclRuleNotFound	The specified access control rule does not exist.	The error message returned because the specified rule does not exist.

Error code	Error message	Description
ExtensiveDomainHasBeenUsedByOthers	Another user has used this wildcard domain in WAF.	The error message returned because the specified wildcard domain has already been used by another account.
AuthorizeCertFailed	There are some errors when the system checks your certificate.	The error message returned because the certificate verification failed.
CertServiceError	There are some errors in the certificate service.	The error message returned because a certificate error occurred.
CertNameExisted	The certificate name already exists.	The error message returned because the specified certificate name already exists.
CertKeysIsNotMatch	The certificate file and private key do not match.	The error message returned because the specified certificate and private key do not match.
CertKeysIsEmpty	The private key of the certificate is required.	The error message returned because the certificate private key is not specified.
CertKeyFormatError	The private key of the certificate is malformed.	The error message returned because the certificate private key format is invalid.
SaveCertFailed	There are some errors when the system save your certificate.	The error message returned because the system failed to save the certificate.
CertHasExisted	This certificate has already been uploaded. Do not upload it again.	The error message returned because the specified certificate already exists.
CertHasExpired	The certificate has expired. Do not continue using this certificate.	The error message returned because the specified certificate has expired.
CertKeyServerError	The certificate service is unavailable,Please try again later.	The error message returned because a certificate error occurred.

Error code	Error message	Description
ParamError	The parameters of your request are invalid.	The error message returned because the specified parameters are invalid.
CertIsNotMatchDomain	The certificate does not include this domain.	The error message returned because the certificate and the domain do not match.
CertNotExist	The certificate is not exist.	The error message returned because the specified certificate does not exist.
CertHasDelInCA	The certificate is deleted in CA service.	The error message returned because the certificate has been deleted by the certificate authority.
NotOperateOtherCallerConfig	You are not authorized to perform other channel config.	The error message returned because you cannot manage a domain configuration record created by other services.
DomainNotCloseInAntibot	The domain is still used in Anti-Bot service.	The error message returned because the Anti-Bot Service protection feature is enabled for the specified domain.
AntibotServerError	Anti-bot service is unavailable.	The error message returned because Anti-Bot Service is unavailable.
TaskNotFound	The specified task does not exist.	The error message returned because the task does not exist.
TaskIsRejected	The task has been rejected.	The error message returned because the task has been rejected.
TaskStillRunning	The task is running.	The error message returned because the task is still running.
TaskTimeOut	The task is timeout.	The error message returned because the task timed out.