

Web Application Firewall

API Reference

Issue 28
Date 2024-03-22



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Before You Start.....	1
1.1 Overview.....	1
1.2 API Calling.....	1
1.3 Endpoints.....	1
1.4 Concepts.....	1
2 API Overview.....	3
3 API Calling.....	4
3.1 Making an API Request.....	4
3.2 Authentication.....	7
3.3 Response.....	8
4 APIs.....	10
4.1 Managing Websites Protected by Dedicated WAF Engines.....	10
4.1.1 Querying the List of Domain Names Protected by Dedicated WAF Instances.....	10
4.1.2 Adding a Domain Name to a Dedicated WAF Instance.....	16
4.1.3 Modifying a Domain Name Protected by a Dedicated WAF Instance.....	29
4.1.4 Querying Domain Name Settings in Dedicated Mode.....	47
4.1.5 Deleting a Domain Name from a Dedicated WAF Instance.....	57
4.1.6 Modifying the Protection Status of a Domain Name in Dedicated Mode.....	62
4.2 Rule Management.....	65
4.2.1 Changing the Status of a Rule.....	65
4.2.2 Querying CC Attack Protection Rules.....	69
4.2.3 Creating a CC Attack Protection Rule.....	78
4.2.4 Querying a CC Attack Protection Rule by ID.....	94
4.2.5 Updating a CC Attack Protection Rule.....	102
4.2.6 Deleting a CC Attack Protection Rule.....	118
4.2.7 Querying the List of Precise Protection Rules.....	126
4.2.8 Creating a precise protection rule.....	131
4.2.9 Querying a Precise Protection Rule by ID.....	138
4.2.10 Updating a precise protection rule.....	143
4.2.11 Deleting a precise protection rule.....	150
4.2.12 Creating a Global Protection Whitelist (Formerly False Alarm Masking) Rule.....	155
4.2.13 Querying the List of Global Protection Whitelist (Formerly False Alarm Masking) Rules.....	163

4.2.14 Updating a Global Protection Whitelist (Formerly False Alarm Masking) Rule.....	168
4.2.15 Deleting a Global Protection Whitelist (Formerly False Alarm Masking) Rule.....	176
4.2.16 Querying the Blacklist and Whitelist Rule List.....	181
4.2.17 Creating a Blacklist/Whitelist Rule.....	185
4.2.18 Querying a blacklist or whitelist rule.....	189
4.2.19 Updating a Blacklist or Whitelist Protection Rule.....	193
4.2.20 Querying Global Protection Whitelist (Formerly False Alarm Masking) Rules.....	197
4.2.21 Deleting a Blacklist or Whitelist Rule.....	203
4.2.22 Querying the JavaScript Anti-Crawler Rule List.....	207
4.2.23 Updating a JavaScript Anti-Crawler Protection Rule.....	211
4.2.24 Creating a JavaScript Anti-Crawler Rule.....	215
4.2.25 Querying a JavaScript Anti-Crawler Rule.....	220
4.2.26 Updating a JavaScript Anti-Crawler Rule.....	224
4.2.27 Deleting a JavaScript Anti-Crawler Rule.....	229
4.2.28 Querying the list of Data Masking Rules.....	233
4.2.29 Creating a Data Masking Rule.....	238
4.2.30 Querying a Data Masking Rule.....	242
4.2.31 Updating a Data Masking Rule.....	245
4.2.32 Deleting a Data Masking Rule.....	250
4.2.33 Querying the List of Known Attack Source Rules.....	253
4.2.34 Creating a Known Attack Source Rule.....	257
4.2.35 Querying a Known Attack Source Rule by ID.....	260
4.2.36 Updating a Known Attack Source Rule.....	263
4.2.37 Deleting a Known Attack Source Rule.....	266
4.2.38 Querying the List of Geolocation Access Control Rules.....	269
4.2.39 Creating a Geolocation Access Control Rule.....	273
4.2.40 Querying a Geolocation Access Control Rule by ID.....	278
4.2.41 Updating a Geolocation Access Control Rule.....	282
4.2.42 Deleting a Geolocation Access Control Rule.....	286
4.2.43 Querying the List of Web Tamper Protection Rules.....	290
4.2.44 Creating a Web Tamper Protection Rule.....	293
4.2.45 Querying a Web Tamper Protection Rule.....	296
4.2.46 Deleting a Web Tamper Protection Rule.....	299
4.2.47 Updating the Cache for a Web Tamper Protection Rule.....	302
4.2.48 Querying the List of Information Leakage Prevention Rules.....	305
4.2.49 Creating an Information Leakage Prevention Rule.....	309
4.2.50 Querying an Information Leakage Prevention Rule.....	313
4.2.51 Updating an Information Leakage Prevention Rule.....	316
4.2.52 Deleting an Information Leakage Prevention Rule.....	319
4.2.53 Querying the Reference Table List.....	322
4.2.54 Creating a Reference Table.....	326
4.2.55 Querying a Reference Table.....	330

4.2.56 Modifying a Reference Table.....	333
4.2.57 Deleting a Reference Table.....	337
4.3 Address Group Management.....	340
4.3.1 Querying IP Address Groups.....	340
4.3.2 Creating an IP Address Group.....	344
4.3.3 Querying IP Addresses in an Address Group.....	347
4.3.4 Modifying an IP Address Group.....	351
4.3.5 Deleting an IP Address Group.....	354
4.4 Certificate Management.....	357
4.4.1 Querying the List of Certificates.....	357
4.4.2 Uploading a Certificate.....	362
4.4.3 Querying a Certificate.....	366
4.4.4 Modifying a Certificate.....	370
4.4.5 Deleting a Certificate.....	373
4.4.6 Applying a Certificate to a Domain Name.....	376
4.5 Event Management.....	380
4.5.1 This API is used to query details about an event of a specified ID.....	380
4.5.2 Querying the List of Attack Events.....	384
4.6 Dashboard.....	390
4.6.1 Querying the QPS Statistics.....	391
4.6.2 Querying Statistics of Requests and Attacks.....	395
4.6.3 Querying Bandwidth Usage Statistics.....	399
4.6.4 Querying Statistics of Top Exceptions.....	403
4.6.5 Querying Top Security Statistics by Category.....	407
4.6.6 Querying Website Requests.....	414
4.7 Dedicated Instance Management.....	418
4.7.1 Querying Dedicated WAF Instances.....	418
4.7.2 Creating a Dedicated WAF Instance.....	424
4.7.3 Querying Details about a Dedicated WAF Instance.....	428
4.7.4 Renaming a Dedicated WAF Instance.....	433
4.7.5 Deleting a Dedicated WAF Instance.....	437
4.8 Log Reporting.....	442
4.8.1 Querying LTS Settings.....	442
4.8.2 Configuring LTS for WAF Logging.....	445
4.9 Managing Your Subscriptions.....	449
4.9.1 Request body for buying a yearly/monthly-billed cloud WAF instance.....	449
4.9.2 Changing specifications of a cloud WAF instance billed yearly/monthly.....	453
4.9.3 Enabling Pay-Per-Use Billing for Cloud WAF.....	457
4.9.4 Disabling Pay-Per-Use Pricing for Cloud WAF.....	462
4.9.5 Querying Your Subscriptions.....	466
4.10 Domain Name Management.....	470
4.10.1 Migrating Protected Domain Names by Enterprise Project.....	470

4.11 System Management.....	474
4.11.1 Querying the IP addresses of WAF.....	474
4.12 Alarm Management.....	476
4.12.1 This API is used to query configuration of alarm notifications.....	476
4.12.2 This API is used to update alarm notification configuration.....	480
4.13 Protected Website Management in Cloud Mode.....	485
4.13.1 Querying the List of Domain Names Protected in Cloud Mode.....	485
4.13.2 Adding a Domain Name to the Cloud WAF.....	491
4.13.3 Querying Details About a Domain Name by Domain Name ID in Cloud Mode.....	503
4.13.4 Updating Configurations of Domain Names Protected with Cloud WAF.....	514
4.13.5 Deleting a Domain Name from the Cloud WAF.....	534
4.13.6 Changing the Protection Status of a Domain Name.....	539
4.13.7 Obtaining Domain Name Routing Information (in Cloud Mode).....	542
4.14 Querying the Domain Name of a Tenant.....	546
4.14.1 Querying Domain Names Protected with All WAF Instances.....	546
4.14.2 Querying a Domain Name by ID.....	553
4.15 Querying Features Available at a Site.....	560
4.15.1 Querying Features Available at a Site.....	560
4.16 Policy management.....	565
4.16.1 Querying the Protection Policy List.....	565
4.16.2 Creating a Protection Policy.....	573
4.16.3 Querying a Policy by ID.....	581
4.16.4 Updating a Protection Policy.....	589
4.16.5 Deleting a Protection Policy.....	602
4.16.6 Updating the Domain Name Protection Policy.....	610
A Appendix.....	618
A.1 Status Code.....	618
A.2 Error Codes.....	619
A.3 Obtaining a Project ID.....	627
A.4 Geographical Location Codes.....	628
B Change History.....	634

1 Before You Start

1.1 Overview

Web Application Firewall (WAF) keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following attacks: Structured Query Language (SQL) injection, cross-site scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

This document describes how to use application programming interfaces (APIs) to perform operations on WAF, such as querying and updating.

Before you start, ensure that you are familiar with WAF. For details, see [Web Application Firewall \(WAF\)](#).

1.2 API Calling

WAF provides Representational State Transfer (REST) APIs, allowing you to use HTTPS requests to call them. For details, see [API Calling](#).

1.3 Endpoints

An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions. For the endpoints of all services, see [Regions and Endpoints](#).

1.4 Concepts

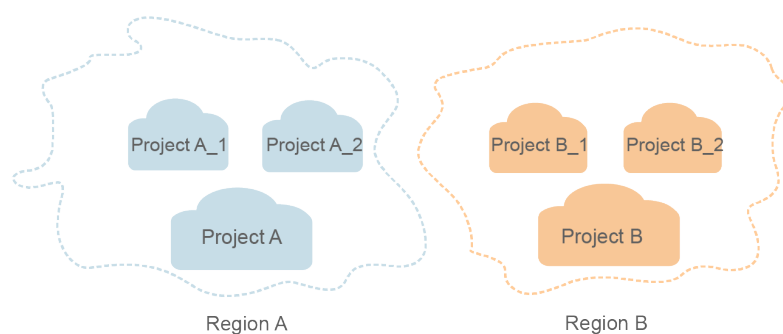
- Account

An account is created upon successful registration. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity and should not be used to perform routine management. For security

purposes, create IAM users and grant them permissions for routine management.

- User
An IAM user is created by an account in IAM to use cloud services. Each IAM user has its own identity credentials (password and access keys).
- Region
Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- Availability Zone (AZ)
An AZ comprises one or multiple physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Compute, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.
- Project
Projects group and isolate compute, storage, and network resources across physical regions. A default project is provided for each region, and subprojects can be created under each default project. Users can be granted permissions to access all resources in a specific project. For more refined access control, create subprojects under a project and create resources in the subprojects. Users can then be assigned permissions to access only specific resources in the subprojects.

Figure 1-1 Project isolation model



2 API Overview

You can use all functions of WAF through its APIs.

Type	Description
Cloud mode APIs	APIs for creating, modifying, querying, and removing domain names in cloud mode.
Dedicated mode APIs	APIs for creating, modifying, querying, and removing domain names in dedicated mode
Protection policy APIs	APIs for creating policies in batches and modifying the domain names that a policy applies to.
Protection rule APIs	APIs for creating, updating, querying, and deleting protection rules.
Certificate APIs	APIs for creating, modifying, and querying certificates.
Event API	API for querying details of an event.
Security overview APIs	APIs for querying overall security statistics.
Feature query API	API for querying features available in a site.
Domain name query API	API for querying domain names connected to WAF.

3 API Calling

3.1 Making an API Request

This section describes the structure of a REST API request, and uses the IAM API for [obtaining a user token](#) as an example to demonstrate how to call an API. The obtained token can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

{URI-scheme} :// {Endpoint} / {resource-path} ? {query-string}

Although a request URI is included in the request header, most programming languages or frameworks require the request URI to be transmitted separately.

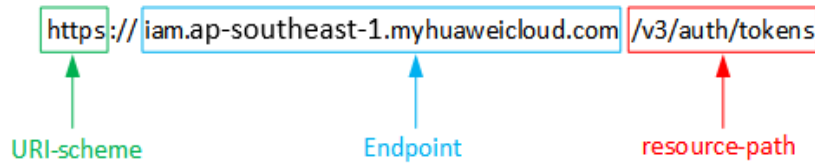
- **URI-scheme:**
Protocol used to transmit requests. All APIs use HTTPS.
- **Endpoint:**
Domain name or IP address of the server bearing the RESTful service. The endpoint varies between services in different regions. It can be obtained from the [Regions and Endpoints](#).
For example, the endpoint of IAM in region **CN-Hong Kong** is **iam.ap-southeast-1.myhuaweicloud.com**.
- **resource-path:**
Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.
- **query-string:**
Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in the **CN-Hong Kong** region, obtain the endpoint of IAM (iam.ap-southeast-1.myhuaweicloud.com)) for this region and

the **resource-path** (/v3/auth/tokens) in the URI of the API used to **obtain a user token**. Then, construct the URI as follows:

```
https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

Figure 3-1 Example URI



NOTE

To simplify the URI display in this document, each API is provided only with a **resource-path** and a request method. The **URI-scheme** of all APIs is **HTTPS**, and the endpoints of all APIs in the same region are identical.

Request Methods

The HTTP protocol defines the following request methods that can be used to send a request to the server:

- **GET**: requests the server to return specified resources.
- **PUT**: requests the server to update specified resources.
- **POST**: requests the server to add resources or perform special operations.
- **DELETE**: requests the server to delete specified resources, for example, an object.
- **HEAD**: same as GET except that the server must return only the response header.
- **PATCH**: requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API used to **obtain a user token**, the request method is POST. The request is as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

Request Header

You can also add additional header fields to a request, such as the fields required by a specified URI or HTTP method. For example, to request for the authentication information, add **Content-Type**, which specifies the request body type.

Common request header fields are as follows:

- **Content-Type**: specifies the request body type or format. This field is mandatory and its default value is **application/json**. Other values of this field will be provided for specific APIs if any.
- **X-Auth-Token**: specifies a user token only for token-based API authentication. The user token is a response to the API used to **obtain a user token**. This API is the only one that does not require authentication.

 NOTE

In addition to supporting token-based authentication, APIs also support authentication using access key ID/secret access key (AK/SK). During AK/SK-based authentication, an SDK is used to sign the request, and the **Authorization** (signature information) and **X-Sdk-Date** (time when the request is sent) header fields are automatically added to the request.

For more information, see [AK/SK Authentication](#).

The API used to [obtain a user token](#) does not require authentication. Therefore, only the **Content-Type** field needs to be added to requests for calling the API. An example of such requests is as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
```

Request Body

The body of a request is often sent in a structured format as specified in the **Content-Type** header field. The request body transfers content except the request header.

The request body varies between APIs. Some APIs do not require the request body, such as the APIs requested using the GET and DELETE methods.

In the case of the API used to [obtain a user token](#), the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Set **username** to the name of a user, **domainname** to the name of the account that the user belongs to, ********* to the user's login password, and **xxxxxxxxxxxxxxxxxxxx** to the project name. You can learn more information about projects from [Regions and Endpoints](#). Check the value of the **Region** column.

 NOTE

The **scope** parameter specifies where a token takes effect. You can set **scope** to an account or a project under an account. In the following example, the token takes effect only for the resources in a specified project. For more information about this API, see [Obtaining a User Token](#).

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
Content-Type: application/json
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "name": "username",
          "password": "*****",
          "domain": {
            "name": "domainname"
          }
        }
      }
    },
    "scope": {
      "project": {
        "name": "xxxxxxxxxxxxxxxxxxxx"
      }
    }
  }
}
```

```
}  
}
```

If all data required for the API request is available, you can send the request to call the API through [curl](#), [Postman](#), or coding. In the response to the API used to obtain a user token, **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

3.2 Authentication

Requests for calling an API can be authenticated using either of the following methods:

- Token-based authentication: Requests are authenticated using a token.
- AK/SK-based authentication: Requests are authenticated by encrypting the request body using an AK/SK pair. This method is recommended because it provides higher security than token-based authentication.

Token-based Authentication

NOTE

The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the IAM API used to obtain a user token.

A token specifies temporary permissions in a computer system. During API authentication using a token, the token is added to requests to get permissions for calling the API.

The token can be obtained by calling the required API. For more information, see [Obtaining a User Token](#). A project-level token is required for calling this API, that is, **auth.scope** must be set to **project** in the request body. Example:

```
{  
  "auth": {  
    "identity": {  
      "methods": [  
        "password"  
      ],  
      "password": {  
        "user": {  
          "name": "username",  
          "password": "*****#",  
          "domain": {  
            "name": "domainname"  
          }  
        }  
      }  
    }  
  },  
  "scope": {  
    "project": {  
      "name": "xxxxxxxx"  
    }  
  }  
}
```

After a token is obtained, the **X-Auth-Token** header field must be added to requests to specify the token when calling other APIs. For example, if the token is **ABCDEFJ....**, **X-Auth-Token: ABCDEFJ....** can be added to a request as follows:

```
POST https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK-based Authentication

NOTE

AK/SK-based authentication supports API requests with a body not larger than 12 MB. For API requests with a larger body, token-based authentication is recommended.

In AK/SK-based authentication, AK/SK is used to sign requests and the signature is then added to the requests for authentication.

- AK: access key ID, which is a unique identifier used in conjunction with a secret access key to sign requests cryptographically.
- SK: secret access key used in conjunction with an AK to sign requests cryptographically. It identifies a request sender and prevents the request from being modified.

In AK/SK-based authentication, you can use an AK/SK to sign requests based on the signature algorithm or use the signing SDK to sign requests. For details about how to sign requests and use the signing SDK, see [API Signature Guide](#).

NOTICE

The signing SDK is only used for signing requests and is different from the SDKs provided by services.

3.3 Response

Status Code

After sending a request, you will receive a response, including a status code, response header, and response body.

A status code is a group of digits, ranging from 1xx to 5xx. It indicates the status of a request. For more information, see [Status Code](#).

For example, if status code **201** is returned for calling the API used to [obtain a user token](#), the request is successful.

Response Header

Similar to a request, a response also has a header, for example, **content-type**.

The following shows the response header for the API to [obtain a user token](#), in which **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

Figure 3-2 Header fields of the response to the request for obtaining a user token

```

connection → keep-alive

content-type → application/json

date → Tue, 12 Feb 2019 06:52:13 GMT

server → Web Server

strict-transport-security → max-age=31536000; includeSubdomains;

transfer-encoding → chunked

via → proxy A

x-content-type-options → nosniff

x-download-options → noopen

x-frame-options → SAMEORIGIN

x-iam-trace-id → 218d45ab-d674-4995-af3a-2d0255ba41b5

x-subject-token
→ MIIYXQYJKoZIhvcNAQcCoIIVTJCGEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOensiZXhwaXJlc19hdCI6IjwMTktMDItMTNUMD
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkajACgklqO1wi4JIGzrpd18LGXK5bdfq4lqHCYb8P4NaYONYejeAgzVefYtLWT1GSO0zxKZmlQHq82HBqHdgIZO9fuEbl5dMhdavj+33wEl
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jggIFkNPQuFSOU8+uSsttVwRtnfsc+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUVhVpxk8pxiX1wTEboX-
RzT6MUbpvGw-oPNFYxJECKnoH3HRozv0vN--n5d6Nbxg==

x-xss-protection → 1; mode=block;

```

(Optional) Response Body

The body of a response is often returned in structured format as specified in the **Content-Type** header field. The response body transfers content except the response header.

The following shows part of the response body for the API to **obtain a user token**. For the sake of space, only part of the content is displayed here.

```

{
  "token": {
    "expires_at": "2019-02-13T06:52:13.855000Z",
    "methods": [
      "password"
    ],
    "catalog": [
      {
        "endpoints": [
          {
            "region_id": "xxxxxxx",
            .....

```

If an error occurs during API calling, an error code and a message will be displayed. The following shows an error response body.

```

{
  "error_msg": "The format of message is error",
  "error_code": "AS.0001"
}

```

In the response body, **error_code** is an error code, and **error_msg** provides information about the error.

4 APIs

4.1 Managing Websites Protected by Dedicated WAF Engines

4.1.1 Querying the List of Domain Names Protected by Dedicated WAF Instances

Function

This API is used to query domain names protected by dedicated WAF instances.

URI

GET /v1/{project_id}/premium-waf/host

Table 4-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-2 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS. The default value is 0. 0: indicates the default enterprise project. Default value: 0
page	No	String	Page number of the data to be returned during pagination query. Value range: 0 to 100,000 . The default value is 1 , indicating that the data on the first page is returned. Default: 1
pagesize	No	String	Number of results on each page in query pagination. The value range is 1 to 100. The default value is 10 , indicating that each page contains 10 results. To query all domain names at a time, set this parameter to -1 . Default: 10
hostname	No	String	Domain name
policyname	No	String	Policy name
protect_status	No	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> • 0: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.

Request Parameters

Table 4-3 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

Table 4-4 Response body parameters

Parameter	Type	Description
total	Integer	Total number of protected domain names
items	Array of SimplePremiumWafHost objects	Array of details about all protected domain names

Table 4-5 SimplePremiumWafHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
extend	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.
region	String	Region ID. This parameter is included when the domain name was added to WAF through the console. This parameter is left blank when the domain name was added to WAF by calling an API. You can query the region ID on the Regions and Endpoints page on the website.
flag	Flag object	Special identifier, which is used on the console.

Parameter	Type	Description
description	String	Domain name description
policyid	String	ID of the policy initially used to the domain name. You can call the ListPolicy API to query the policy list and view the ID of a specific policy.
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
hostid	String	Domain name ID, which is the same as the value of id and is a redundant field.

Table 4-6 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. <ul style="list-style-type: none"> • true: The website passed the PCI 3DS certification check. • false: The website failed the PCI 3DS certification check. Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
pci_dss	String	Whether the website passed the PCI DSS certification check. <ul style="list-style-type: none"> ● true: The website passed the PCI DSS certification check. ● false: The website failed the PCI DSS certification check. Enumeration values: <ul style="list-style-type: none"> ● true ● false
cname	String	The CNAME record being used. <ul style="list-style-type: none"> ● old: The old CNAME record is used. ● new: The new CNAME record is used. Enumeration values: <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	Whether WAF support Multi-AZ DR <ul style="list-style-type: none"> ● true: WAF supports multi-AZ DR. ● false: WAF does not support multi-AZ DR. Enumeration values: <ul style="list-style-type: none"> ● true ● false
ipv6	String	Whether IPv6 protection is supported. <ul style="list-style-type: none"> ● true: IPv6 protection is supported. ● false: IPv6 protection is not supported. Enumeration values: <ul style="list-style-type: none"> ● true ● false

Status code: 400

Table 4-7 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-8 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-9 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to obtain the list of domain names protected with dedicated WAF instances in a project. The project ID is specified by `project_id`.

```
GET https://{Endpoint}/v1/{project_id}/premium-waf/host?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "items": [ {
    "id": "ee896796e1a84f3f85865ae0853d8974",
    "hostname": "www.demo.com",
    "extend": { },
    "region": "cn-north-4",
    "flag": {
      "pci_3ds": "false",
      "pci_dss": "false"
    },
    "description": "",
    "policyid": "df15d0eb84194950a8fdc615b6c012dc",
    "protect_status": 1,
    "access_status": 0,
    "hostid": "ee896796e1a84f3f85865ae0853d8974"
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	Invalid request
401	The token does not have the required permission.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.1.2 Adding a Domain Name to a Dedicated WAF Instance

Function

This API is used to add a domain name to a dedicated WAF instance.

URI

POST /v1/{project_id}/premium-waf/host

Table 4-10 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-11 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-12 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-13 Request body parameters

Parameter	Mandatory	Type	Description
certificateid	No	String	Certificate ID. It can be obtained by calling the ListCertificates API. <ul style="list-style-type: none"> This parameter is not required when the client protocol is HTTP. This parameter is mandatory when the client protocol is HTTPS.
certificatenam e	No	String	Certificate name. <ul style="list-style-type: none"> This parameter is not required when the client protocol is HTTP. This parameter is mandatory when the client protocol is HTTPS.
hostname	Yes	String	Protected domain name or IP address (port allowed)
proxy	Yes	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> false: No proxy is used. true: A proxy is used.
policyid	No	String	ID of the policy initially used to the domain name. You can call the ListPolicy API to query the policy list and view the ID of a specific policy.

Parameter	Mandatory	Type	Description
server	Yes	Array of PremiumWaf Server objects	Origin server configuration of the protected domain name
block_page	No	BlockPage object	Alarm page configuration. This parameter is optional. When a user-defined page needs to be configured, all subfields of this parameter are mandatory.
forward_header_map	No	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: <ul style="list-style-type: none"> • \$time_local • \$request_id • \$connection_requests • \$tenant_id • \$project_id • \$remote_addr • \$remote_port • \$scheme • \$request_method • \$http_host • \$origin_uri • \$request_length • \$ssl_server_name • \$ssl_protocol • \$ssl_curves • \$ssl_session_reused
description	No	String	Remarks of the protected domain name

Table 4-14 PremiumWafServer

Parameter	Mandatory	Type	Description
front_protocol	Yes	String	Protocol used by the client to request access to the origin server. Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
back_protocol	Yes	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
weight	No	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is 1 . This field is not included by cloud WAF.
address	Yes	String	IP address of your origin server requested by the client
port	Yes	Integer	Port used by WAF to forward client requests to the origin server
type	Yes	String	The origin server address is an IPv4 or IPv6 address. Enumeration values: <ul style="list-style-type: none"> • ipv4 • ipv6

Parameter	Mandatory	Type	Description
vpc_id	Yes	String	VPC ID. To obtain the VPC ID, perform the following steps: Use either of the following methods to obtain the VPC ID. <ul style="list-style-type: none"> Log in to the WAF console and choose Instance Management > Dedicated Engine > VPC\Subnet. The VPC ID is in the VPC \Subnet column. Log in to the VPC console and click the VPC name. On the page displayed, copy the ID in the VPC Information area.

Table 4-15 BlockPage

Parameter	Mandatory	Type	Description
template	Yes	String	Template name
custom_page	No	CustomPage object	Custom alarm page
redirect_url	No	String	URL of the redirected page

Table 4-16 CustomPage

Parameter	Mandatory	Type	Description
status_code	Yes	String	Status Codes
content_type	Yes	String	The content type of the custom alarm page. The value can be text/html , text/xml , or application/json .
content	Yes	String	The page content based on the selected page type. For details, see the <i>Web Application Firewall (WAF) User Guide</i> .

Response Parameters

Status code: 200

Table 4-17 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Protected domain names
protocol	String	Client protocol, which is the protocol used by a client (for example, a browser) to access your website. Enumeration values: <ul style="list-style-type: none"> • HTTPS • HTTP • HTTP&HTTPS
server	Array of PremiumWaf Server objects	Origin server configuration of the protected domain name
proxy	Boolean	Whether to use a proxy <ul style="list-style-type: none"> • true: A proxy is used. • false: No proxy is used.
locked	Integer	Domain name status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The domain name is not frozen. • 1: The domain name is frozen. This parameter is redundant in this version.
timestamp	Long	Time the domain name was added to WAF. The value is a 13-digit timestamp in ms.
tls	String	TLS version. You can use TLS v1.0, TLS v1.1, or TLS v1.2. TLS v1.0 is used by default. Parameter tls is available only when the client protocol is HTTPS. Enumeration values: <ul style="list-style-type: none"> • TLS v1.0 • TLS v1.1 • TLS v1.2

Parameter	Type	Description
cipher	String	<p>Parameter cipher is required only when the client protocol is HTTPS. The value can be cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default.</p> <ul style="list-style-type: none"> • cipher_1: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH • cipher_2: ECDH+AESGCM:EDH+AESGCM • cipher_3: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH • cipher_4: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH • cipher_default: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. <p>Enumeration values:</p> <ul style="list-style-type: none"> • cipher_1 • cipher_2 • cipher_3 • cipher_4 • cipher_default
extend	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.
flag	Flag object	Special identifier, which is used on the console.
description	String	Domain name description
policyid	String	ID of the policy initially used to the domain name. You can call the ListPolicy API to query the policy list and view the ID of a specific policy.
domainid	String	Account ID, which is the same as the account ID on the My Credentials page. To go to this page, log in to Cloud management console, hover the cursor over your username, and click My Credentials in the displayed window.

Parameter	Type	Description
projectid	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
enterprise_project_id	String	Enterprise project ID. To obtain the ID, log in to the Cloud management console first. On the menu bar at the top of the page, choose Enterprise > Project Management . Then, click the project name and view the ID.
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
block_page	BlockPage object	Alarm page configuration

Parameter	Type	Description
forward_header_map	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: <ul style="list-style-type: none"> • \$time_local • \$request_id • \$connection_requests • \$tenant_id • \$project_id • \$remote_addr • \$remote_port • \$scheme • \$request_method • \$http_host • \$origin_uri • \$request_length • \$ssl_server_name • \$ssl_protocol • \$ssl_curves • \$ssl_session_reused

Table 4-18 PremiumWafServer

Parameter	Type	Description
front_protocol	String	Protocol used by the client to request access to the origin server. Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
back_protocol	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
weight	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is 1 . This field is not included by cloud WAF.

Parameter	Type	Description
address	String	IP address of your origin server requested by the client
port	Integer	Port used by WAF to forward client requests to the origin server
type	String	The origin server address is an IPv4 or IPv6 address. Enumeration values: <ul style="list-style-type: none"> • ipv4 • ipv6
vpc_id	String	VPC ID. To obtain the VPC ID, perform the following steps: Use either of the following methods to obtain the VPC ID. <ul style="list-style-type: none"> • Log in to the WAF console and choose Instance Management > Dedicated Engine > VPC\Subnet. The VPC ID is in the VPC\Subnet column. • Log in to the VPC console and click the VPC name. On the page displayed, copy the ID in the VPC Information area.

Table 4-19 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. <ul style="list-style-type: none"> • true: The website passed the PCI 3DS certification check. • false: The website failed the PCI 3DS certification check. Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
pci_dss	String	Whether the website passed the PCI DSS certification check. <ul style="list-style-type: none"> • true: The website passed the PCI DSS certification check. • false: The website failed the PCI DSS certification check. Enumeration values: <ul style="list-style-type: none"> • true • false
cname	String	The CNAME record being used. <ul style="list-style-type: none"> • old: The old CNAME record is used. • new: The new CNAME record is used. Enumeration values: <ul style="list-style-type: none"> • old • new
is_dual_az	String	Whether WAF support Multi-AZ DR <ul style="list-style-type: none"> • true: WAF supports multi-AZ DR. • false: WAF does not support multi-AZ DR. Enumeration values: <ul style="list-style-type: none"> • true • false
ipv6	String	Whether IPv6 protection is supported. <ul style="list-style-type: none"> • true: IPv6 protection is supported. • false: IPv6 protection is not supported. Enumeration values: <ul style="list-style-type: none"> • true • false

Table 4-20 BlockPage

Parameter	Type	Description
template	String	Template name
custom_page	CustomPage object	Custom alarm page
redirect_url	String	URL of the redirected page

Table 4-21 CustomPage

Parameter	Type	Description
status_code	String	Status Codes
content_type	String	The content type of the custom alarm page. The value can be text/html , text/xml , or application/json .
content	String	The page content based on the selected page type. For details, see the <i>Web Application Firewall (WAF) User Guide</i> .

Status code: 400

Table 4-22 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-23 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-24 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to add a website domain name to a dedicated WAF instance in a specific project. The project ID is specified by `project_id`, and the

domain name is www.demo.com. The client protocol and server protocol is HTTP. The origin server address is ipv4 x.x.x.x. The service port used by WAF to forward client requests to the origin server is 80. The ID of the VPC where the dedicated WAF instance is deployed is cf6dbace-b36a-4d51-ae04-52a3319ae247.

```
POST https://{Endpoint}/v1/{project_id}/premium-waf/host?enterprise_project_id=0
{
  "hostname": "www.demo.com",
  "server": [ {
    "front_protocol": "HTTP",
    "back_protocol": "HTTP",
    "vpc_id": "cf6dbace-b36a-4d51-ae04-52a3319ae247",
    "type": "ipv4",
    "address": "x.x.x.x",
    "port": 80
  } ],
  "proxy": false,
  "description": ""
}
```

Example Responses

Status code: 200

OK

```
{
  "id": "51a5649e52d341a9bb802044950969dc",
  "hostname": "www.demo.com",
  "protocol": "HTTP",
  "server": [ {
    "address": "x.x.x.x",
    "port": 80,
    "type": "ipv4",
    "weight": 1,
    "front_protocol": "HTTP",
    "back_protocol": "HTTP",
    "vpc_id": "cf6dbace-b36a-4d51-ae04-52a3319ae247"
  } ],
  "proxy": false,
  "locked": 0,
  "timestamp": 1650596007113,
  "flag": {
    "pci_3ds": "false",
    "pci_dss": "false"
  },
  "description": "",
  "policyid": "1607df035bc847b582ce9c838c083b88",
  "domainid": "d4ecb00b031941ce9171b7bc3386883f",
  "enterprise_project_id": "0",
  "protect_status": 1,
  "access_status": 0
}
```

Status Codes

Status Code	Description
200	OK
400	Invalid request.

Status Code	Description
401	The token does not have the required permission.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.1.3 Modifying a Domain Name Protected by a Dedicated WAF Instance

Function

This API is used to update configurations of domain names protected with a dedicated WAF instance. The new origin server information will overwrite the old origin server information. If you want to keep the old information, provide them as new data. You can provide only the updated information in the request body.

URI

PUT /v1/{project_id}/premium-waf/host/{host_id}

Table 4-25 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
host_id	Yes	String	ID of the domain name protected by the dedicated WAF engine

Table 4-26 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-27 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-28 Request body parameters

Parameter	Mandatory	Type	Description
proxy	No	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> • false: No proxy is used. • true: A proxy is used.
certificateid	No	String	Certificate ID. It can be obtained by calling the ListCertificates API. <ul style="list-style-type: none"> • This parameter is not required when the client protocol is HTTP. • This parameter is mandatory when the client protocol is HTTPS.
certificatenam e	No	String	Certificate name. <ul style="list-style-type: none"> • This parameter is not required when the client protocol is HTTP. • This parameter is mandatory when the client protocol is HTTPS.

Parameter	Mandatory	Type	Description
tls	No	String	TLS version. TLS v1.0 is supported by default. Enumeration values: <ul style="list-style-type: none">• TLS v1.0• TLS v1.1• TLS v1.2

Parameter	Mandatory	Type	Description
cipher	No	String	<p>Cipher suite. The value can be cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default:</p> <ul style="list-style-type: none"> cipher_1: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH • cipher_2: ECDH+AESGCM:EDH+AESGCM • cipher_3: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH • cipher_4: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH • cipher_default: The cryptographic algorithms are ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. <p>Enumeration values:</p> <ul style="list-style-type: none"> • cipher_1 • cipher_2 • cipher_3 • cipher_4 • cipher_default
mode	No	String	<p>Special domain name node in dedicated mode. This parameter is required only for special WAF modes, such as ELB.</p>

Parameter	Mandatory	Type	Description
locked	No	Integer	This parameter is reserved, which will be used to freeze a domain name.
protect_status	No	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	No	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
timestamp	No	Integer	Timestamp.
pool_ids	No	Array of strings	Dedicated engine group the domain name was added to. This parameter is required only in special WAF mode, such as ELB mode.
block_page	No	BlockPage object	Alarm page configuration
traffic_mark	No	TrafficMark object	Traffic identifier
circuit_breaker	No	CircuitBreaker object	Circuit breaker configuration
timeout_config	No	TimeoutConfig object	Timeout settings
flag	No	HostFlag object	Feature switch for configuring compliance certification checks for domain names protected with the dedicated WAF instance.

Parameter	Mandatory	Type	Description
forward_header_map	No	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: <ul style="list-style-type: none"> • \$time_local • \$request_id • \$connection_requests • \$tenant_id • \$project_id • \$remote_addr • \$remote_port • \$scheme • \$request_method • \$http_host • \$origin_uri • \$request_length • \$ssl_server_name • \$ssl_protocol • \$ssl_curves • \$ssl_session_reused

Table 4-29 BlockPage

Parameter	Mandatory	Type	Description
template	Yes	String	Template name
custom_page	No	CustomPage object	Custom alarm page
redirect_url	No	String	URL of the redirected page

Table 4-30 CustomPage

Parameter	Mandatory	Type	Description
status_code	Yes	String	Status Codes

Parameter	Mandatory	Type	Description
content_type	Yes	String	The content type of the custom alarm page. The value can be text/html , text/xml , or application/json .
content	Yes	String	The page content based on the selected page type. For details, see the <i>Web Application Firewall (WAF) User Guide</i> .

Table 4-31 TrafficMark

Parameter	Mandatory	Type	Description
sip	No	Array of strings	IP tag. HTTP request header field of the original client IP address.
cookie	No	String	Session tag. This tag is used by known attack source rules to block malicious attacks based on cookie attributes. This parameter must be configured in known attack source rules to block requests based on cookie attributes.
params	No	String	User tag. This tag is used by known attack source rules to block malicious attacks based on params attributes. This parameter must be configured to block requests based on the params attributes.

Table 4-32 CircuitBreaker

Parameter	Mandatory	Type	Description
switch	No	Boolean	Whether to enable connection protection. <ul style="list-style-type: none"> • true: Enable connection protection. • false: Disable the connection protection.

Parameter	Mandatory	Type	Description
dead_num	No	Integer	502/504 error threshold. 502/504 errors allowed for every 30 seconds.
dead_ratio	No	Number	A breakdown protection is triggered when the 502/504 error threshold and percentage threshold have been reached.
block_time	No	Integer	Protection period upon the first breakdown. During this period, WAF stops forwarding client requests.
superposition_num	No	Integer	The maximum multiplier you can use for consecutive breakdowns. The number of breakdowns are counted from 0 every time the accumulated breakdown protection duration reaches 3,600s. For example, assume that Initial Downtime (s) is set to 180s and Multiplier for Consecutive Breakdowns is set to 3. If the breakdown is triggered for the second time, that is, less than 3, the protection duration is 360s (180s X 2). If the breakdown is triggered for the third or fourth time, that is, equal to or greater than 3, the protection duration is 540s (180s X 3). When the accumulated downtime duration exceeds 1 hour (3,600s), the number of breakdowns are counted from 0.
suspend_num	No	Integer	Threshold of the number of pending URL requests. Connection protection is triggered when the threshold has been reached.

Parameter	Mandatory	Type	Description
sus_block_time	No	Integer	Downtime duration after the connection protection is triggered. During this period, WAF stops forwarding website requests.

Table 4-33 TimeoutConfig

Parameter	Mandatory	Type	Description
connect_timeout	No	Integer	Timeout for WAF to connect to the origin server.
send_timeout	No	Integer	Timeout for WAF to send requests to the origin server.
read_timeout	No	Integer	Timeout for WAF to receive responses from the origin server.

Table 4-34 HostFlag

Parameter	Mandatory	Type	Description
pci_3ds	No	String	<p>Status of the PCI 3DS compliance certification check. The value can be:</p> <ul style="list-style-type: none"> • true: enabled. • false: disabled. This parameter must be used together with tls and cipher. tls must be set to TLS v1.2, and cipher must be set to cipher_2. Note: The PCI 3DS compliance certification check cannot be disabled after being enabled. Before enabling the check, read the corresponding description in the WAF documentation in Help Center. <p>Enumeration values:</p> <ul style="list-style-type: none"> • true • false

Parameter	Mandatory	Type	Description
pci_dss	No	String	<p>Status of the PCI DSS compliance certification check. The value can be:</p> <ul style="list-style-type: none"> • true: enabled. • false: disabled. This parameter must be used together with tls and cipher. tls must be set to TLS v1.2, and cipher must be set to cipher_2. Note: Before enabling the check, read the corresponding description in WAF documentation in Help Center. <p>Enumeration values:</p> <ul style="list-style-type: none"> • true • false

Response Parameters

Status code: 200

Table 4-35 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name added to the dedicated WAF instance
protocol	String	Client protocol, which is the protocol used by a client (for example, a browser) to access your website.
server	Array of PremiumWaf Server objects	Origin server configuration of the protected domain name
proxy	Boolean	<p>Whether a proxy is used for the protected domain name.</p> <ul style="list-style-type: none"> • false: No proxy is used. • true: A proxy is used.
locked	Integer	<p>This parameter is reserved, which will be used to freeze a domain name.</p> <p>Default: 0</p>

Parameter	Type	Description
timestamp	Long	Time the domain name was added to WAF.
tls	String	<p>Minimum TLS version. The value can be TLS v1.0, TLS v1.1, or TLS v1.2. TLS v1.0 is used by default.</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • TLS v1.0 • TLS v1.1 • TLS v1.2
cipher	String	<p>Cipher suite. The value can be cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default: cipher_1: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH</p> <ul style="list-style-type: none"> • cipher_2: ECDH+AESGCM:EDH+AESGCM • cipher_3: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH • cipher_4: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH • cipher_default: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. <p>Enumeration values:</p> <ul style="list-style-type: none"> • cipher_1 • cipher_2 • cipher_3 • cipher_4 • cipher_default
extend	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.
flag	Flag object	Special identifier, which is used on the console.
description	String	Domain name description

Parameter	Type	Description
policyid	String	ID of the policy initially used to the domain name. You can call the ListPolicy API to query the policy list and view the ID of the specific policy.
domainid	String	Account ID, which is the same as the account ID on the My Credentials page. To go to this page, log in to Cloud management console, hover the cursor over your username, and click My Credentials in the displayed window.
projectid	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
enterprise_project_id	String	Enterprise project ID. To obtain the ID, log in to the Cloud management console first. On the menu bar at the top of the page, choose Enterprise > Project Management . Then, click the project name and view the ID.
certificateid	String	HTTPS certificate ID.
certificatename	String	Certificate name
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> ● 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
lb_algorithm	String	Load balancing algorithm. Weighted round robin is used by default and cannot be changed.
block_page	BlockPage object	Alarm page configuration

Parameter	Type	Description
traffic_mark	TrafficMark object	Traffic identifier
timeout_config	TimeoutConfig object	Timeout settings
forward_header_map	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: <ul style="list-style-type: none"> • \$time_local • \$request_id • \$connection_requests • \$tenant_id • \$project_id • \$remote_addr • \$remote_port • \$scheme • \$request_method • \$http_host • \$origin_uri • \$request_length • \$ssl_server_name • \$ssl_protocol • \$ssl_curves • \$ssl_session_reused
access_progress	Array of Access_progress objects	Access progress, which is used only for the new WAF console.

Table 4-36 PremiumWafServer

Parameter	Type	Description
front_protocol	String	Protocol used by the client to request access to the origin server. Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS

Parameter	Type	Description
back_protocol	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
weight	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is 1 . This field is not included by cloud WAF.
address	String	IP address of your origin server requested by the client
port	Integer	Port used by WAF to forward client requests to the origin server
type	String	The origin server address is an IPv4 or IPv6 address. Enumeration values: <ul style="list-style-type: none"> • ipv4 • ipv6
vpc_id	String	VPC ID. To obtain the VPC ID, perform the following steps: Use either of the following methods to obtain the VPC ID. <ul style="list-style-type: none"> • Log in to the WAF console and choose Instance Management > Dedicated Engine > VPC\Subnet. The VPC ID is in the VPC\Subnet column. • Log in to the VPC console and click the VPC name. On the page displayed, copy the ID in the VPC Information area.

Table 4-37 Flag

Parameter	Type	Description
pci_3ds	String	<p>Whether the website passes the PCI 3DS certification check.</p> <ul style="list-style-type: none"> ● true: The website passed the PCI 3DS certification check. ● false: The website failed the PCI 3DS certification check. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
pci_dss	String	<p>Whether the website passed the PCI DSS certification check.</p> <ul style="list-style-type: none"> ● true: The website passed the PCI DSS certification check. ● false: The website failed the PCI DSS certification check. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
cname	String	<p>The CNAME record being used.</p> <ul style="list-style-type: none"> ● old: The old CNAME record is used. ● new: The new CNAME record is used. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	<p>Whether WAF support Multi-AZ DR</p> <ul style="list-style-type: none"> ● true: WAF supports multi-AZ DR. ● false: WAF does not support multi-AZ DR. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
ipv6	String	<p>Whether IPv6 protection is supported.</p> <ul style="list-style-type: none"> ● true: IPv6 protection is supported. ● false: IPv6 protection is not supported. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false

Table 4-38 BlockPage

Parameter	Type	Description
template	String	Template name
custom_page	CustomPage object	Custom alarm page
redirect_url	String	URL of the redirected page

Table 4-39 CustomPage

Parameter	Type	Description
status_code	String	Status Codes
content_type	String	The content type of the custom alarm page. The value can be text/html , text/xml , or application/json .
content	String	The page content based on the selected page type. For details, see the <i>Web Application Firewall (WAF) User Guide</i> .

Table 4-40 TrafficMark

Parameter	Type	Description
sip	Array of strings	IP tag. HTTP request header field of the original client IP address.
cookie	String	Session tag. This tag is used by known attack source rules to block malicious attacks based on cookie attributes. This parameter must be configured in known attack source rules to block requests based on cookie attributes.
params	String	User tag. This tag is used by known attack source rules to block malicious attacks based on params attributes. This parameter must be configured to block requests based on the params attributes.

Table 4-41 TimeoutConfig

Parameter	Type	Description
connect_time out	Integer	Timeout for WAF to connect to the origin server.

Parameter	Type	Description
send_timeout	Integer	Timeout for WAF to send requests to the origin server.
read_timeout	Integer	Timeout for WAF to receive responses from the origin server.

Table 4-42 Access_progress

Parameter	Type	Description
step	Integer	Procedure <ul style="list-style-type: none"> • 1: Whitelisting the WAF IP addresses. • 2: Testing connectivity. • 3: Modifying DNS records.
status	Integer	Status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The step has not been finished. • 1: The step has finished.

Status code: 400

Table 4-43 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-44 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-45 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to change proxy settings for a dedicated WAF instance. The project ID is specified by `project_id`. The domain name ID is specified by `host_id`. Proxy settings: No proxy is used.

```
PUT https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}?enterprise_project_id=0
{
  "proxy": false
}
```

Example Responses

Status code: 200

OK

```
{
  "id": "27995fb98a2d4928a1e453e65ee8117a",
  "hostname": "www.demo.com",
  "protocol": "HTTP",
  "server": [ {
    "address": "192.168.0.209",
    "port": 80,
    "type": "ipv4",
    "weight": 1,
    "front_protocol": "HTTP",
    "back_protocol": "HTTP",
    "vpc_id": "cf6dbace-b36a-4d51-ae04-52a8459ae247"
  } ],
  "proxy": false,
  "locked": 0,
  "timestamp": 1650590814885,
  "flag": {
    "pci_3ds": "false",
    "pci_dss": "false"
  },
  "description": "",
  "policyid": "9555cda636ef4ca294dfe4b14bc94c47",
  "domainid": "d4ecb00b031941ce9171b7bc3386883f",
  "projectid": "05e33ecd328025dd2f7fc00696201fb4",
  "enterprise_project_id": "0",
  "protect_status": 1,
  "access_status": 0
}
```

Status Codes

Status Code	Description
200	OK
400	Invalid request.
401	The token does not have the required permission.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.1.4 Querying Domain Name Settings in Dedicated Mode

Function

This API is used to query settings of domain names protected with dedicated WAF instances.

URI

GET /v1/{project_id}/premium-waf/host/{host_id}

Table 4-46 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
host_id	Yes	String	ID of the domain name protected by the dedicated WAF engine

Table 4-47 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-48 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

Table 4-49 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name added to the dedicated WAF instance
protocol	String	Client protocol, which is the protocol used by a client (for example, a browser) to access your website.
server	Array of PremiumWafServer objects	Origin server configuration of the protected domain name
proxy	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> ● false: No proxy is used. ● true: A proxy is used.

Parameter	Type	Description
locked	Integer	This parameter is reserved, which will be used to freeze a domain name. Default: 0
timestamp	Long	Time the domain name was added to WAF.
tls	String	Minimum TLS version. You can use TLS v1.0, TLS v1.1, or TLS v1.2. TLS v1.0 is used by default. Parameter tls is required only when the client protocol is HTTPS. Enumeration values: <ul style="list-style-type: none"> • TLS v1.0 • TLS v1.1 • TLS v1.2
cipher	String	Parameter cipher is required only when the client protocol is HTTPS. The value can be cipher_1 , cipher_2 , cipher_3 , cipher_4 , or cipher_default . <ul style="list-style-type: none"> • cipher_1: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH • cipher_2: ECDH+AESGCM:EDH+AESGCM • cipher_3: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH • cipher_4: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH • cipher_default: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. Enumeration values: <ul style="list-style-type: none"> • cipher_1 • cipher_2 • cipher_3 • cipher_4 • cipher_default
extend	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.

Parameter	Type	Description
flag	Flag object	Special identifier, which is used on the console.
description	String	Domain name description
policyid	String	ID of the policy initially used to the domain name. You can call the ListPolicy API to query the policy list and view the ID of the specific policy.
domainid	String	Account ID, which is the same as the account ID on the My Credentials page. To go to this page, log in to Cloud management console, hover the cursor over your username, and click My Credentials in the displayed window.
projectid	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
enterprise_project_id	String	Enterprise project ID. To obtain the ID, log in to the Cloud management console first. On the menu bar at the top of the page, choose Enterprise > Project Management . Then, click the project name and view the ID.
certificateid	String	HTTPS certificate ID.
certificatename	String	Certificate name
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> ● 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
block_page	BlockPage object	Alarm page configuration

Parameter	Type	Description
traffic_mark	TrafficMark object	Traffic identifier
timeout_config	TimeoutConfig object	Timeout settings
forward_header_map	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: <ul style="list-style-type: none"> • \$time_local • \$request_id • \$connection_requests • \$tenant_id • \$project_id • \$remote_addr • \$remote_port • \$scheme • \$request_method • \$http_host • \$origin_uri • \$request_length • \$ssl_server_name • \$ssl_protocol • \$ssl_curves • \$ssl_session_reused
access_progress	Array of AccessProgress objects	Access progress, which is used only for the new WAF console.

Table 4-50 PremiumWafServer

Parameter	Type	Description
front_protocol	String	Protocol used by the client to request access to the origin server. Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS

Parameter	Type	Description
back_protocol	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
weight	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is 1 . This field is not included by cloud WAF.
address	String	IP address of your origin server requested by the client
port	Integer	Port used by WAF to forward client requests to the origin server
type	String	The origin server address is an IPv4 or IPv6 address. Enumeration values: <ul style="list-style-type: none"> • ipv4 • ipv6
vpc_id	String	VPC ID. To obtain the VPC ID, perform the following steps: Use either of the following methods to obtain the VPC ID. <ul style="list-style-type: none"> • Log in to the WAF console and choose Instance Management > Dedicated Engine > VPC\Subnet. The VPC ID is in the VPC\Subnet column. • Log in to the VPC console and click the VPC name. On the page displayed, copy the ID in the VPC Information area.

Table 4-51 Flag

Parameter	Type	Description
pci_3ds	String	<p>Whether the website passes the PCI 3DS certification check.</p> <ul style="list-style-type: none"> ● true: The website passed the PCI 3DS certification check. ● false: The website failed the PCI 3DS certification check. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
pci_dss	String	<p>Whether the website passed the PCI DSS certification check.</p> <ul style="list-style-type: none"> ● true: The website passed the PCI DSS certification check. ● false: The website failed the PCI DSS certification check. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
cname	String	<p>The CNAME record being used.</p> <ul style="list-style-type: none"> ● old: The old CNAME record is used. ● new: The new CNAME record is used. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	<p>Whether WAF support Multi-AZ DR</p> <ul style="list-style-type: none"> ● true: WAF supports multi-AZ DR. ● false: WAF does not support multi-AZ DR. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
ipv6	String	<p>Whether IPv6 protection is supported.</p> <ul style="list-style-type: none"> ● true: IPv6 protection is supported. ● false: IPv6 protection is not supported. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false

Table 4-52 BlockPage

Parameter	Type	Description
template	String	Template name
custom_page	CustomPage object	Custom alarm page
redirect_url	String	URL of the redirected page

Table 4-53 CustomPage

Parameter	Type	Description
status_code	String	Status Codes
content_type	String	The content type of the custom alarm page. The value can be text/html , text/xml , or application/json .
content	String	The page content based on the selected page type. For details, see the <i>Web Application Firewall (WAF) User Guide</i> .

Table 4-54 TrafficMark

Parameter	Type	Description
sip	Array of strings	IP tag. HTTP request header field of the original client IP address.
cookie	String	Session tag. This tag is used by known attack source rules to block malicious attacks based on cookie attributes. This parameter must be configured in known attack source rules to block requests based on cookie attributes.
params	String	User tag. This tag is used by known attack source rules to block malicious attacks based on params attributes. This parameter must be configured to block requests based on the params attributes.

Table 4-55 TimeoutConfig

Parameter	Type	Description
connect_time out	Integer	Timeout for WAF to connect to the origin server.

Parameter	Type	Description
send_timeout	Integer	Timeout for WAF to send requests to the origin server.
read_timeout	Integer	Timeout for WAF to receive responses from the origin server.

Table 4-56 Access_progress

Parameter	Type	Description
step	Integer	Procedure <ul style="list-style-type: none"> • 1: Whitelisting the WAF IP addresses. • 2: Testing connectivity. • 3: Modifying DNS records.
status	Integer	Status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The step has not been finished. • 1: The step has finished.

Status code: 400

Table 4-57 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-58 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-59 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following shows how to query configurations of a domain name protected with a dedicated WAF instance in a specific project. The project ID is specified by `project_id`, and the domain ID is specified by `host_id`.

```
GET https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "id" : "ee896796e1a84f3f85865ae0853d8974",
  "hostname" : "www.demo.com",
  "protocol" : "HTTPS",
  "server" : [ {
    "address" : "1.2.3.4",
    "port" : 443,
    "type" : "ipv4",
    "weight" : 1,
    "front_protocol" : "HTTPS",
    "back_protocol" : "HTTPS",
    "vpc_id" : "ebfc553a-386d-4746-b0c2-18ff3f0e903d"
  } ],
  "proxy" : false,
  "locked" : 0,
  "timestamp" : 1650593801380,
  "tls" : "TLS v1.0",
  "cipher" : "cipher_1",
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false"
  },
  "description" : "",
  "policyid" : "df15d0eb84194950a8fdc615b6c012dc",
  "domainid" : "0ee78615ca08419f81f539d97c9ee353",
  "projectid" : "550500b49078408682d0d4f7d923f3e1",
  "protect_status" : 1,
  "access_status" : 0,
  "certificateid" : "360f992501a64de0a65c50a64d1ca7b3",
  "certificatename" : "certificatename75315"
}
```

Status Codes

Status Code	Description
200	OK

Status Code	Description
400	Invalid request
401	The token does not have the required permission.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.1.5 Deleting a Domain Name from a Dedicated WAF Instance

Function

This API is used to delete a domain name protected with a dedicated WAF instance.

URI

DELETE /v1/{project_id}/premium-waf/host/{host_id}

Table 4-60 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
host_id	Yes	String	ID of the domain name protected by the dedicated WAF engine

Table 4-61 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Parameter	Mandatory	Type	Description
keepPolicy	No	Boolean	Whether to retain the rule. false : The policy for the domain name will not be retained. true : The policy for the domain name will be retained. If the policy used for the domain name you want to delete is also used for other domain names, this parameter must be left blank. Default: 1

Request Parameters

Table 4-62 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

Table 4-63 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
extend	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.

Parameter	Type	Description
region	String	Region ID. This parameter is included when the domain name was added to WAF through the console. This parameter is left blank when the domain name was added to WAF by calling an API. You can query the region ID on the Regions and Endpoints page on the website.
flag	Flag object	Special identifier, which is used on the console.
description	String	Domain name description
policyid	String	ID of the policy initially used to the domain name. You can call the ListPolicy API to query the policy list and view the ID of a specific policy.
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
host_id	String	Domain name ID, which is the same as the value of <i>*id</i> . This field is redundant.

Table 4-64 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. <ul style="list-style-type: none"> • true: The website passed the PCI 3DS certification check. • false: The website failed the PCI 3DS certification check. Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
pci_dss	String	Whether the website passed the PCI DSS certification check. <ul style="list-style-type: none"> ● true: The website passed the PCI DSS certification check. ● false: The website failed the PCI DSS certification check. Enumeration values: <ul style="list-style-type: none"> ● true ● false
cname	String	The CNAME record being used. <ul style="list-style-type: none"> ● old: The old CNAME record is used. ● new: The new CNAME record is used. Enumeration values: <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	Whether WAF support Multi-AZ DR <ul style="list-style-type: none"> ● true: WAF supports multi-AZ DR. ● false: WAF does not support multi-AZ DR. Enumeration values: <ul style="list-style-type: none"> ● true ● false
ipv6	String	Whether IPv6 protection is supported. <ul style="list-style-type: none"> ● true: IPv6 protection is supported. ● false: IPv6 protection is not supported. Enumeration values: <ul style="list-style-type: none"> ● true ● false

Status code: 400

Table 4-65 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-66 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-67 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following shows how to remove a domain name from a dedicated WAF instance in a specific project. The project ID is specified by `project_id`, and the domain ID is specified by `host_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "id": "ee896796e1a84f3f85865ae0853d8974",
  "hostname": "www.demo.com",
  "region": "cn-north-4",
  "flag": {
    "pci_3ds": "false",
    "pci_dss": "false"
  },
  "description": "",
  "policyid": "df15d0eb84194950a8fdc615b6c012dc",
  "protect_status": 1,
  "access_status": 0,
  "hostid": "ee896796e1a84f3f85865ae0853d8974"
}
```

Status Codes

Status Code	Description
200	OK
400	Invalid request

Status Code	Description
401	The token does not have the required permission.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.1.6 Modifying the Protection Status of a Domain Name in Dedicated Mode

Function

This API is used to modify the protection status of a domain name connected to a dedicated WAF instance.

URI

PUT /v1/{project_id}/premium-waf/host/{host_id}/protect-status

Table 4-68 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
host_id	Yes	String	ID of the domain name protected by the dedicated WAF engine

Table 4-69 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-70 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Table 4-71 Request body parameters

Parameter	Mandatory	Type	Description
protect_status	Yes	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.

Response Parameters

Status code: 200

Table 4-72 Response body parameters

Parameter	Type	Description
protect_status	Integer	<p>WAF status of the protected domain name.</p> <ul style="list-style-type: none"> • -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.

Status code: 400

Table 4-73 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-74 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-75 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following shows how to change the protection status of a dedicated WAF instance to enabled for a domain name in a specific project. The project ID is specified by `project_id`, and the domain ID is specified by `host_id`.

```
PUT https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}/protect-status?enterprise_project_id=0
{
  "protect_status" : 1
}
```

Example Responses

Status code: 200

OK

```
{
  "protect_status" : 1
}
```

Status Codes

Status Code	Description
200	OK
400	Invalid request
401	The token does not have the required permission.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2 Rule Management

4.2.1 Changing the Status of a Rule

Function

This API is used to change the status of a single rule, for example, disabling a Precise Protection rule.

URI

```
PUT /v1/{project_id}/waf/policy/{policy_id}/{ruletype}/{rule_id}/status
```

Table 4-76 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.
ruletype	Yes	String	Policy Type Enumeration values: <ul style="list-style-type: none"> • whiteblackip • geoip • privacy • antitamper • custom • ignore • cc
rule_id	Yes	String	Rule ID. It can be obtained by calling the specific API that is used to obtain the rule list of a certain type. For example, you can call the ListWhiteblackipRule API to obtain the ID of a blacklist or whitelist rule.

Table 4-77 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-78 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-79 Request body parameters

Parameter	Mandatory	Type	Description
status	No	Integer	Status. The options are 0 and 1 . 0 : Disabled. 1 : Enabled.

Response Parameters

Status code: 200

Table 4-80 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
timestamp	Long	Time when the rule was created.
description	String	Rule Description
status	Integer	Status. The options are 0 and 1 . 0 : Disabled. 1 : Enabled.

Status code: 400

Table 4-81 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Status code: 401

Table 4-82 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-83 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to change the protection status of a rule to disabled. Details about the rule are specified by project_id, policy_id, ruletype, and rule_id.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/{ruletype}/{rule_id}/status?
enterprise_project_id=0

{
  "status" : 0
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "709bfd0d62a9410394ffa9e25eb82c36",
  "policyid" : "62fd7f8c36234a4ebedabc2ce451ed45",
  "timestamp" : 1650362797070,
  "description" : "demo",
  "status" : 0
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.2 Querying CC Attack Protection Rules

Function

This API is used to query the list of CC attack protection rules.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/cc

Table 4-84 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.

Table 4-85 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
offset	Yes	Integer	Offset. The records after the offset are queried.
limit	Yes	Integer	Maximum number of records that can be returned.

Request Parameters

Table 4-86 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-87 Response body parameters

Parameter	Type	Description
total	Integer	Number of rules in the policy
items	Array of CcrulesListInfo objects	Array of Cc rules

Table 4-88 CcrulesListInfo

Parameter	Type	Description
name	String	Rule name.

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
url	String	When the value of mode is 0, this parameter has a return value. URL to which the rule applies, excluding a domain name.
prefix	Boolean	Whether a prefix is used for the path. If the protected URL ends with an asterisk (*), a path prefix is used. When the value of mode is 0, this parameter has a return value.
mode	Integer	CC rule protection mode, which corresponds to mode on the console. Currently, only advanced CC rule protection mode is supported. <ul style="list-style-type: none"> 0: standard. Only the protection path of the domain name can be restricted. 1: advanced. The path, IP address, cookie, header, and params fields can be restricted. Enumeration values: <ul style="list-style-type: none"> 0 1
status	Integer	Rule status. The value can be 0 or 1. <ul style="list-style-type: none"> 0: The rule is disabled. 1: The rule is enabled.
conditions	Array of CcCondition objects	Condition list. This parameter is returned when mode is set to 1.
action	action object	Action to take if the number of requests reaches the upper limit.

Parameter	Type	Description
tag_type	String	<p>Limit mode.</p> <ul style="list-style-type: none"> ● ip: IP-based rate limiting. Website visitors are identified by IP address. ● cookie: User-based rate limiting. Website visitors are identified by the cookie key value. ● other: Website visitors are identified by the Referer field (user-defined request source). ● policy: Policy-based rate limiting ● domain: Domain name rate limit ● url: URL rate limit <p>Enumeration values:</p> <ul style="list-style-type: none"> ● ip ● cookie ● header ● other ● policy ● domain ● url
tag_index	String	<p>User identifier. This parameter is mandatory when the rate limit mode is set to user (cookie or header).</p> <ul style="list-style-type: none"> ● cookie: Set the cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the name field in the cookie to uniquely identify a website visitor, select name. ● header: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.
tag_condition	tag_condition object	<p>User tag. This parameter is mandatory when the rate limit mode is set to other. -other: A website visitor is identified by the Referer field (user-defined request source).</p>
limit_num	Integer	<p>Rate limit frequency based on the number of requests. The value ranges from 1 to 2,147,483,647.</p>

Parameter	Type	Description
limit_period	Integer	Rate limit period, in seconds. The value ranges from 1 to 3,600.
unlock_num	Integer	Allowable frequency based on the number of requests. The value ranges from 0 to 2,147,483,647. This parameter is required only when the protection action type is dynamic_block .
lock_time	Integer	Block duration, in seconds. The value ranges from 0 to 65,535. Access requests are blocked during the configured block duration, and an error page is displayed.
domain_aggregation	Boolean	Whether to enable domain name aggregation statistics
region_aggregation	Boolean	Whether to enable global counting.
description	String	Rule description.
total_num	Integer	This parameter is reserved and can be ignored currently.
unaggregation	Boolean	This parameter is reserved and can be ignored currently.
aging_time	Integer	Rule aging time. This parameter is reserved and can be ignored currently.
producer	Integer	Rule creation object. This parameter is reserved and can be ignored currently.
timestamp	Long	Timestamp the rule is created.

Table 4-89 CcCondition

Parameter	Type	Description
category	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • ip • ipv6 • params • cookie • header • response_code

Parameter	Type	Description
logic_operation	String	<p>Logic for matching the condition.</p> <ul style="list-style-type: none"> If the category is url, the optional operations are contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal and len_not_equal If the category is ip, the optional operations are: equal, not_equal, , equal_any and not_equal_all If the category is params, cookie and header, the optional operations are: contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist and not_exist
contents	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.
index	String	Subfield. When Field Type is set to params, cookie, or header, set this parameter based on the site requirements and this parameter is mandatory.

Table 4-90 action

Parameter	Type	Description
category	String	<p>Action type:</p> <ul style="list-style-type: none"> • captcha: Verification code. WAF requires visitors to enter a correct verification code to continue their access to requested page on your website. • block: WAF blocks the requests. When tag_type is set to other, the value can only be block. • log: WAF logs the event only. • dynamic_block: In the previous rate limit period, if the request frequency exceeds the value of Rate Limit Frequency, the request is blocked. In the next rate limit period, if the request frequency exceeds the value of Permit Frequency, the request is still blocked. Note: The dynamic_block protection action can be set only when the advanced protection mode is enabled for the CC protection rule. <p>Enumeration values:</p> <ul style="list-style-type: none"> • captcha • block • log • dynamic_block
detail	detail object	<p>Block page information. When protection action category is set to block or dynamic_block, you need to set the returned block page.</p> <ul style="list-style-type: none"> • If you want to use the default block page, this parameter can be excluded. • If you want to use a custom block page, set this parameter.

Table 4-91 detail

Parameter	Type	Description
response	response object	Block Page.

Table 4-92 response

Parameter	Type	Description
content_type	String	Content type. The value can only be application/json , text/html , or text/xml . Enumeration values: <ul style="list-style-type: none"> • application/json • text/html • text/xml
content	String	Block page information.

Table 4-93 tag_condition

Parameter	Type	Description
category	String	User identifier. The value is fixed at referer .
contents	Array of strings	Content of the user identifier field.

Status code: 400

Table 4-94 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-95 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-96 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the CC attack protection rule list. Details about the query are specified by project_id and policy_id.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/cc?offset=0&limit=1
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total": 1,
  "items": [ {
    "id": "f88c5eabff9b4ff9ba6e7dd8e38128ba",
    "policyid": "d471eef691684f1c8d7784532fd8f4bd",
    "timestamp": 1678873040603,
    "name": "test",
    "description": "",
    "status": 1,
    "mode": 1,
    "conditions": [ {
      "category": "url",
      "contents": [ "/url" ],
      "logic_operation": "contain"
    } ],
    "action": {
      "category": "captcha"
    },
    "producer": 1,
    "unaggregation": false,
    "total_num": 0,
    "limit_num": 10,
    "limit_period": 60,
    "lock_time": 0,
    "tag_type": "ip",
    "aging_time": 0,
    "region_aggregation": false,
    "domain_aggregation": false
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.

Status Code	Description
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.3 Creating a CC Attack Protection Rule

Function

This API is used to create a CC attack protection rule.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/cc

Table 4-97 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.

Table 4-98 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-99 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-100 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Rule name.
mode	Yes	Integer	Work mode. The value can be 0 (standard) or 1 (advanced). The parameters of the advanced mode cannot be described in the same document of the same API. For details, see this parameter on the console page. Enumeration values: <ul style="list-style-type: none">• 0• 1
conditions	Yes	Array of CcCondition objects	Condition list. This parameter is returned when mode is set to 1.
action	Yes	action object	Action to take if the number of requests reaches the upper limit.

Parameter	Mandatory	Type	Description
tag_type	Yes	String	<p>Limit mode.</p> <ul style="list-style-type: none"> • ip: IP-based rate limiting. Website visitors are identified by IP address. • cookie: User-based rate limiting. Website visitors are identified by the cookie key value. • other: Website visitors are identified by the Referer field (user-defined request source). • policy: Policy-based rate limiting • domain: Domain name rate limit • url: URL rate limit <p>Enumeration values:</p> <ul style="list-style-type: none"> • ip • cookie • header • other • policy • domain • url

Parameter	Mandatory	Type	Description
tag_index	No	String	<p>User identifier. This parameter is mandatory when the rate limit mode is set to user (cookie or header).</p> <ul style="list-style-type: none"> • cookie: Set the cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the name field in the cookie to uniquely identify a website visitor, select name. • header: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.
tag_condition	No	tag_condition object	User tag. This parameter is mandatory when the rate limit mode is set to other . -other: A website visitor is identified by the Referer field (user-defined request source).
limit_num	Yes	Integer	Rate limit frequency based on the number of requests. The value ranges from 1 to 2,147,483,647.
limit_period	Yes	Integer	Rate limit period, in seconds. The value ranges from 1 to 3,600.
unlock_num	No	Integer	Allowable frequency based on the number of requests. The value ranges from 0 to 2,147,483,647. This parameter is required only when the protection action type is dynamic_block .

Parameter	Mandatory	Type	Description
lock_time	No	Integer	Block duration, in seconds. The value ranges from 0 to 65,535. Access requests are blocked during the configured block duration, and an error page is displayed.
domain_aggregation	No	Boolean	Whether to enable domain name aggregation statistics
region_aggregation	No	Boolean	Whether to enable global counting.
description	No	String	Rule description.

Table 4-101 CcCondition

Parameter	Mandatory	Type	Description
category	Yes	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • ip • ipv6 • params • cookie • header • response_code

Parameter	Mandatory	Type	Description
logic_operation	Yes	String	<p>Logic for matching the condition.</p> <ul style="list-style-type: none"> • If the category is url, the optional operations are contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal and len_not_equal • If the category is ip, the optional operations are: equal, not_equal, , equal_any and not_equal_all • If the category is params, cookie and header, the optional operations are: contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist and not_exist
contents	No	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.

Parameter	Mandatory	Type	Description
value_list_id	No	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.
index	No	String	Subfield. When Field Type is set to params, cookie, or header, set this parameter based on the site requirements and this parameter is mandatory.

Table 4-102 action

Parameter	Mandatory	Type	Description
category	Yes	String	<p>Action type:</p> <ul style="list-style-type: none"> • captcha: Verification code. WAF requires visitors to enter a correct verification code to continue their access to requested page on your website. • block: WAF blocks the requests. When tag_type is set to other, the value can only be block. • log: WAF logs the event only. • dynamic_block: In the previous rate limit period, if the request frequency exceeds the value of Rate Limit Frequency, the request is blocked. In the next rate limit period, if the request frequency exceeds the value of Permit Frequency, the request is still blocked. Note: The dynamic_block protection action can be set only when the advanced protection mode is enabled for the CC protection rule. <p>Enumeration values:</p> <ul style="list-style-type: none"> • captcha • block • log • dynamic_block
detail	No	detail object	<p>Block page information. When protection action category is set to block or dynamic_block, you need to set the returned block page.</p> <ul style="list-style-type: none"> • If you want to use the default block page, this parameter can be excluded. • If you want to use a custom block page, set this parameter.

Table 4-103 detail

Parameter	Mandatory	Type	Description
response	No	response object	Block Page.

Table 4-104 response

Parameter	Mandatory	Type	Description
content_type	No	String	Content type. The value can only be application/json , text/html , or text/xml . Enumeration values: <ul style="list-style-type: none"> • application/json • text/html • text/xml
content	No	String	Block page information.

Table 4-105 tag_condition

Parameter	Mandatory	Type	Description
category	No	String	User identifier. The value is fixed at referer .
contents	No	Array of strings	Content of the user identifier field.

Response Parameters

Status code: 200

Table 4-106 Response body parameters

Parameter	Type	Description
name	String	Rule name.
id	String	Rule ID.
policyid	String	Policy ID.

Parameter	Type	Description
url	String	When the value of mode is 0, this parameter has a return value. URL to which the rule applies, excluding a domain name.
prefix	Boolean	Whether a prefix is used for the path. If the protected URL ends with an asterisk (*), a path prefix is used. If the value of mode is 0, this parameter has a return value.
mode	Integer	Mode. <ul style="list-style-type: none"> • 0: Standard. • 1: Advanced. Enumeration values: <ul style="list-style-type: none"> • 0 • 1
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The rule is disabled. • 1: The rule is enabled.
conditions	Array of CcCondition objects	Condition list. This parameter is returned when mode is set to 1 .
action	action object	Action to take if the number of requests reaches the upper limit.
tag_type	String	Limit mode. <ul style="list-style-type: none"> • ip: IP-based rate limiting. Website visitors are identified by IP address. • cookie: User-based rate limiting. Website visitors are identified by the cookie key value. • other: Website visitors are identified by the Referer field (user-defined request source). • policy: Policy-based rate limiting • domain: Domain name rate limit • url: URL rate limit Enumeration values: <ul style="list-style-type: none"> • ip • cookie • header • other • policy • domain • url

Parameter	Type	Description
tag_index	String	User identifier. This parameter is mandatory when the rate limit mode is set to user (cookie or header). <ul style="list-style-type: none"> • cookie: Set the cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the name field in the cookie to uniquely identify a website visitor, select name. • header: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.
tag_condition	tag_condition object	User tag. This parameter is mandatory when the rate limit mode is set to other . -other: A website visitor is identified by the Referer field (user-defined request source).
limit_num	Integer	Rate limit frequency based on the number of requests. The value ranges from 1 to 2,147,483,647.
limit_period	Integer	Rate limit period, in seconds. The value ranges from 1 to 3,600.
unlock_num	Integer	Allowable frequency based on the number of requests. The value ranges from 0 to 2,147,483,647. This parameter is required only when the protection action type is dynamic_block .
lock_time	Integer	Block duration, in seconds. The value ranges from 0 to 65,535. Access requests are blocked during the configured block duration, and an error page is displayed.
domain_aggregation	Boolean	Whether to enable domain name aggregation statistics
region_aggregation	Boolean	Whether to enable global counting.
description	String	Rule description.
total_num	Integer	This parameter is reserved and can be ignored currently.
unaggregation	Boolean	This parameter is reserved and can be ignored currently.

Parameter	Type	Description
aging_time	Integer	Rule aging time. This parameter is reserved and can be ignored currently.
producer	Integer	Rule creation object. This parameter is reserved and can be ignored currently.
timestamp	Long	Timestamp the rule is created.

Table 4-107 CcCondition

Parameter	Type	Description
category	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • ip • ipv6 • params • cookie • header • response_code
logic_operation	String	Logic for matching the condition. <ul style="list-style-type: none"> • If the category is url, the optional operations are contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal and len_not_equal • If the category is ip, the optional operations are: equal, not_equal, , equal_any and not_equal_all • If the category is params, cookie and header, the optional operations are: contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist and not_exist

Parameter	Type	Description
contents	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.
index	String	Subfield. When Field Type is set to params, cookie, or header, set this parameter based on the site requirements and this parameter is mandatory.

Table 4-108 action

Parameter	Type	Description
category	String	<p>Action type:</p> <ul style="list-style-type: none"> ● captcha: Verification code. WAF requires visitors to enter a correct verification code to continue their access to requested page on your website. ● block: WAF blocks the requests. When tag_type is set to other, the value can only be block. ● log: WAF logs the event only. ● dynamic_block: In the previous rate limit period, if the request frequency exceeds the value of Rate Limit Frequency, the request is blocked. In the next rate limit period, if the request frequency exceeds the value of Permit Frequency, the request is still blocked. Note: The dynamic_block protection action can be set only when the advanced protection mode is enabled for the CC protection rule. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● captcha ● block ● log ● dynamic_block

Parameter	Type	Description
detail	detail object	Block page information. When protection action category is set to block or dynamic_block , you need to set the returned block page. <ul style="list-style-type: none"> • If you want to use the default block page, this parameter can be excluded. • If you want to use a custom block page, set this parameter.

Table 4-109 detail

Parameter	Type	Description
response	response object	Block Page.

Table 4-110 response

Parameter	Type	Description
content_type	String	Content type. The value can only be application/json , text/html , or text/xml . Enumeration values: <ul style="list-style-type: none"> • application/json • text/html • text/xml
content	String	Block page information.

Table 4-111 tag_condition

Parameter	Type	Description
category	String	User identifier. The value is fixed at referer .
contents	Array of strings	Content of the user identifier field.

Status code: 400

Table 4-112 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-113 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-114 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a CC protection rule. The project ID is specified by `project_id` and protection policy ID is specified by `policy_id`. The rule name is `test55`, rate limit mode is IP-based rate limit, the rate limit frequency is 10, the rate limit duration is 60s, and the protective action is verification code. The protection mode of the CC rule is advanced. The field type of the rate limit condition is the URL that contains `/url`. There is no subfield. Requests are counted only for the current WAF instance.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/cc?
```

```
{
  "description" : "",
  "name" : "test55",
  "tag_type" : "ip",
  "limit_num" : 10,
  "limit_period" : 60,
  "action" : {
    "category" : "captcha"
  },
  "mode" : 1,
  "domain_aggregation" : false,
  "conditions" : [ {
    "category" : "url",
```

```
"logic_operation" : "contain",  
"contents" : [ "/url" ],  
"index" : null  
}],  
"region_aggregation" : false  
}
```

Example Responses

Status code: 200

Request succeeded.

```
{  
  "id" : "f88c5eabff9b4ff9ba6e7dd8e38128ba",  
  "policyid" : "d471eef691684f1c8d7784532fd8f4bd",  
  "name" : "test55",  
  "timestamp" : 1678873040603,  
  "description" : "",  
  "status" : 1,  
  "mode" : 1,  
  "conditions" : [ {  
    "category" : "url",  
    "contents" : [ "/url" ],  
    "logic_operation" : "contain"  
  } ],  
  "action" : {  
    "category" : "captcha"  
  },  
  "producer" : 1,  
  "unaggregation" : false,  
  "total_num" : 0,  
  "limit_num" : 10,  
  "limit_period" : 60,  
  "lock_time" : 0,  
  "tag_type" : "ip",  
  "aging_time" : 0,  
  "region_aggregation" : false,  
  "domain_aggregation" : false  
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.4 Querying a CC Attack Protection Rule by ID

Function

This API is used to query a CC attack protection rule by ID.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}

Table 4-115 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.
rule_id	Yes	String	"ID of the cc rule. It can be obtained by calling the ListCcRules API."

Table 4-116 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-117 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-118 Response body parameters

Parameter	Type	Description
name	String	Rule name.
id	String	Rule ID.
policyid	String	Policy ID.
url	String	When the value of mode is 0, this parameter has a return value. URL to which the rule applies, excluding a domain name.
prefix	Boolean	Whether a prefix is used for the path. If the protected URL ends with an asterisk (*), a path prefix is used. When the value of mode is 0, this parameter has a return value.
mode	Integer	Mode. <ul style="list-style-type: none"> ● 0: Standard. ● 1: Advanced. Enumeration values: <ul style="list-style-type: none"> ● 0 ● 1
status	Integer	Rule status. The value can be 0 or 1. <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.

Parameter	Type	Description
conditions	Array of CcCondition objects	Condition list. This parameter is returned when mode is set to 1 .
action	action object	Action to take if the number of requests reaches the upper limit.
tag_type	String	Limit mode. <ul style="list-style-type: none"> • ip: IP-based rate limiting. Website visitors are identified by IP address. • cookie: User-based rate limiting. Website visitors are identified by the cookie key value. • other: Website visitors are identified by the Referer field (user-defined request source). Enumeration values: <ul style="list-style-type: none"> • ip • cookie • header • other • policy • domain • url
tag_index	String	User identifier. This parameter is mandatory when the rate limit mode is set to user (cookie or header). <ul style="list-style-type: none"> • cookie: Set the cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the name field in the cookie to uniquely identify a website visitor, select name. • header: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.
tag_condition	tag_condition object	User tag. This parameter is mandatory when the rate limit mode is set to other . -other: A website visitor is identified by the Referer field (user-defined request source).

Parameter	Type	Description
limit_num	Integer	Rate limit frequency based on the number of requests. The value ranges from 1 to 2,147,483,647.
limit_period	Integer	Rate limit period, in seconds. The value ranges from 1 to 3,600.
unlock_num	Integer	Allowable frequency based on the number of requests. The value ranges from 0 to 2,147,483,647. This parameter is required only when the protection action type is dynamic_block .
lock_time	Integer	Block duration, in seconds. The value ranges from 0 to 65,535. Access requests are blocked during the configured block duration, and an error page is displayed.
domain_aggregation	Boolean	Whether to enable domain name aggregation statistics
region_aggregation	Boolean	Whether to enable global counting.
description	String	Rule description.
total_num	Integer	This parameter is reserved and can be ignored currently.
unaggregation	Boolean	This parameter is reserved and can be ignored currently.
aging_time	Integer	Rule aging time. This parameter is reserved and can be ignored currently.
producer	Integer	Rule creation object. This parameter is reserved and can be ignored currently.
timestamp	Long	Timestamp the rule is created.

Table 4-119 CcCondition

Parameter	Type	Description
category	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • ip • ipv6 • params • cookie • header • response_code
logic_operation	String	Logic for matching the condition. <ul style="list-style-type: none"> • If the category is url, the optional operations are contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal and len_not_equal • If the category is ip, the optional operations are: equal, not_equal, , equal_any and not_equal_all • If the category is params, cookie and header, the optional operations are: contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist and not_exist
contents	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.

Parameter	Type	Description
index	String	Subfield. When Field Type is set to params, cookie, or header, set this parameter based on the site requirements and this parameter is mandatory.

Table 4-120 action

Parameter	Type	Description
category	String	<p>Action type:</p> <ul style="list-style-type: none"> • block: WAF blocks discovered attacks. • captcha: Verification code. WAF requires visitors to enter a correct verification code to continue their access to requested page on your website. • If tag_type is set to other, the value can only be block. <p>Enumeration values:</p> <ul style="list-style-type: none"> • captcha • block • log • dynamic_block
detail	detail object	<p>Action details. If detail is null, the default block page is displayed by default.</p> <ul style="list-style-type: none"> • This parameter cannot be included when category is set to captcha. • This parameter is required when category is set to block.

Table 4-121 detail

Parameter	Type	Description
response	response object	Returned page

Table 4-122 response

Parameter	Type	Description
content_type	String	Content type. The value can only be application/json, text/html, or text/xml. Enumeration values: <ul style="list-style-type: none"> • application/json • text/html • text/xml
content	String	Content

Table 4-123 tag_condition

Parameter	Type	Description
category	String	User identifier. The value is fixed at referer .
contents	Array of strings	Content of the user identifier field.

Status code: 400

Table 4-124 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-125 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-126 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a CC attack protection rule. Details about the query are specified by project_id, policy_id, and rule_id.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}?
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "f88c5eabff9b4ff9ba6e7dd8e38128ba",
  "policyid" : "d471eef691684f1c8d7784532fd8f4bd",
  "name" : "test55",
  "timestamp" : 1678873040603,
  "description" : "",
  "status" : 1,
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "/url" ],
    "logic_operation" : "contain"
  } ],
  "action" : {
    "category" : "captcha"
  },
  "producer" : 1,
  "unaggregation" : false,
  "total_num" : 0,
  "limit_num" : 10,
  "limit_period" : 60,
  "lock_time" : 0,
  "tag_type" : "ip",
  "aging_time" : 0,
  "region_aggregation" : false,
  "domain_aggregation" : false
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.

Status Code	Description
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.5 Updating a CC Attack Protection Rule

Function

This API is used to update a CC attack protection rule.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}

Table 4-127 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.
rule_id	Yes	String	"ID of the cc rule. It can be obtained by calling the ListCcRules API."

Table 4-128 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-129 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-130 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Rule name.
mode	Yes	Integer	Mode. <ul style="list-style-type: none"> • 0: Standard. • 1: Advanced. Enumeration values: <ul style="list-style-type: none"> • 0 • 1
url	No	String	Path to be protected in the CC attack protection rule. This parameter is mandatory when the CC attack protection rule is in standard mode (i.e. the value of mode is 0).
conditions	Yes	Array of CcCondition objects	Condition list. This parameter is returned when mode is set to 1.

Parameter	Mandatory	Type	Description
action	Yes	action object	Action to take if the number of requests reaches the upper limit.
tag_type	Yes	String	<p>Protection mode.</p> <ul style="list-style-type: none"> ● ip: IP-based rate limiting. Website visitors are identified by IP address. ● cookie: User-based rate limiting. Website visitors are identified by the cookie key value. ● other: Website visitors are identified by the Referer field (user-defined request source). <p>Enumeration values:</p> <ul style="list-style-type: none"> ● ip ● cookie ● header ● other ● policy ● domain ● url

Parameter	Mandatory	Type	Description
tag_index	No	String	<p>User identifier. This parameter is mandatory when the rate limit mode is set to user (cookie or header).</p> <ul style="list-style-type: none"> • cookie: Set the cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the name field in the cookie to uniquely identify a website visitor, select name. • header: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.
tag_condition	No	tag_condition object	User tag. This parameter is mandatory when the rate limit mode is set to other . -other: A website visitor is identified by the Referer field (user-defined request source).
limit_num	Yes	Integer	Rate limit frequency based on the number of requests. The value ranges from 1 to 2,147,483,647.
limit_period	Yes	Integer	Rate limit period, in seconds. The value ranges from 1 to 3,600.
unlock_num	No	Integer	Allowable frequency based on the number of requests. The value ranges from 0 to 2,147,483,647. This parameter is required only when the protection action type is dynamic_block .

Parameter	Mandatory	Type	Description
lock_time	No	Integer	Block duration, in seconds. The value ranges from 0 to 65,535. Access requests are blocked during the configured block duration, and an error page is displayed.
domain_aggregation	No	Boolean	Whether to enable domain name aggregation statistics
region_aggregation	No	Boolean	Whether to enable global counting.
description	No	String	Rule description.

Table 4-131 CcCondition

Parameter	Mandatory	Type	Description
category	Yes	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • ip • ipv6 • params • cookie • header • response_code

Parameter	Mandatory	Type	Description
logic_operation	Yes	String	<p>Logic for matching the condition.</p> <ul style="list-style-type: none"> • If the category is url, the optional operations are contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal and len_not_equal • If the category is ip, the optional operations are: equal, not_equal, , equal_any and not_equal_all • If the category is params, cookie and header, the optional operations are: contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist and not_exist
contents	No	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.

Parameter	Mandatory	Type	Description
value_list_id	No	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.
index	No	String	Subfield. When Field Type is set to params, cookie, or header, set this parameter based on the site requirements and this parameter is mandatory.

Table 4-132 action

Parameter	Mandatory	Type	Description
category	Yes	String	<p>Action type:</p> <ul style="list-style-type: none"> • captcha: Verification code. WAF requires visitors to enter a correct verification code to continue their access to requested page on your website. • block: WAF blocks the requests. When tag_type is set to other, the value can only be block. • log: WAF logs the event only. • dynamic_block: In the previous rate limit period, if the request frequency exceeds the value of Rate Limit Frequency, the request is blocked. In the next rate limit period, if the request frequency exceeds the value of Permit Frequency, the request is still blocked. Note: The dynamic_block protection action can be set only when the advanced protection mode is enabled for the CC protection rule. <p>Enumeration values:</p> <ul style="list-style-type: none"> • captcha • block • log • dynamic_block
detail	No	detail object	<p>Block page information. When protection action category is set to block or dynamic_block, you need to set the returned block page.</p> <ul style="list-style-type: none"> • If you want to use the default block page, this parameter can be excluded. • If you want to use a custom block page, set this parameter.

Table 4-133 detail

Parameter	Mandatory	Type	Description
response	No	response object	Block Page.

Table 4-134 response

Parameter	Mandatory	Type	Description
content_type	No	String	Content type. The value can only be application/json , text/html , or text/xml . Enumeration values: <ul style="list-style-type: none"> • application/json • text/html • text/xml
content	No	String	Block page information.

Table 4-135 tag_condition

Parameter	Mandatory	Type	Description
category	No	String	User identifier. The value is fixed at referer .
contents	No	Array of strings	Content of the user identifier field.

Response Parameters

Status code: 200

Table 4-136 Response body parameters

Parameter	Type	Description
name	String	Rule name.
id	String	Rule ID.
policyid	String	Policy ID.

Parameter	Type	Description
url	String	<p>When the value of mode is 0, this parameter has a return value. URL to which the rule applies, excluding a domain name.</p> <ul style="list-style-type: none"> • Prefix match: A path ending with * indicates that the path is used as a prefix. For example, to protect /admin/test.php or /adminabc, you can set Path to /admin*. • Exact match: The path you enter must exactly match the path you want to protect. If the path you want to protect is /admin, set url to /admin.
prefix	Boolean	Whether a prefix is used for the path. If the protected URL ends with an asterisk (*), a path prefix is used.
mode	Integer	<p>Mode.</p> <ul style="list-style-type: none"> • 0: Standard. • 1: Advanced. <p>Enumeration values:</p> <ul style="list-style-type: none"> • 0 • 1
conditions	Array of CcCondition objects	Condition list. This parameter is returned when mode is set to 1.
action	action object	Action to take if the number of requests reaches the upper limit.
tag_type	String	<p>Protection mode.</p> <ul style="list-style-type: none"> • ip: IP-based rate limiting. Website visitors are identified by IP address. • cookie: User-based rate limiting. Website visitors are identified by the cookie key value. • other: Website visitors are identified by the Referer field (user-defined request source). <p>Enumeration values:</p> <ul style="list-style-type: none"> • ip • cookie • header • other • policy • domain • url

Parameter	Type	Description
tag_index	String	User identifier. This parameter is mandatory when the rate limit mode is set to user (cookie or header). <ul style="list-style-type: none"> • cookie: Set the cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the name field in the cookie to uniquely identify a website visitor, select name. • header: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.
tag_condition	tag_condition object	User tag. This parameter is mandatory when the rate limit mode is set to other . -other: A website visitor is identified by the Referer field (user-defined request source).
limit_num	Integer	Rate limit frequency based on the number of requests. The value ranges from 1 to 2,147,483,647.
limit_period	Integer	Rate limit period, in seconds. The value ranges from 1 to 3,600.
unlock_num	Integer	Allowable frequency based on the number of requests. The value ranges from 0 to 2,147,483,647. This parameter is required only when the protection action type is dynamic_block .
lock_time	Integer	Block duration, in seconds. The value ranges from 0 to 65,535. Access requests are blocked during the configured block duration, and an error page is displayed.
domain_aggregation	Boolean	Whether to enable domain name aggregation statistics
region_aggregation	Boolean	Whether to enable global counting.
description	String	Rule description.
total_num	Integer	This parameter is reserved and can be ignored currently.
unaggregation	Boolean	This parameter is reserved and can be ignored currently.

Parameter	Type	Description
aging_time	Integer	Rule aging time. This parameter is reserved and can be ignored currently.
producer	Integer	Rule creation object. This parameter is reserved and can be ignored currently.

Table 4-137 CcCondition

Parameter	Type	Description
category	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • ip • ipv6 • params • cookie • header • response_code
logic_operation	String	Logic for matching the condition. <ul style="list-style-type: none"> • If the category is url, the optional operations are contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal and len_not_equal • If the category is ip, the optional operations are: equal, not_equal, , equal_any and not_equal_all • If the category is params, cookie and header, the optional operations are: contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist and not_exist

Parameter	Type	Description
contents	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.
index	String	Subfield. When Field Type is set to params, cookie, or header, set this parameter based on the site requirements and this parameter is mandatory.

Table 4-138 action

Parameter	Type	Description
category	String	<p>Action type:</p> <ul style="list-style-type: none"> ● captcha: Verification code. WAF requires visitors to enter a correct verification code to continue their access to requested page on your website. ● block: WAF blocks the requests. When tag_type is set to other, the value can only be block. ● log: WAF logs the event only. ● dynamic_block: In the previous rate limit period, if the request frequency exceeds the value of Rate Limit Frequency, the request is blocked. In the next rate limit period, if the request frequency exceeds the value of Permit Frequency, the request is still blocked. Note: The dynamic_block protection action can be set only when the advanced protection mode is enabled for the CC protection rule. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● captcha ● block ● log ● dynamic_block

Parameter	Type	Description
detail	detail object	Block page information. When protection action category is set to block or dynamic_block , you need to set the returned block page. <ul style="list-style-type: none"> • If you want to use the default block page, this parameter can be excluded. • If you want to use a custom block page, set this parameter.

Table 4-139 detail

Parameter	Type	Description
response	response object	Returned page

Table 4-140 response

Parameter	Type	Description
content_type	String	Content type. The value can only be application/json, text/html, or text/xml. Enumeration values: <ul style="list-style-type: none"> • application/json • text/html • text/xml
content	String	Content

Table 4-141 tag_condition

Parameter	Type	Description
category	String	User identifier. The value is fixed at referer .
contents	Array of strings	Content of the user identifier field.

Status code: 400

Table 4-142 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-143 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-144 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to change the rate limit settings of a CC protection rule. The project ID is specified by `project_id` and protection policy ID is specified by `policy_id`. The rule name is `test55`, the rate limit mode is IP-based rate limit, rate limit frequency is 10, the rate limit duration is 60s, and the protective action is verification code. The protection mode of the CC rule is advanced. The field type of the rate limit condition is the URL that contains `/url`. There is no subfield. Requests are counted only for the current WAF instance.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}?
```

```
{
  "description" : "",
  "tag_type" : "ip",
  "limit_num" : 10,
  "limit_period" : 60,
  "action" : {
    "category" : "captcha"
  },
  "mode" : 1,
  "name" : "test55",
  "domain_aggregation" : false,
  "conditions" : [ {
    "category" : "url",
```

```
"logic_operation" : "contain",  
"contents" : [ "/url" ],  
"index" : null  
}],  
"region_aggregation" : false  
}
```

Example Responses

Status code: 200

Request succeeded.

```
{  
  "id" : "f88c5eabff9b4ff9ba6e7dd8e38128ba",  
  "policyid" : "d471eef691684f1c8d7784532fd8f4bd",  
  "name" : "test55",  
  "description" : "",  
  "mode" : 1,  
  "conditions" : [ {  
    "category" : "url",  
    "contents" : [ "/url" ],  
    "logic_operation" : "contain"  
  } ],  
  "action" : {  
    "category" : "captcha"  
  },  
  "producer" : 1,  
  "unaggregation" : false,  
  "total_num" : 0,  
  "limit_num" : 10,  
  "limit_period" : 60,  
  "lock_time" : 0,  
  "tag_type" : "ip",  
  "aging_time" : 0,  
  "region_aggregation" : false,  
  "domain_aggregation" : false  
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.6 Deleting a CC Attack Protection Rule

Function

This API is used to delete a CC attack protection rule.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}

Table 4-145 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.
rule_id	Yes	String	"ID of the cc rule. It can be obtained by calling the ListCcRules API."

Table 4-146 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-147 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-148 Response body parameters

Parameter	Type	Description
name	String	Rule name.
id	String	Rule ID.
policyid	String	Policy ID.
url	String	When the value of mode is 0, this parameter has a return value. URL to which the rule applies, excluding a domain name.
prefix	Boolean	Whether a prefix is used for the path. If the protected URL ends with an asterisk (*), a path prefix is used.
mode	Integer	Mode. <ul style="list-style-type: none"> ● 0: Standard. ● 1: Advanced. Enumeration values: <ul style="list-style-type: none"> ● 0 ● 1
status	Integer	Rule status. The value can be 0 or 1. <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
conditions	Array of CcCondition objects	Condition list. This parameter is returned when mode is set to 1.

Parameter	Type	Description
action	action object	Action to take if the number of requests reaches the upper limit.
tag_type	String	Protection mode. <ul style="list-style-type: none"> ● ip: IP-based rate limiting. Website visitors are identified by IP address. ● cookie: User-based rate limiting. Website visitors are identified by the cookie key value. ● other: Website visitors are identified by the Referer field (user-defined request source). Enumeration values: <ul style="list-style-type: none"> ● ip ● cookie ● header ● other ● policy ● domain ● url
tag_index	String	User identifier. This parameter is mandatory when the rate limit mode is set to user (cookie or header). <ul style="list-style-type: none"> ● cookie: Set the cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the name field in the cookie to uniquely identify a website visitor, select name. ● header: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.
tag_condition	tag_condition object	User tag. This parameter is mandatory when the rate limit mode is set to other . -other: A website visitor is identified by the Referer field (user-defined request source).
limit_num	Integer	Rate limit frequency based on the number of requests. The value ranges from 1 to 2,147,483,647.
limit_period	Integer	Rate limit period, in seconds. The value ranges from 1 to 3,600.

Parameter	Type	Description
unlock_num	Integer	Allowable frequency based on the number of requests. The value ranges from 0 to 2,147,483,647. This parameter is required only when the protection action type is dynamic_block .
lock_time	Integer	Block duration, in seconds. The value ranges from 0 to 65,535. Access requests are blocked during the configured block duration, and an error page is displayed.
domain_aggregation	Boolean	Whether to enable domain name aggregation statistics
region_aggregation	Boolean	Whether to enable global counting.
description	String	Rule description.
total_num	Integer	This parameter is reserved and can be ignored.
unaggregation	Boolean	This parameter is reserved and can be ignored.
aging_time	Integer	This parameter is reserved and can be ignored.
producer	Integer	This parameter is reserved and can be ignored.
timestamp	Long	Timestamp the rule is created.

Table 4-149 CcCondition

Parameter	Type	Description
category	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • ip • ipv6 • params • cookie • header • response_code

Parameter	Type	Description
logic_operation	String	<p>Logic for matching the condition.</p> <ul style="list-style-type: none"> If the category is url, the optional operations are contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal and len_not_equal If the category is ip, the optional operations are: equal, not_equal, , equal_any and not_equal_all If the category is params, cookie and header, the optional operations are: contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, not_suffix, contain_any, not_contain_all, equal_any, not_equal_all, equal_any, not_equal_all, prefix_any, not_prefix_all, suffix_any, not_suffix_all, len_greater, len_less, len_equal, len_not_equal, num_greater, num_less, num_equal, num_not_equal, exist and not_exist
contents	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.
index	String	Subfield. When Field Type is set to params, cookie, or header, set this parameter based on the site requirements and this parameter is mandatory.

Table 4-150 action

Parameter	Type	Description
category	String	<p>Action type:</p> <ul style="list-style-type: none"> • captcha: Verification code. WAF requires visitors to enter a correct verification code to continue their access to requested page on your website. • block: WAF blocks the requests. When tag_type is set to other, the value can only be block. • log: WAF logs the event only. • dynamic_block: In the previous rate limit period, if the request frequency exceeds the value of Rate Limit Frequency, the request is blocked. In the next rate limit period, if the request frequency exceeds the value of Permit Frequency, the request is still blocked. Note: The dynamic_block protection action can be set only when the advanced protection mode is enabled for the CC protection rule. <p>Enumeration values:</p> <ul style="list-style-type: none"> • captcha • block • log • dynamic_block
detail	detail object	<p>Block page information. When protection action category is set to block or dynamic_block, you need to set the returned block page.</p> <ul style="list-style-type: none"> • If you want to use the default block page, this parameter can be excluded. • If you want to use a custom block page, set this parameter.

Table 4-151 detail

Parameter	Type	Description
response	response object	Returned page

Table 4-152 response

Parameter	Type	Description
content_type	String	Content type. The value can only be application/json, text/html, or text/xml. Enumeration values: <ul style="list-style-type: none"> • application/json • text/html • text/xml
content	String	Content

Table 4-153 tag_condition

Parameter	Type	Description
category	String	User identifier. The value is fixed at referer .
contents	Array of strings	Content of the user identifier field.

Status code: 400

Table 4-154 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-155 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-156 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a CC attack protection rule. Details about the deletion are specified by `project_id`, `policy_id`, and `rule_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}?
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "f88c5eabff9b4ff9ba6e7dd8e38128ba",
  "policyid" : "d471eef691684f1c8d7784532fd8f4bd",
  "name" : "test55",
  "timestamp" : 1678873040603,
  "description" : "",
  "status" : 1,
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "/url" ],
    "logic_operation" : "contain"
  } ],
  "action" : {
    "category" : "captcha"
  },
  "producer" : 1,
  "unaggregation" : false,
  "total_num" : 0,
  "limit_num" : 10,
  "limit_period" : 60,
  "lock_time" : 0,
  "tag_type" : "ip",
  "aging_time" : 0,
  "region_aggregation" : false,
  "domain_aggregation" : false
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.

Status Code	Description
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.7 Querying the List of Precise Protection Rules

Function

This API is used to query the list of precise protection rules.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/custom

Table 4-157 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.

Table 4-158 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
offset	Yes	Integer	Offset. The records after the offset are queried.

Parameter	Mandatory	Type	Description
limit	Yes	Integer	Maximum number of records that can be returned.

Request Parameters

Table 4-159 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-160 Response body parameters

Parameter	Type	Description
total	Integer	Number of rules in the policy
items	Array of CustomRule objects	Array of rules

Table 4-161 CustomRule

Parameter	Type	Description
id	String	Policy ID.
policyid	String	Rule ID.
description	String	Rule description.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> 0: The rule is disabled. 1: The rule is enabled.

Parameter	Type	Description
conditions	Array of conditions objects	List of matching conditions. All conditions must be met.
action	CustomAction object	Protective action of the precise protection rule.
action_mode	Boolean	This parameter is reserved and can be ignored.
priority	Integer	Priority of a rule. A small value indicates a high priority. If two rules are assigned with the same priority, the rule added earlier has higher priority. Value range: 0 to 1000.
timestamp	Long	Timestamp when the precise protection rule is created.
time	Boolean	Time the precise protection rule takes effect. <ul style="list-style-type: none"> • false: The rule takes effect immediately. • true: The effective time is customized.
start	Long	Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is set to true.
terminal	Long	Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is set to true .
producer	Integer	This parameter is reserved and can be ignored.
name	String	Rule name.

Table 4-162 conditions

Parameter	Type	Description
category	String	Field type. The options are url , user-agent , ip , params , cookie , referer , header , request_line , method , and request .
index	String	Subfield <ul style="list-style-type: none"> • If the field type is url, user-agent, ip, refer, request_line, method, or request, index is not required. • If the field type is params, header, or cookie, and the subfield is customized, the value of index is the customized subfield.

Parameter	Type	Description
logic_operation	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	Array of strings	Content of the conditions.
value_list_id	String	Reference table ID.

Table 4-163 CustomAction

Parameter	Type	Description
category	String	Protection type <ul style="list-style-type: none"> • block: WAF blocks attacks. • pass: WAF allows requests. • log: WAF only logs discovered attacks. Enumeration values: <ul style="list-style-type: none"> • block • pass • log
followed_action_id	String	ID of a known attack source rule. This parameter can be configured only when category is set to block .

Status code: 400

Table 4-164 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-165 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Status code: 500

Table 4-166 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the precise protection rule list. Details about the query are specified by project_id and policy_id.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/custom?offset=0&limit=1
```

Example Responses

Status code: 200

ok

```
{
  "total": 1,
  "items": [ {
    "id": "c637138b6fe048e4a797d1c3712e85b3",
    "policyid": "41424a44c2904e1b9e505ccdbfe8c1fb",
    "timestamp": 1679888279852,
    "description": "",
    "status": 1,
    "time": false,
    "priority": 50,
    "action_mode": false,
    "conditions": [ {
      "category": "url",
      "contents": [ "test" ],
      "logic_operation": "contain"
    } ],
    "action": {
      "category": "block"
    },
    "producer": 1
  } ]
}
```


Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.8 Creating a precise protection rule

Function

This API is used to create a precise protection rule.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/custom

Table 4-167 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.

Table 4-168 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-169 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-170 Request body parameters

Parameter	Mandatory	Type	Description
time	Yes	Boolean	Time the precise protection rule takes effect. <ul style="list-style-type: none"> false: The rule takes effect immediately. true: The effective time is customized.
start	No	Long	Timestamp (ms) when the precise protection rule takes effect. This parameter is mandatory only when time is set to true .
terminal	No	Long	Timestamp (ms) when the precise protection rule expires. This parameter is mandatory only when time is set to true .
description	No	String	Rule description.
conditions	Yes	Array of CustomConditions objects	Match condition List

Parameter	Mandatory	Type	Description
action	Yes	CustomAction object	Protective action of the precise protection rule.
priority	Yes	Integer	Priority of a rule. A small value indicates a high priority. If two rules are assigned with the same priority, the rule added earlier has higher priority. Value range: 0 to 1000.
name	Yes	String	Rule name.

Table 4-171 CustomConditions

Parameter	Mandatory	Type	Description
category	No	String	Field type. The options can be url , user-agent , ip , params , cookie , referer , header , request_line , method , or request . Enumeration values: <ul style="list-style-type: none"> • url • user-agent • referer • ip • method • request_line • request • params • cookie • header
index	No	String	Subfield type. <ul style="list-style-type: none"> • If the field type is set to url, user-agent, ip, referer, request_line, method, or request, index can be null. • If the field type is set to params, header, or cookie and subfields are customized, index is set to the target custom subfield.

Parameter	Mandatory	Type	Description
logic_operation	No	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	No	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	No	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.

Table 4-172 CustomAction

Parameter	Mandatory	Type	Description
category	Yes	String	Protection type <ul style="list-style-type: none"> • block: WAF blocks attacks. • pass: WAF allows requests. • log: WAF only logs discovered attacks. Enumeration values: <ul style="list-style-type: none"> • block • pass • log
followed_action_id	No	String	ID of a known attack source rule. This parameter can be configured only when category is set to block .

Response Parameters

Status code: 200

Table 4-173 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.
policyid	String	Policy ID.
description	String	Rule description.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
conditions	Array of conditions objects	List of matching conditions. All conditions must be met.
action	CustomAction object	Protective action of the precise protection rule.
action_mode	Boolean	This parameter is reserved and can be ignored.
priority	Integer	Priority of a rule. A small value indicates a high priority. If two rules are assigned with the same priority, the rule added earlier has higher priority. Value range: 0 to 1000.
timestamp	Long	Timestamp when the precise protection rule is created.
time	Boolean	Time the precise protection rule takes effect. <ul style="list-style-type: none"> ● false: The rule takes effect immediately. ● true: The effective time is customized.
start	Long	Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is set to true .
terminal	Long	Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is set to true .
producer	Integer	This parameter is reserved and can be ignored.

Table 4-174 conditions

Parameter	Type	Description
category	String	Field type. The options are url , user-agent , ip , params , cookie , referer , header , request_line , method , and request .

Parameter	Type	Description
index	String	Subfield <ul style="list-style-type: none"> When the field type is url, user-agent, ip, refer, request_line, method, or request, index is not required. If the field type is params, header, or cookie, and the subfield is customized, the value of index is the customized subfield.
logic_operation	String	Logic for matching the condition.
contents	Array of strings	Content of the conditions.
value_list_id	String	Reference table ID.

Table 4-175 CustomAction

Parameter	Type	Description
category	String	Protection type <ul style="list-style-type: none"> block: WAF blocks attacks. pass: WAF allows requests. log: WAF only logs discovered attacks. Enumeration values: <ul style="list-style-type: none"> block pass log
followed_action_id	String	ID of a known attack source rule. This parameter can be configured only when category is set to block .

Status code: 400

Table 4-176 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-177 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-178 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a precise protection rule. Details about the query are specified by `project_id` and `policy_id`. The rule name is `test55`. The protective action is `Block`. The priority for executing the rule is `50`. The matching condition is that the `demo` field in the header contains `demo`. The rule takes effect immediately.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/custom?enterprise_project_id=0
```

```
{
  "name" : "test55",
  "description" : "",
  "action" : {
    "category" : "block"
  },
  "priority" : 50,
  "conditions" : [ {
    "category" : "header",
    "logic_operation" : "contain",
    "index" : "demo",
    "contents" : [ "demo" ]
  } ],
  "time" : false
}
```

Example Responses

Status code: 200

ok

```
{
  "action" : {
    "category" : "block"
  },
  "action_mode" : false,
  "conditions" : [ {
    "category" : "header",
    "index" : "demo",
```

```

    "logic_operation" : "contain",
    "contents" : [ "demo" ]
  } ],
  "description" : "",
  "name" : "test55",
  "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "priority" : 50,
  "status" : 1,
  "time" : false,
  "timestamp" : 1656495488880
}

```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.9 Querying a Precise Protection Rule by ID

Function

Querying a Precise Protection Rule by ID

URI

GET /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}

Table 4-179 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Parameter	Mandatory	Type	Description
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.
rule_id	Yes	String	ID of a precise protection rule. You can obtain it by calling the ListCustomRules API.

Table 4-180 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-181 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-182 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.

Parameter	Type	Description
policyid	String	Policy ID.
description	String	Rule description.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
conditions	Array of conditions objects	List of matching conditions. All conditions must be met.
action	CustomAction object	Protective action of the precise protection rule.
action_mode	Boolean	This parameter is reserved and can be ignored.
priority	Integer	Priority of a rule. A small value indicates a high priority. If two rules are assigned with the same priority, the rule added earlier has higher priority. Value range: 0 to 1000.
timestamp	Long	Timestamp when the precise protection rule is created.
time	Boolean	Time the precise protection rule takes effect. <ul style="list-style-type: none"> ● false: The rule takes effect immediately. ● true: The effective time is customized.
start	Long	Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is set to true .
terminal	Long	Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is set to true .
producer	Integer	This parameter is reserved and can be ignored currently.

Table 4-183 conditions

Parameter	Type	Description
category	String	Field type. The options are url , user-agent , ip , params , cookie , referer , header , request_line , method , and request .

Parameter	Type	Description
index	String	Subfield <ul style="list-style-type: none"> When the field type is url, user-agent, ip, refer, request_line, method, or request, index is not required. If the field type is params, header, or cookie, and the subfield is customized, the value of index is the customized subfield.
logic_operation	String	Logic for matching the condition.
contents	Array of strings	Content of the conditions.
value_list_id	String	Reference table ID.

Table 4-184 CustomAction

Parameter	Type	Description
category	String	Protection type <ul style="list-style-type: none"> block: WAF blocks attacks. pass: WAF allows requests. log: WAF only logs discovered attacks. Enumeration values: <ul style="list-style-type: none"> block pass log
followed_action_id	String	ID of a known attack source rule. This parameter can be configured only when category is set to block .

Status code: 400

Table 4-185 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-186 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-187 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a precise protection rule. Details about the query are specified by `project_id`, `policy_id`, and `rule_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}?
```

Example Responses

Status code: 200

ok

```
{
  "action" : {
    "category" : "block"
  },
  "action_mode" : false,
  "conditions" : [ {
    "category" : "header",
    "index" : "demo",
    "logic_operation" : "contain",
    "contents" : [ "demo" ]
  } ],
  "description" : "",
  "name" : "test55",
  "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "priority" : 50,
  "status" : 1,
  "time" : false,
  "timestamp" : 1656495488880
}
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.10 Updating a precise protection rule

Function

This API is used to update a precise protection rule.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}

Table 4-188 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.
rule_id	Yes	String	ID of a precise protection rule. You can obtain it by calling the ListCustomRules API.

Table 4-189 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-190 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-191 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rule name.
time	Yes	Boolean	Time the precise protection rule takes effect. <ul style="list-style-type: none">● false: The rule takes effect immediately.● true: The effective time is customized.
start	No	Long	Timestamp (ms) when the precise protection rule takes effect. This parameter is mandatory only when time is set to true .
terminal	No	Long	Timestamp (ms) when the precise protection rule expires. This parameter is mandatory only when time is set to true .
description	No	String	Rule description.

Parameter	Mandatory	Type	Description
conditions	Yes	Array of CustomConditions objects	Match condition List
action	Yes	CustomAction object	Protective action of the precise protection rule.
priority	Yes	Integer	Priority of a rule. A small value indicates a high priority. If two rules are assigned with the same priority, the rule added earlier has higher priority. Value range: 0 to 1000.

Table 4-192 CustomConditions

Parameter	Mandatory	Type	Description
category	No	String	Field type. The options can be url , user-agent , ip , params , cookie , referer , header , request_line , method , or request . Enumeration values: <ul style="list-style-type: none"> • url • user-agent • referer • ip • method • request_line • request • params • cookie • header
index	No	String	Subfield type. <ul style="list-style-type: none"> • If the field type is set to url, user-agent, ip, referer, request_line, method, or request, index can be null. • If the field type is set to params, header, or cookie and subfields are customized, index is set to the target custom subfield.

Parameter	Mandatory	Type	Description
logic_operation	No	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	No	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	No	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.

Table 4-193 CustomAction

Parameter	Mandatory	Type	Description
category	Yes	String	Protection type <ul style="list-style-type: none"> • block: WAF blocks attacks. • pass: WAF allows requests. • log: WAF only logs discovered attacks. Enumeration values: <ul style="list-style-type: none"> • block • pass • log
followed_action_id	No	String	ID of a known attack source rule. This parameter can be configured only when category is set to block .

Response Parameters

Status code: 200

Table 4-194 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.
policyid	String	Policy ID.
description	String	Rule description.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
conditions	Array of conditions objects	List of matching conditions. All conditions must be met.
action	CustomAction object	Protective action of the precise protection rule.
action_mode	Boolean	This parameter is reserved and can be ignored.
priority	Integer	Priority of a rule. A small value indicates a high priority. If two rules are assigned with the same priority, the rule added earlier has higher priority. Value range: 0 to 1000.
time	Boolean	Time the precise protection rule takes effect. <ul style="list-style-type: none"> ● false: The rule takes effect immediately. ● true: The effective time is customized.
start	Long	Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is set to true .
terminal	Long	Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is set to true .
producer	Integer	This parameter is reserved and can be ignored currently.

Table 4-195 conditions

Parameter	Type	Description
category	String	Field type. The options are url , user-agent , ip , params , cookie , referer , header , request_line , method , and request .

Parameter	Type	Description
index	String	Subfield <ul style="list-style-type: none"> When the field type is url, user-agent, ip, refer, request_line, method, or request, index is not required. If the field type is params, header, or cookie, and the subfield is customized, the value of index is the customized subfield.
logic_operation	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	Array of strings	Content of the conditions.
value_list_id	String	Reference table ID.

Table 4-196 CustomAction

Parameter	Type	Description
category	String	Protection type <ul style="list-style-type: none"> block: WAF blocks attacks. pass: WAF allows requests. log: WAF only logs discovered attacks. Enumeration values: <ul style="list-style-type: none"> block pass log
followed_action_id	String	ID of a known attack source rule. This parameter can be configured only when category is set to block .

Status code: 400

Table 4-197 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-198 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-199 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to edit a precise protection rule. Details about the change are specified by `project_id`, `policy_id`, and `rule_id`. The rule name is `test55`. The protective action is `Block`. The priority for executing the rule is `50`. The matching condition is that the `demo2` field in the header contains `demo`. The rule takes effect immediately.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}?
```

```
{
  "name" : "test55",
  "description" : "",
  "action" : {
    "category" : "block"
  },
  "priority" : 50,
  "conditions" : [ {
    "category" : "header",
    "logic_operation" : "contain",
    "index" : "demo2",
    "contents" : [ "demo" ]
  } ],
  "time" : false
}
```

Example Responses

Status code: 200

ok

```
{
  "action" : {
    "category" : "block"
  },
  "action_mode" : false,
```

```

"conditions" : [ {
  "category" : "header",
  "index" : "demo2",
  "logic_operation" : "contain",
  "contents" : [ "demo" ]
} ],
"description" : "",
"name" : "test55",
"id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
"policyid" : "1f016cde588646aca3fb19f277c44d03",
"priority" : 50,
"status" : 1,
"time" : false
}

```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.11 Deleting a precise protection rule

Function

This API is used to delete a precise protection rule.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}

Table 4-200 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Parameter	Mandatory	Type	Description
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.
rule_id	Yes	String	ID of a precise protection rule. You can obtain it by calling the ListCustomRules API.

Table 4-201 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-202 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-203 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Rule name.

Parameter	Type	Description
policyid	String	Policy ID.
description	String	Rule description.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
conditions	Array of conditions objects	List of matching conditions. All conditions must be met.
action	CustomAction object	Protective action of the precise protection rule.
action_mode	Boolean	This parameter is reserved and can be ignored.
priority	Integer	Priority of a rule. A small value indicates a high priority. If two rules are assigned with the same priority, the rule added earlier has higher priority. Value range: 0 to 1000.
timestamp	Long	Timestamp when the precise protection rule is created.
time	Boolean	Time the precise protection rule takes effect. <ul style="list-style-type: none"> ● false: The rule takes effect immediately. ● true: The effective time is customized.
start	Long	Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is set to true .
terminal	Long	Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is set to true .
producer	Integer	This parameter is reserved and can be ignored currently.

Table 4-204 conditions

Parameter	Type	Description
category	String	Field type. The options are url , user-agent , ip , params , cookie , referer , header , request_line , method , and request .

Parameter	Type	Description
index	String	Subfield <ul style="list-style-type: none"> When the field type is url, user-agent, ip, refer, request_line, method, or request, index is not required. If the field type is params, header, or cookie, and the subfield is customized, the value of index is the customized subfield.
logic_operation	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	Array of strings	Content of the conditions.
value_list_id	String	Reference table ID.

Table 4-205 CustomAction

Parameter	Type	Description
category	String	Protection type <ul style="list-style-type: none"> block: WAF blocks attacks. pass: WAF allows requests. log: WAF only logs discovered attacks. Enumeration values: <ul style="list-style-type: none"> block pass log
followed_action_id	String	ID of a known attack source rule. This parameter can be configured only when category is set to block .

Status code: 400

Table 4-206 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-207 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-208 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a precise protection rule. Details about the deletion are specified by `project_id`, `policy_id`, and `rule_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}?
```

Example Responses

Status code: 200

ok

```
{
  "action" : {
    "category" : "block"
  },
  "action_mode" : false,
  "conditions" : [ {
    "category" : "header",
    "index" : "demo",
    "logic_operation" : "contain",
    "contents" : [ "demo" ]
  } ],
  "description" : "",
  "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "priority" : 50,
  "status" : 1,
  "time" : false,
  "timestamp" : 1656495488880
}
```


Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.12 Creating a Global Protection Whitelist (Formerly False Alarm Masking) Rule

Function

This API is used to create a global protection whitelist (formerly false alarm masking) rule.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/ignore

Table 4-209 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-210 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-211 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-212 Request body parameters

Parameter	Mandatory	Type	Description
domain	Yes	Array of strings	Domain name or website to be protected. If the array length is 0 , the rule takes effect for all domain names or websites.
conditions	Yes	Array of CreateCondition objects	Condition list
mode	Yes	Integer	The value is fixed at 1 , indicating v2 false alarm masking rules. v1 is used only for compatibility with earlier versions, and false alarm rules cannot be created in v1.

Parameter	Mandatory	Type	Description
rule	Yes	String	<p>Items to be masked. You can provide multiple items and separate them with semicolons (;).</p> <ul style="list-style-type: none"> If you want to block a specific built-in rule, the value of this parameter is the rule ID. To query the rule ID, go to the WAF console, choose Policies and click the target policy name. On the displayed page, in the Basic Web Protection area, select the Protection Rules tab, and view the ID of the specific rule. You can also query the rule ID in the event details. If you want to mask a type of basic web protection rules, set this parameter to the name of the type of basic web protection rules. xss: XSS attacks webshell: Web shells vuln: Other types of attacks sqli: SQL injection attack robot: Malicious crawlers rfi: Remote file inclusion lfi: Local file inclusion cmdi: Command injection attack To bypass the basic web protection, set this parameter to all. To bypass all WAF protection, set this parameter to bypass.
advanced	No	Array of Advanced objects	"Advanced settings. The current parameter type is incorrect. Ignore this parameter. If the parameter type is correct, see the update interface. The parameter type will be corrected later."
description	No	String	Description of a masking rule

Table 4-213 CreateCondition

Parameter	Mandatory	Type	Description
category	Yes	String	Field type. The value can be ip , url , params , cookie , or header .
contents	Yes	Array of strings	Content. The array length is limited to 1 . The content format varies depending on the field type. For example, if the field type is ip , the value must be an IP address or IP address range. If the field type is url , the value must be in the standard URL format. IF the field type is params , cookie , or header , the content format is not limited.
logic_operation	Yes	String	The matching logic varies depending on the field type. For example, if the field type is ip , the logic can be equal or not_equal . If the field type is url , params , cookie , or header , the logic can be equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , not_suffix .
check_all_indexes_logic	No	Integer	This parameter is reserved and can be ignored.
index	No	String	If the field type is ip and the subfield is the client IP address, the index parameter is not required. If the subfield type is X-Forwarded-For , the value is x-forwarded-for . If the field type is params , header , or cookie , and the subfield is user-defined, the value of index is the user-defined subfield.

Table 4-214 Advanced

Parameter	Mandatory	Type	Description
index	No	String	Field type. The following field types are supported: params , cookie , header , body , and multipart** . <ul style="list-style-type: none"> If you select params, cookie, or header, you can select All or configure subfields you need. If you select body or multipart, you can select All.
contensts	No	Array of strings	Subfield of the specified field type. The default value is all .

Response Parameters

Status code: 200

Table 4-215 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
timestamp	Long	Timestamp the rule was created.
description	String	Rule Description
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> 0: The rule is disabled. 1: The rule is enabled.
rule	String	ID of the built-in rule to be masked. You can query the rule ID by choosing Policies > Policy Name > Basic Web Protection > Protection Rules on the WAF console or on the event details page.
mode	Integer	The value is fixed at 1 , indicating v2 false alarm masking rules are used. v1 is used only for compatibility with earlier versions, and false alarm rules cannot be created in v1.
conditions	Array of Condition objects	Condition list

Parameter	Type	Description
advanced	Array of Advanced objects	"Advanced settings. The current parameter type is incorrect. Ignore this parameter. If the parameter type is correct, see the update interface. The parameter type will be corrected later."
domain	Array of strings	Protected domain name or website

Table 4-216 Condition

Parameter	Type	Description
category	String	Field type. The value can be ip , url , params , cookie , or header .
contents	Array of strings	Content. The array length must be 1. The content format varies depending on field types. For example, if the field type is ip , the value must be an IP address or IP address range. If the field type is url , the value must be a URL in standard format. If the field type is params , cookie , or header , the content format is not limited.
logic_operation	String	The matching logic varies depending on the field type. For example, if the field type is ip , the logic can be equal or not_equal . If the field type is url , params , cookie , or header , the logic can be equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , not_suffix .
check_all_indexes_logic	Integer	This parameter is reserved and can be ignored.
index	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For , the value is x-forwarded-for . If the field type is params , header , or cookie , and the subfield is user-defined, the value of index is the user-defined subfield.

Table 4-217 Advanced

Parameter	Type	Description
index	String	Field type. The following field types are supported: params , cookie , header , body , and multipart** . <ul style="list-style-type: none">• If you select params, cookie, or header, you can select All or configure subfields you need.• If you select body or multipart, you can select All.
contensts	Array of strings	Subfield of the specified field type. The default value is all .

Status code: 400**Table 4-218** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401**Table 4-219** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500**Table 4-220** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a global whitelist protect (the formerly false alarm masking) rule. Details about the rule are specified by `project_id` and `policy_id`. The domain name is `we.test.418lab.cn`, the URL contains `x.x.x.x`, the description is `demo`, and the ID of the rule to be masked is `091004`.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore?enterprise_project_id=0
{
  "domain" : [ "we.test.418lab.cn" ],
  "conditions" : [ {
    "category" : "url",
    "logic_operation" : "contain",
    "contents" : [ "x.x.x.x" ],
    "index" : null
  } ],
  "mode" : 1,
  "description" : "demo",
  "rule" : "091004"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "a57f20ced01e4e0d8bea8e7c49eea254",
  "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",
  "timestamp" : 1650522310447,
  "description" : "demo",
  "status" : 1,
  "rule" : "091004",
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "x.x.x.x" ],
    "logic_operation" : "contain"
  } ],
  "domain" : [ "we.test.418lab.cn" ]
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.13 Querying the List of Global Protection Whitelist (Formerly False Alarm Masking) Rules

Function

This API is used to query the list of global protection whitelist (formerly false alarm masking) rules.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}

Table 4-221 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of a false alarm masking rule. You can obtain the rule ID from the id field in the response body of the ListIgnoreRule API, which is used for querying false alarm masking rules.

Table 4-222 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-223 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200**Table 4-224** Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
timestamp	Long	Timestamp the rule is created.
description	String	Rule description.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none">● 0: The rule is disabled.● 1: The rule is enabled.
url	String	The path for false masking alarms. This parameter is available only when mode is set to 0 .

Parameter	Type	Description
rule	String	<p>Items to be masked. You can provide multiple items and separate them with semicolons (;).</p> <ul style="list-style-type: none">To block a specific built-in rule, set the value of this parameter to the rule ID. To query the rule ID, go to the WAF console, choose Policies and click the target policy name. On the displayed page, in the Basic Web Protection area, select the Protection Rules tab, and view the ID of the specific rule. You can also query the rule ID in the event details.To mask a type of basic web protection rules, set this parameter to the name of the basic web protection rule type. xss: XSS attacks webshell: Web shells vuln: Other types of attacks sql: SQL injection attack robot: Malicious crawlers rfi: Remote file inclusion lfi: Local file inclusion cmdi: Command injection attackTo bypass the basic web protection, set this parameter to all.To bypass all WAF protection, set this parameter to bypass.
mode	Integer	<p>Version number. The value can be 0 or 1. 0: indicates the old version V1. 1 indicates the new version V2. When the value of mode is 0, the conditions field does not exist, but the url and url_logic fields exist. When the value of mode is 1, the url and url_logic fields do not exist, but the conditions field exists.</p>
url_logic	String	URL match logic
conditions	Array of Condition objects	Conditions
advanced	IgnoreAdvanced object	Advanced settings
domain	Array of strings	Protected domain name or website

Table 4-225 Condition

Parameter	Type	Description
category	String	Field type. The value can be ip , url , params , cookie , or header .
contents	Array of strings	Content. The array length must be 1. The content format varies depending on field types. For example, if the field type is ip , the value must be an IP address or IP address range. If the field type is url , the value must be a URL in standard format. If the field type is params , cookie , or header , the content format is not limited.
logic_operation	String	The matching logic varies depending on the field type. For example, if the field type is ip , the logic can be equal or not_equal . If the field type is url , params , cookie , or header , the logic can be equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , or not_suffix .
check_all_indexes_logic	Integer	This parameter is reserved and can be ignored.
index	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For , the value is x-forwarded-for . If the field type is params , header , or cookie , and the subfield is user-defined, the value of index is the user-defined subfield.

Table 4-226 IgnoreAdvanced

Parameter	Type	Description
index	String	Field type. The following field types are supported: Params , Cookie , Header , Body , and Multipart . <ul style="list-style-type: none"> When you select Params, Cookie, or Header, you can set this parameter to all or configure subfields as required. When you select Body or Multipart, set this parameter to all.
contents	Array of strings	Subfield of the specified field type. The default value is all .

Status code: 400

Table 4-227 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-228 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-229 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a global whitelist protect (the formerly false alarm masking) rule. Details about the query are specified by project_id, policy_id, and rule_id.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}
```

Example Responses

Status code: 200

Request sent.

```
{
  "id" : "16e81d9a9e0244359204d7f00326ee4f",
  "policyid" : "0681f69f94ac408e9688373e45a61fdb",
  "timestamp" : 1679106005786,
  "description" : "",
  "status" : 1,
  "rule" : "webshell;vuln",
  "mode" : 1,
```

```
"conditions": [ {
  "category": "url",
  "contents": [ "/test" ],
  "logic_operation": "contain"
}],
"domain": [ ],
"advanced": {
  "index": "params",
  "contents": [ ]
}
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.14 Updating a Global Protection Whitelist (Formerly False Alarm Masking) Rule

Function

This API is used to update a global protection whitelist (formerly false alarm masking) rule.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}

Table 4-230 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of a false alarm masking rule. You can obtain the rule ID from the id field in the response body of the ListIgnoreRule API, which is used for querying false alarm masking rules.

Table 4-231 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-232 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-233 Request body parameters

Parameter	Mandatory	Type	Description
domain	Yes	Array of strings	Domain name or website to be protected. If the array length is 0 , the rule takes effect for all domain names or websites.

Parameter	Mandatory	Type	Description
conditions	Yes	Array of CreateCondition objects	Condition list
mode	Yes	Integer	The value is fixed at 1 , indicating v2 false alarm masking rules. v1 is used only for compatibility with earlier versions, and false alarm rules cannot be created in v1.
rule	Yes	String	<p>Items to be masked. You can provide multiple items and separate them with semicolons (;).</p> <ul style="list-style-type: none"> To block a specific built-in rule, set the value of this parameter to the rule ID. To query the rule ID, go to the WAF console, choose Policies and click the target policy name. On the displayed page, in the Basic Web Protection area, select the Protection Rules tab, and view the ID of the specific rule. You can also query the rule ID in the event details. To mask a type of basic web protection rules, set this parameter to the name of the basic web protection rule type. xss: XSS attacks webshell: Web shells vuln: Other types of attacks sqli: SQL injection attack robot: Malicious crawlers rfi: Remote file inclusion lfi: Local file inclusion cmdi: Command injection attack To bypass the basic web protection, set this parameter to all. To bypass all WAF protection, set this parameter to bypass.
advanced	No	IgnoreAdvanced object	Advanced settings

Parameter	Mandatory	Type	Description
description	No	String	Description of a masking rule

Table 4-234 CreateCondition

Parameter	Mandatory	Type	Description
category	Yes	String	Field type. The value can be ip , url , params , cookie , or header .
contents	Yes	Array of strings	Content. The array length is limited to 1 . The content format varies depending on the field type. For example, if the field type is ip , the value must be an IP address or IP address range. If the field type is url , the value must be in the standard URL format. If the field type is params , cookie , or header , the content format is not limited.
logic_operation	Yes	String	The matching logic varies depending on the field type. For example, if the field type is ip , the logic can be equal or not_equal . If the field type is url , params , cookie , or header , the logic can be equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , or not_suffix .
check_all_indexes_logic	No	Integer	This parameter is reserved and can be ignored.
index	No	String	If the field type is ip and the subfield is the client IP address, the index parameter is not required. If the subfield type is X-Forwarded-For , the value is x-forwarded-for . If the field type is params , header , or cookie , and the subfield is user-defined, the value of index is the user-defined subfield.

Table 4-235 IgnoreAdvanced

Parameter	Mandatory	Type	Description
index	No	String	Field type. The following field types are supported: Params, Cookie, Header, Body, and Multipart. <ul style="list-style-type: none">• When you select Params, Cookie, or Header, you can set this parameter to all or configure subfields as required.• When you select Body or Multipart, set this parameter to all.
contents	No	Array of strings	Subfield of the specified field type. The default value is all .

Response Parameters

Status code: 200

Table 4-236 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
timestamp	Long	Timestamp the rule is created.
description	String	Rule description.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none">• 0: The rule is disabled.• 1: The rule is enabled.
url	String	The path for false masking alarms. This parameter is available only when mode is set to 0 .

Parameter	Type	Description
rule	String	<p>Items to be masked. You can provide multiple items and separate them with semicolons (;).</p> <ul style="list-style-type: none"> To block a specific built-in rule, set the value of this parameter to the rule ID. To query the rule ID, go to the WAF console, choose Policies and click the target policy name. On the displayed page, in the Basic Web Protection area, select the Protection Rules tab, and view the ID of the specific rule. You can also query the rule ID in the event details. To mask a type of basic web protection rules, set this parameter to the name of the basic web protection rule type. xss: XSS attacks webshell: Web shells vuln: Other types of attacks sqli: SQL injection attack robot: Malicious crawlers rfi: Remote file inclusion lfi: Local file inclusion cmdi: Command injection attack To bypass the basic web protection, set this parameter to all. To bypass all WAF protection, set this parameter to bypass.
mode	Integer	Version number. The value can be 0 or 1 . 0 : indicates the old version V1. 1 indicates the new version V2. When the value of mode is 0 , the conditions field does not exist, but the url and url_logic fields exist. When the value of mode is 1 , the url and url_logic fields do not exist, but the conditions field exists.
url_logic	String	URL match logic
conditions	Array of Condition objects	Conditions
advanced	IgnoreAdvanced object	Advanced settings
domain	Array of strings	Protected domain name or website

Table 4-237 Condition

Parameter	Type	Description
category	String	Field type. The value can be ip , url , params , cookie , or header .
contents	Array of strings	Content. The array length must be 1. The content format varies depending on field types. For example, if the field type is ip , the value must be an IP address or IP address range. If the field type is url , the value must be a URL in standard format. If the field type is params , cookie , or header , the content format is not limited.
logic_operation	String	The matching logic varies depending on the field type. For example, if the field type is ip , the logic can be equal or not_equal . If the field type is url , params , cookie , or header , the logic can be equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , or not_suffix .
check_all_indexes_logic	Integer	This parameter is reserved and can be ignored.
index	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For , the value is x-forwarded-for . If the field type is params , header , or cookie , and the subfield is user-defined, the value of index is the user-defined subfield.

Table 4-238 IgnoreAdvanced

Parameter	Type	Description
index	String	Field type. The following field types are supported: Params , Cookie , Header , Body , and Multipart . <ul style="list-style-type: none"> When you select Params, Cookie, or Header, you can set this parameter to all or configure subfields as required. When you select Body or Multipart, set this parameter to all.
contents	Array of strings	Subfield of the specified field type. The default value is all .

Status code: 400

Table 4-239 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-240 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-241 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a global whitelist protect (the formerly false alarm masking) rule. Details about the rule are specified by project_id, policy_id, and rule_id. Set the protection condition to URL containing /test, set the rules to be masked to website Trojans and other types of attacks, and set advanced settings to all parameters.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}
```

```
{
  "domain" : [ ],
  "mode" : 1,
  "description" : "",
  "conditions" : [ {
    "category" : "url",
    "logic_operation" : "contain",
    "index" : null,
    "contents" : [ "/test" ]
  } ],
  "rule" : "webshell;vuln",
  "advanced" : {
    "index" : "params",
```

```
"contents" : [ ]  
}  
}
```

Example Responses

Status code: 200

Request sent.

```
{  
  "id" : "16e81d9a9e0244359204d7f00326ee4f",  
  "policyid" : "0681f69f94ac408e9688373e45a61fdb",  
  "timestamp" : 1679106005786,  
  "description" : "",  
  "status" : 1,  
  "rule" : "webshell;vuln",  
  "mode" : 1,  
  "conditions" : [ {  
    "category" : "url",  
    "contents" : [ "/test" ],  
    "logic_operation" : "contain"  
  } ],  
  "domain" : [ ],  
  "advanced" : {  
    "index" : "params",  
    "contents" : [ ]  
  }  
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.15 Deleting a Global Protection Whitelist (Formerly False Alarm Masking) Rule

Function

This API is used to delete a global protection whitelist (formerly false alarm masking) rule.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}

Table 4-242 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of a false alarm masking rule. You can obtain the rule ID from the id field in the response body of the ListIgnoreRule API, which is used for querying false alarm masking rules.

Table 4-243 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-244 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-245 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
timestamp	Long	Timestamp the rule was created.
description	String	Rule Description
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> 0: The rule is disabled. 1: The rule is enabled.
url	String	The path for false masking alarms. This parameter is available only when mode is set to 0 .
rule	String	ID of the built-in rule to be masked. You can query the rule ID by choosing Policies > Policy Name > Basic Web Protection > Protection Rules on the WAF console or on the event details page.
mode	Integer	Version number. The value can be 0 or 1 . 0 : indicates the old version V1. 1 indicates the new version V2. When the value of mode is 0 , the conditions field does not exist, but the url and url_logic fields exist. When the value of mode is 1 , the url and url_logic fields do not exist, but the conditions field exists.
url_logic	String	URL match logic
conditions	Array of Condition objects	Filter
advanced	Array of Advanced objects	"Advanced settings. The current parameter type is incorrect. Ignore this parameter. If the parameter type is correct, see the update interface. The parameter type will be corrected later."
domains	Array of strings	Protected domain name or website

Table 4-246 Condition

Parameter	Type	Description
category	String	Field type. The value can be ip , url , params , cookie , or header .
contents	Array of strings	Content. The array length must be 1. The content format varies depending on field types. For example, if the field type is ip , the value must be an IP address or IP address range. If the field type is url , the value must be a URL in standard format. If the field type is params , cookie , or header , the content format is not limited.
logic_operation	String	The matching logic varies depending on the field type. For example, if the field type is ip , the logic can be equal or not_equal . If the field type is url , params , cookie , or header , the logic can be equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , not_suffix .
check_all_indexes_logic	Integer	This parameter is reserved and can be ignored.
index	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For , the value is x-forwarded-for . If the field type is params , header , or cookie , and the subfield is user-defined, the value of index is the user-defined subfield.

Table 4-247 Advanced

Parameter	Type	Description
index	String	Field type. The following field types are supported: params , cookie , header , body , and multipart** . <ul style="list-style-type: none"> If you select params, cookie, or header, you can select All or configure subfields you need. If you select body or multipart, you can select All.
contentsts	Array of strings	Subfield of the specified field type. The default value is all .

Status code: 400

Table 4-248 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-249 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-250 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a global whitelist protect (the formerly false alarm masking) rule Details about the rule are specified by project_id, policy_id, and rule_id.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}
```

Example Responses

Status code: 200

Request succeeded.

```
{  
  "id" : "40484384970948d79ffe4e4ae1fc54d",  
  "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",  
  "timestamp" : 1650512535222,  
  "description" : "demo",  
  "status" : 1,  
  "rule" : "091004",  
  "mode" : 1,  
}
```

```
"conditions" : [ {
  "category" : "ip",
  "contents" : [ "x.x.x.x" ],
  "logic_operation" : "equal"
} ],
"domain" : [ "we.test.418lab.cn" ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.16 Querying the Blacklist and Whitelist Rule List

Function

This API is used to query the list of blacklist and whitelist rules.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip

Table 4-251 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-252 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned. Default: 1
pagesize	No	Integer	Number of results on each page during pagination query. Value range: 1 to 100 . The default value is 10 , indicating that each page contains 10 results. Default: 10
name	No	String	Name of the whitelist or blacklist rule

Request Parameters

Table 4-253 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-254 Response body parameters

Parameter	Type	Description
total	Integer	Number of the whitelist and blacklist rules

Parameter	Type	Description
items	Array of WhiteBlackIpResponseBody objects	Details of blacklist or whitelist rules

Table 4-255 WhiteBlackIpResponseBody

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the whitelist or blacklist rule
policyid	String	Policy ID
timestamp	Long	Timestamp (ms) when the rule was created
description	String	Rule Description
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
addr	String	IP address/IP address group
white	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.
ip_group	Ip_group object	IP address group

Table 4-256 Ip_group

Parameter	Type	Description
id	String	ID of the IP address group
name	String	Name of the IP address group
size	Long	Number of IP addresses or IP address ranges in the IP address group

Status code: 400

Table 4-257 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-258 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-259 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the whitelist and blacklist rule list in a project. The project ID is specified by `project_id`, and the policy is specified by `policy_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "items": [ {
    "id": "3c96caf769ca4f57814fcf4259ea89a1",
    "policyid": "4dddfd44fc89453e9fd9cd6bfdc39db2",
    "name": "hkhtest",
    "timestamp": 1650362891844,
    "description": "demo",
    "status": 1,
    "addr": "x.x.x.x",
    "white": 0
  }
]
```

```
}]  
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.17 Creating a Blacklist/Whitelist Rule

Function

This API is used to create a blacklist or whitelist rule.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/whiteblackip

Table 4-260 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-261 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-262 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-263 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rue name. The value can contain a maximum of 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
addr	No	String	IP address or IP address ranges in the blacklist or whitelist rule, for example, 42.123.120.66 or 42.123.120.0/16.
description	No	String	Rule description
white	Yes	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.

Parameter	Mandatory	Type	Description
ip_group_id	No	String	ID of the created IP address group. Use either this parameter or addr . To add an IP address group, go to the WAF console, choose Objects > Address Groups , and click Add Address Group .

Response Parameters

Status code: 200

Table 4-264 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the whitelist or blacklist rule
policyid	String	Policy ID
addr	String	IP address or IP address ranges in the blacklist or whitelist rule, for example, 42.123.120.66 or 42.123.120.0/16.
white	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.
ip_group	ip_group object	IP address group
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
description	String	Rule Description
timestamp	Long	Time a rule is created. The value is a 13-digit timestamp in millisecond.

Table 4-265 Ip_group

Parameter	Type	Description
id	String	ID of the IP address group
name	String	Name of the IP address group
size	Long	Number of IP addresses or IP address ranges in the IP address group

Status code: 400

Table 4-266 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-267 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-268 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a whitelist or blacklist rule in a protection policy. The project ID is specified by `project_id`, and the policy ID is specified by `policy_id`. The rule name is `demo`, the protective action is `block`, the description is `demo`, and the IP address of the rule is `x.x.x`.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip?enterprise_project_id=0
```

```
{  
  "name" : "demo",  
  "white" : 0,  
  "description" : "demo",  
  "addr" : "x.x.x.x"  
}
```

Example Responses

Status code: 200

OK

```
{  
  "id" : "5d43af25404341058d5ab17b7ba78b56",  
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",  
  "name" : "demo",  
  "timestamp" : 1650531872900,  
  "description" : "demo",  
  "status" : 1,  
  "addr" : "x.x.x.x",  
  "white" : 0  
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.18 Querying a blacklist or whitelist rule

Function

Querying a blacklist or whitelist rule

URI

GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}

Table 4-269 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of the IP address whitelist or blacklist rule. You can obtain the ID by calling the ListWhiteblackipRule API used for querying the IP address whitelist and blacklist rules.

Table 4-270 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-271 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-272 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
name	String	Name of the whitelist or blacklist rule
policyid	String	Policy ID.
addr	String	IP address or IP address ranges in the blacklist or whitelist rule, for example, 42.123.120.66 or 42.123.120.0/16.
white	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests hit the rule. ● 1: WAF allows requests hit the rule. ● 2: WAF only record requests hit the rule.
ip_group	ip_group object	IP address group
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
description	String	Rule description.
timestamp	Long	Time a rule is created. The value is a 13-digit timestamp in millisecond.

Table 4-273 Ip_group

Parameter	Type	Description
id	String	ID of the IP address group
name	String	Name of the IP address group
size	Long	Number of IP addresses or IP address ranges in the IP address group

Status code: 400

Table 4-274 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-275 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-276 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a whitelist or blacklist protection rule in a policy. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

Request sent.

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650531872900,
  "description" : "demo",
  "status" : 1,
  "addr" : "1.1.1.2",
  "white" : 0
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.19 Updating a Blacklist or Whitelist Protection Rule

Function

This API is used to update blacklist and whitelist protection rules. You can update IP addresses, IP address ranges, protective actions, and other information.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}

Table 4-277 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of the blacklist or whitelist rule. It can be obtained by calling the ListWhiteblackipRule API.

Table 4-278 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-279 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-280 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the whitelist or blacklist rule
addr	No	String	IP address or IP address ranges in the blacklist or whitelist rule, for example, 42.123.120.66 or 42.123.120.0/16.
description	No	String	Rule description
white	Yes	Integer	Protective action <ul style="list-style-type: none">● 0: WAF blocks requests that hit the rule.● 1: WAF allows requests that hit the rule.● 2: WAF only record requests that hit the rule.

Parameter	Mandatory	Type	Description
ip_group_id	No	String	ID of the created IP address group. Use either this parameter or addr . To add an IP address group, go to the WAF console, choose Objects > Address Groups , and click Add Address Group .

Response Parameters

Status code: 200

Table 4-281 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the whitelist or blacklist rule
policyid	String	Policy ID
addr	String	IP address or IP address ranges included in the whitelist or blacklist rule.
description	String	Description of the blacklist or whitelist rule
white	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.
ip_group	Ip_group object	IP address group

Table 4-282 Ip_group

Parameter	Type	Description
id	String	ID of the IP address group
name	String	Name of the IP address group
size	Long	Number of IP addresses or IP address ranges in the IP address group

Status code: 400

Table 4-283 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-284 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-285 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a whitelist or blacklist protection rule in a policy. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`. The rule name is changed to `demo`, protective action to `block`, description to `demo`, and blacklist/whitelist IP address to `1.1.1.2`.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}?enterprise_project_id=0
{
  "name" : "demo",
  "white" : 0,
  "description" : "demo",
  "addr" : "1.1.1.2"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
}
```

```

"policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
"name" : "demo",
"description" : "demo",
"addr" : "1.1.1.2",
"white" : 0
}

```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.20 Querying Global Protection Whitelist (Formerly False Alarm Masking) Rules

Function

Querying Global Protection Whitelist (Formerly False Alarm Masking) Rules

URI

GET /v1/{project_id}/waf/policy/{policy_id}/ignore

Table 4-286 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-287 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned. Default: 1
pagesize	No	Integer	Number of results on each page during pagination query. Value range: 1 to 100 . The default value is 10 , indicating that each page contains 10 results. Default: 10

Request Parameters

Table 4-288 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-289 Response body parameters

Parameter	Type	Description
total	Integer	The number of global protection whitelist (formerly false alarm masking) rules in the protection policy.

Parameter	Type	Description
items	Array of IgnoreRuleBody objects	Domain names the global protection whitelist (formerly false alarm masking) rule is used for.

Table 4-290 IgnoreRuleBody

Parameter	Type	Description
id	String	Rule ID
policyid	String	ID of the protection policy that includes the rule
timestamp	Long	Timestamp the rule was created.
description	String	Rule description
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
url	String	The path for false masking alarms. This parameter is available only when mode is set to 0 .
rule	String	Rules to be masked <ul style="list-style-type: none"> ● If you want to block a specific built-in rule, the value of this parameter is the rule ID. To query the rule ID, go to the WAF console, choose Policies and click the target policy name. On the displayed page, in the Basic Web Protection area, select the Protection Rules tab, and view the ID of the specific rule. You can also query the rule ID in the event details. ● If you want to mask a type of basic web protection rules, set this parameter to the name of the type of basic web protection rules. xss: XSS attacks webshell: Web shells vuln: Other types of attacks sqli: SQL injection attack robot: Malicious crawlers rfi: Remote file inclusion lfi: Local file inclusion cmdi: Command injection attack ● To bypass the basic web protection, set this parameter to all. ● To bypass all WAF protection, set this parameter to bypass.

Parameter	Type	Description
mode	Integer	Version number. The value 0 indicates the old version V1, and the value 1 indicates the new version V2. If the value of mode is 0, the conditions field does not exist, and the url and url_logic fields exist. When the value of mode is 1, the url and url_logic fields do not exist, and the conditions field exists.
url_logic	String	Matching logic. The value can be equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , not_suffix .
conditions	Array of Condition objects	Condition list
domain	Array of strings	Protecting Domain Names or Protecting Websites
advanced	Array of Advanced objects	"Advanced settings."

Table 4-291 Condition

Parameter	Type	Description
category	String	Field type. The value can be ip , url , params , cookie , or header .
contents	Array of strings	Content. The array length must be 1. The content format varies depending on field types. For example, if the field type is ip, the value must be an IP address or IP address range. If the field type is url, the value must be a URL in standard format. If the field type is params, cookie, or header, the content format is not limited.
logic_operation	String	The matching logic varies depending on the field type. For example, if the field type is ip , the logic can be equal or not_equal . If the field type is url , params , cookie , or header , the logic can be equal , not_equal , contain , not_contain , prefix , not_prefix , suffix , not_suffix .
check_all_indexes_logic	Integer	This parameter is reserved and can be ignored.

Parameter	Type	Description
index	String	If the field type is ip and the subfield is the client IP address, the index parameter does not exist. If the subfield type is X-Forwarded-For , the value is x-forwarded-for . If the field type is params , header , or cookie , and the subfield is user-defined, the value of index is the user-defined subfield.

Table 4-292 Advanced

Parameter	Type	Description
index	String	Field type. The following field types are supported: params , cookie , header , body , and multipart** . <ul style="list-style-type: none"> If you select params, cookie, or header, you can select All or configure subfields you need. If you select body or multipart, you can select All.
contensts	Array of strings	Subfield of the specified field type. The default value is all .

Status code: 400

Table 4-293 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-294 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 403

Table 4-295 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-296 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the global whitelist protect (the formerly false alarm masking) rule list. Details about the query are specified by project_id and policy_id.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/ignore?
enterprise_project_id=0&page=1&pagesize=10
```

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "40484384970948d79ffe4e4ae1fc54d",
    "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",
    "timestamp" : 1650512535222,
    "description" : "demo",
    "status" : 1,
    "rule" : "091004",
    "mode" : 1,
    "conditions" : [ {
      "category" : "ip",
      "contents" : [ "x.x.x.x" ],
      "logic_operation" : "equal"
    } ],
    "domain" : [ "we.test.418lab.cn" ]
  } ]
}
```


Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
403	Insufficient resource quota.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.21 Deleting a Blacklist or Whitelist Rule

Function

This API is used to delete a blacklist or whitelist rule.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}

Table 4-297 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of a blacklist or whitelist rule. You can obtain the rule ID by calling the ListWhiteblackipRule API.

Table 4-298 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-299 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-300 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
name	String	Name of the whitelist or blacklist rule
timestamp	Long	Time a rule is deleted. The value must be a 13-digit timestamp in millisecond.
description	String	Description
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> 0: The rule is disabled. 1: The rule is enabled.
addr	String	IP address or IP address ranges in the blacklist or whitelist rule, for example, 42.123.120.66 or 42.123.120.0/16.

Parameter	Type	Description
white	Integer	Protective action <ul style="list-style-type: none"> • 0: WAF blocks requests that hit the rule. • 1: WAF allows requests that hit the rule. • 2: WAF only record requests that hit the rule.
ip_group	Ip_group object	IP address group

Table 4-301 Ip_group

Parameter	Type	Description
id	String	ID of the IP address group
name	String	Name of the IP address group
size	Long	Number of IP addresses or IP address ranges in the IP address group

Status code: 400

Table 4-302 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-303 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-304 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a whitelist or blacklist protection rule in a policy. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}?
enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650531872900,
  "description" : "demo",
  "status" : 1,
  "addr" : "1.1.1.2",
  "white" : 0
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.22 Querying the JavaScript Anti-Crawler Rule List

Function

This API is used to query the list of JavaScript anti-crawler rules.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/anticrawler

Table 4-305 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.

Table 4-306 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
offset	Yes	Integer	Offset. The records after the offset are queried.
limit	Yes	Integer	Maximum number of records that can be returned.

Parameter	Mandatory	Type	Description
type	No	String	JavaScript anti-crawler rule protection mode <ul style="list-style-type: none"> • anticrawler_except_url: In this mode, all paths are protected except the one specified in the queried anti-crawler rule. • anticrawler_specific_url: In this mode, the path specified in the queried rule is protected.

Request Parameters

Table 4-307 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json; charset=utf8

Response Parameters

Status code: 200

Table 4-308 Response body parameters

Parameter	Type	Description
total	Integer	The number of anti-crawler rules in the current policy.
items	Array of AnticrawlerRule objects	The list of anti-crawler protection rules.

Table 4-309 AnticrawlerRule

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
conditions	Array of AnticrawlerCondition objects	Condition list.
name	String	Rule name.
type	String	JavaScript anti-crawler rule type. <ul style="list-style-type: none"> • anticrawler_specific_url: used to protect a specific path specified by the rule. • anticrawler_except_url: used to protect all paths except the one specified by the rule.
timestamp	Long	Timestamp the rule is created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The rule is disabled. • 1: The rule is enabled.
priority	Integer	Priority of the rule. A smaller value indicates a higher priority. If the value is the same, the rule is created earlier and the priority is higher. Value range: 0 to 1000.

Table 4-310 AnticrawlerCondition

Parameter	Type	Description
category	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • user-agent
logic_operation	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.

Parameter	Type	Description
value_list_id	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.

Status code: 400

Table 4-311 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-312 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-313 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the JavaScript-based anti-crawler protection rule list in a policy. The project ID is specified by `project_id`, and the policy ID is specified by `policy_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/anticrawler?
```


Example Responses

Status code: 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "c06ec2e5d93241a694fcd9e0312657a1",
    "policyid" : "0681f69f94ac408e9688373e45a61fdb",
    "name" : "test",
    "timestamp" : 1678931359146,
    "status" : 1,
    "type" : "anticrawler_except_url",
    "conditions" : [ {
      "category" : "url",
      "contents" : [ "/test" ],
      "logic_operation" : "contain"
    } ],
    "priority" : 50
  } ]
}
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.23 Updating a JavaScript Anti-Crawler Protection Rule

Function

This API is used to update the protection mode for a JavaScript anti-crawler rule. Before creating a JavaScript anti-crawler rule, you need to call this API to specify the protection mode for the rule.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/anticrawler

Table 4-314 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.

Table 4-315 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-316 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-317 Request body parameters

Parameter	Mandatory	Type	Description
anticrawler_type	Yes	String	JavaScript anti-crawler rule type. <ul style="list-style-type: none"> • anticrawler_specific_url: used to protect a specific path specified by the rule. • anticrawler_except_url: used to protect all paths except the one specified by the rule.

Response Parameters

Status code: 200

Table 4-318 Response body parameters

Parameter	Type	Description
anticrawler_type	String	JavaScript anti-crawler rule type. <ul style="list-style-type: none"> • anticrawler_specific_url: used to protect a specific path specified by the rule. • anticrawler_except_url: used to protect all paths except the one specified by the rule.

Status code: 400

Table 4-319 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-320 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-321 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a JavaScript-based anti-crawler rule in a policy. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`. The rule type is changed to excluding protection paths.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/anticrawler?
{
  "anticrawler_type": "anticrawler_except_url"
}
```

Example Responses

Status code: 200

ok

```
{
  "anticrawler_type": "anticrawler_except_url"
}
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.24 Creating a JavaScript Anti-Crawler Rule

Function

This API is used to create a JavaScript anti-crawler rule. Before invoking this API, you need to call the **UpdateAnticrawlerRuleType** API to specify the protection mode.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/anticrawler

Table 4-322 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.

Table 4-323 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-324 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-325 Request body parameters

Parameter	Mandatory	Type	Description
conditions	Yes	Array of AnticrawlerCondition objects	Condition list.
name	Yes	String	Rule name.
type	Yes	String	JavaScript anti-crawler rule type. <ul style="list-style-type: none">• anticrawler_specific_url: used to protect a specific path specified by the rule.• anticrawler_except_url: used to protect all paths except the one specified by the rule.
priority	Yes	Integer	Priority of the rule. A smaller value indicates a higher priority. If the value is the same, the rule is created earlier and the priority is higher. Value range: 0 to 1000.

Table 4-326 AnticrawlerCondition

Parameter	Mandatory	Type	Description
category	No	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • user-agent
logic_operation	No	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	No	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	No	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.

Response Parameters

Status code: 200

Table 4-327 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
conditions	Array of AnticrawlerCondition objects	Condition list.
name	String	Rule name.

Parameter	Type	Description
type	String	JavaScript anti-crawler rule type. <ul style="list-style-type: none"> ● anticrawler_specific_url: used to protect a specific path specified by the rule. ● anticrawler_except_url: used to protect all paths except the one specified by the rule.
timestamp	Long	Timestamp the rule is created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
priority	Integer	Priority of the rule. A smaller value indicates a higher priority. If the value is the same, the rule is created earlier and the priority is higher. Value range: 0 to 1000.

Table 4-328 AnticrawlerCondition

Parameter	Type	Description
category	String	Field type. Enumeration values: <ul style="list-style-type: none"> ● url ● user-agent
logic_operation	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.

Status code: 400

Table 4-329 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-330 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-331 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a JavaScript-based anti-crawler rule in a policy. The project ID is specified by `project_id`, and the policy ID is specified by `policy_id`. The rule name is `test66`, the rule type is excluding protection paths, the match condition is url that contains `/test66`, and the priority is 50.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/anticrawler?
{
  "name": "test66",
  "type": "anticrawler_except_url",
  "conditions": [ {
    "category": "url",
    "logic_operation": "contain",
    "contents": [ "/test66" ]
  } ],
  "priority": 50
}
```

Example Responses

Status code: 200

ok

```
{
  "id" : "7e7983bf2c9c41029d642bcbf819346d",
  "policyid" : "0681f69f94ac408e9688373e45a61fdb",
  "name" : "test66",
  "timestamp" : 1678931492172,
  "status" : 1,
  "type" : "anticrawler_except_url",
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "/test66" ],
    "logic_operation" : "contain"
  } ],
  "priority" : 50
}
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.25 Querying a JavaScript Anti-Crawler Rule

Function

This API is used to query a JavaScript anti-crawler rule by ID.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}

Table 4-332 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Parameter	Mandatory	Type	Description
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.
rule_id	Yes	String	Rule ID.

Table 4-333 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-334 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-335 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.

Parameter	Type	Description
conditions	Array of AnticrawlerCondition objects	Condition list.
name	String	Rule name.
type	String	JavaScript anti-crawler rule type. <ul style="list-style-type: none"> • anticrawler_specific_url: used to protect a specific path specified by the rule. • anticrawler_except_url: used to protect all paths except the one specified by the rule.
timestamp	Long	Timestamp the rule is created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The rule is disabled. • 1: The rule is enabled.
priority	Integer	Priority of the rule. A smaller value indicates a higher priority. If the value is the same, the rule is created earlier and the priority is higher. Value range: 0 to 1000.

Table 4-336 AnticrawlerCondition

Parameter	Type	Description
category	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • user-agent
logic_operation	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.

Status code: 400

Table 4-337 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-338 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-339 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a JavaScript-based anti-crawler rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}?
```

Example Responses

Status code: 200

ok

```
{  
  "id" : "7e7983bf2c9c41029d642bcbf819346d",  
  "policyid" : "0681f69f94ac408e9688373e45a61fdb",  
  "name" : "test66",  
  "timestamp" : 1678931492172,  
  "status" : 1,  
  "type" : "anticrawler_except_url",  
  "conditions" : [ {
```

```

"category" : "url",
"contents" : [ "/test66" ],
"logic_operation" : "contain"
}],
"priority" : 50
}

```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.26 Updating a JavaScript Anti-Crawler Rule

Function

This API is used to update a JavaScript anti-crawler rule.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}

Table 4-340 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.

Parameter	Mandatory	Type	Description
rule_id	Yes	String	Rule ID.

Table 4-341 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-342 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-343 Request body parameters

Parameter	Mandatory	Type	Description
conditions	Yes	Array of AnticrawlerCondition objects	Condition list.
name	Yes	String	Rule name.
type	Yes	String	JavaScript anti-crawler rule type. <ul style="list-style-type: none">• anticrawler_specific_url: used to protect a specific path specified by the rule.• anticrawler_except_url: used to protect all paths except the one specified by the rule.

Parameter	Mandatory	Type	Description
priority	Yes	Integer	Priority of the rule. A smaller value indicates a higher priority. If the value is the same, the rule is created earlier and the priority is higher. Value range: 0 to 1000.

Table 4-344 AnticrawlerCondition

Parameter	Mandatory	Type	Description
category	No	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • user-agent
logic_operation	No	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	No	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	No	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.

Response Parameters

Status code: 200

Table 4-345 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
conditions	Array of AnticrawlerCondition objects	Condition list.
name	String	Rule name.
type	String	JavaScript anti-crawler rule type. <ul style="list-style-type: none"> • anticrawler_specific_url: used to protect a specific path specified by the rule. • anticrawler_except_url: used to protect all paths except the one specified by the rule.
timestamp	Long	Timestamp the rule is created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The rule is disabled. • 1: The rule is enabled.
priority	Integer	Priority of the rule. A smaller value indicates a higher priority. If the value is the same, the rule is created earlier and the priority is higher. Value range: 0 to 1000.

Table 4-346 AnticrawlerCondition

Parameter	Type	Description
category	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • user-agent
logic_operation	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.
contents	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.

Parameter	Type	Description
value_list_id	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.

Status code: 400

Table 4-347 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-348 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-349 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a JavaScript-based anti-crawler rule in a policy. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`. The rule name is `test66`, the rule type is excluding protection paths, the match condition is url that contains `/test66`, and the priority is 50.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}?  
  
{  
  "name" : "test66",  
  "type" : "anticrawler_except_url",  
  "conditions" : [ {  
    "category" : "url",  
    "logic_operation" : "contain",  
    "contents" : [ "/test66" ]  
  } ],  
  "priority" : 50  
}
```

Example Responses

Status code: 200

ok

```
{  
  "id" : "7e7983bf2c9c41029d642bcbf819346d",  
  "policyid" : "0681f69f94ac408e9688373e45a61fdb",  
  "name" : "test66",  
  "timestamp" : 1678931492172,  
  "status" : 1,  
  "type" : "anticrawler_except_url",  
  "conditions" : [ {  
    "category" : "url",  
    "contents" : [ "/test66" ],  
    "logic_operation" : "contain"  
  } ],  
  "priority" : 50  
}
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.27 Deleting a JavaScript Anti-Crawler Rule

Function

This API is used to delete a JavaScript anti-crawler rule.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}

Table 4-350 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.
rule_id	Yes	String	Rule ID.

Table 4-351 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-352 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-353 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
conditions	Array of AnticrawlerCondition objects	Condition list.
name	String	Rule name.
type	String	JavaScript anti-crawler rule type. <ul style="list-style-type: none"> • anticrawler_specific_url: used to protect a specific path specified by the rule. • anticrawler_except_url: used to protect all paths except the one specified by the rule.
timestamp	Long	Timestamp the rule is created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The rule is disabled. • 1: The rule is enabled.
priority	Integer	Priority of the rule. A smaller value indicates a higher priority. If the value is the same, the rule is created earlier and the priority is higher. Value range: 0 to 1000.

Table 4-354 AnticrawlerCondition

Parameter	Type	Description
category	String	Field type. Enumeration values: <ul style="list-style-type: none"> • url • user-agent
logic_operation	String	Logic for matching the condition. The options are contain , not_contain , equal , not_equal , prefix , not_prefix , suffix , and not_suffix . For more details, see the console UI.

Parameter	Type	Description
contents	Array of strings	Content of the conditions. This parameter is mandatory when the suffix of logic_operation is not any or all.
value_list_id	String	Reference table ID. It can be obtained by calling the API Querying the Reference Table List. This parameter is mandatory when the suffix of logic_operation is any or all. The reference table type must be the same as the category type.

Status code: 400

Table 4-355 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-356 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-357 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a JavaScript-based anti-crawler rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}?
```

Example Responses

Status code: 200

ok

```
{
  "id" : "7e7983bf2c9c41029d642bcbf819346d",
  "policyid" : "0681f69f94ac408e9688373e45a61fdb",
  "name" : "test66",
  "timestamp" : 1678931492172,
  "status" : 1,
  "type" : "anticrawler_except_url",
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "/test66" ],
    "logic_operation" : "contain"
  } ],
  "priority" : 50
}
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.28 Querying the list of Data Masking Rules.

Function

Querying the list of Data Masking Rules.

URI

```
GET /v1/{project_id}/waf/policy/{policy_id}/privacy
```

Table 4-358 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-359 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned.
pagesize	No	Integer	Number of results on each page during pagination query. Value range: 1 to 100 . The default value is 10 , indicating that each page contains 10 results.

Request Parameters

Table 4-360 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json; charset=utf8

Response Parameters

Status code: 200

Table 4-361 Response body parameters

Parameter	Type	Description
total	Integer	Number of rules
items	Array of PrivacyResponseBody objects	Array of rule details

Table 4-362 PrivacyResponseBody

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
timestamp	Long	Time the rule was created. The value is a 13-digit timestamp in ms.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
url	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/. <i>The asterisk () indicates the path prefix.</i>

Parameter	Type	Description
category	String	Masked field. <ul style="list-style-type: none"> • Params: The params field in requests • Cookie: Web visitors distinguished by cookie • Header: Custom HTTP header • Form: Forms Enumeration values: <ul style="list-style-type: none"> • params • cookie • header • form
index	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs.
description	String	(Optional) A description of the rule.

Status code: 400

Table 4-363 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-364 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-365 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the data masking protection rule list. The project ID is specified by `project_id` and the policy ID is specified by `policy_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total": 1,
  "items": [ {
    "id": "97e4d35f375f4736a21cccfad77613eb",
    "policyid": "38ff0cb9a10e4d5293c642bc0350fa6d",
    "timestamp": 1650533191385,
    "description": "demo",
    "status": 1,
    "url": "/demo",
    "category": "cookie",
    "index": "demo"
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.29 Creating a Data Masking Rule

Function

This API is used to create a data masking rule.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/privacy

Table 4-366 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-367 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-368 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-369 Request body parameters

Parameter	Mandatory	Type	Description
url	Yes	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/. The asterisk (*) indicates the path prefix.
category	Yes	String	Masked field. <ul style="list-style-type: none"> • Params: The params field in requests • Cookie: Web visitors distinguished by cookie • Header: Custom HTTP header • Form: Forms Enumeration values: <ul style="list-style-type: none"> • params • cookie • header • form
index	Yes	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs. The masked field name cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.
description	No	String	(Optional) A description of the rule.

Response Parameters

Status code: 200

Table 4-370 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID

Parameter	Type	Description
timestamp	Long	Time the rule was created. The value is a 13-digit timestamp in ms.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
url	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/. <i>The asterisk (*) indicates the path prefix.</i>
category	String	Masked field. <ul style="list-style-type: none"> ● Params: The params field in requests ● Cookie: Web visitors distinguished by cookie ● Header: Custom HTTP header ● Form: Forms Enumeration values: <ul style="list-style-type: none"> ● params ● cookie ● header ● form
index	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs.
description	String	(Optional) A description of the rule.

Status code: 400

Table 4-371 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-372 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-373 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a data masking rule in a policy. The project ID is specified by `project_id` and the policy ID is specified by `policy_id`. The url of the rule is `/demo`, the masking field is `cookie`, the masking field name is `demo`, and the rule description is `demo`.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy?enterprise_project_id=0
{
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo",
  "description" : "demo"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "97e4d35f375f4736a21cccfad77613eb",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "timestamp" : 1650533191385,
  "description" : "demo",
  "status" : 1,
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.30 Querying a Data Masking Rule

Function

Querying a the Data Masking Rule

URI

GET /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}

Table 4-374 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of the data masking rule. You can obtain the rule ID by calling the ListPrivacyRule API which is used for querying the data masking rule list.

Table 4-375 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-376 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-377 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
timestamp	Long	Time the rule was created. The value is a 13-digit timestamp in ms.
description	String	(Optional) A description of the rule.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> 0: The rule is disabled. 1: The rule is enabled.
url	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/. <i>The asterisk () indicates the path prefix.</i>

Parameter	Type	Description
category	String	Masked field. <ul style="list-style-type: none"> • Params: The params field in requests • Cookie: Web visitors distinguished by cookie • Header: Custom HTTP header • Form: Forms
index	String	Name of the masked field

Status code: 400

Table 4-378 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-379 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-380 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a data masking rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}?enterprise_project_id=0

Example Responses

Status code: 200

Request sent.

```
{
  "id" : "97e4d35f375f4736a21cccfad77613eb",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "timestamp" : 1650533191385,
  "description" : "demo",
  "status" : 1,
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo1"
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.31 Updating a Data Masking Rule

Function

This API is used to update a data masking rule.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}

Table 4-381 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of the data masking rule. You can obtain the rule ID by calling the ListPrivacyRule API which is used for querying the data masking rule list.

Table 4-382 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-383 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-384 Request body parameters

Parameter	Mandatory	Type	Description
url	Yes	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/. The asterisk (*) indicates the path prefix.
category	Yes	String	Masked field. <ul style="list-style-type: none"> • Params: The params field in requests • Cookie: Web visitors distinguished by cookie • Header: Custom HTTP header • Form: Forms Enumeration values: <ul style="list-style-type: none"> • params • cookie • header • form
index	Yes	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs. The masked field name cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.
description	No	String	(Optional) A description of the rule.

Response Parameters

Status code: 200

Table 4-385 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID

Parameter	Type	Description
timestamp	Long	Time the rule was created. The value is a 13-digit timestamp in ms.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
url	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/. <i>The asterisk (*) indicates the path prefix.</i>
category	String	Masked field. <ul style="list-style-type: none"> ● Params: The params field in requests ● Cookie: Web visitors distinguished by cookie ● Header: Custom HTTP header ● Form: Forms Enumeration values: <ul style="list-style-type: none"> ● params ● cookie ● header ● form
index	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs.
description	String	(Optional) A description of the rule.

Status code: 400

Table 4-386 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-387 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-388 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a data masking rule. The project ID is specified by `project_id` and the policy ID is specified by `policy_id`. The rule ID is specified by `rule_id`. The url of the rule is `/demo`, the masking field is `cookie`, the masking field name is `demo1`, and the rule description is `demo`.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}?enterprise_project_id=0
{
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo1",
  "description" : "demo"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "97e4d35f375f4736a21cccfad77613eb",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "description" : "demo",
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo1"
}
```

Status Codes

Status Code	Description
200	Request succeeded.

Status Code	Description
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.32 Deleting a Data Masking Rule

Function

This API is used to delete a data masking rule.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}

Table 4-389 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of the data masking rule. You can obtain the rule ID by calling the ListPrivacyRule API which is used for querying the data masking rule list.

Table 4-390 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-391 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-392 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
timestamp	Long	Time the rule was created. The value is a 13-digit timestamp in ms.
description	String	(Optional) A description of the rule.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> 0: The rule is disabled. 1: The rule is enabled.
url	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/. <i>The asterisk () indicates the path prefix.</i>

Parameter	Type	Description
category	String	Masked field. <ul style="list-style-type: none"> • Params: The params field in requests • Cookie: Web visitors distinguished by cookie • Header: Custom HTTP header • Form: Forms
index	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs.

Status code: 400

Table 4-393 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-394 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-395 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a data masking rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "97e4d35f375f4736a21cccfad77613eb",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "timestamp" : 1650533191385,
  "description" : "demo",
  "status" : 1,
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo1"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.33 Querying the List of Known Attack Source Rules

Function

This API is used to query the list of known attack source rules.

URI

```
GET /v1/{project_id}/waf/policy/{policy_id}/punishment
```

Table 4-396 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the known attack source rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.

Table 4-397 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
offset	Yes	Integer	Offset. The records after the offset are queried.
limit	Yes	Integer	Maximum number of records that can be returned.

Request Parameters

Table 4-398 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-399 Response body parameters

Parameter	Type	Description
total	Integer	The number of known attack source rules.
items	Array of PunishmentInfo objects	The list of known attack source rules.

Table 4-400 PunishmentInfo

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
block_time	Integer	Block duration.
category	String	Type of the known attack source rule.
description	String	Rule description.
timestamp	Long	Timestamp the rule is created.

Status code: 400

Table 4-401 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-402 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-403 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the known attack source rule list. The project ID is specified by project_id and the policy ID is specified by policy_id.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/punishment?offset=0&limit=2
```

Example Responses

Status code: 200

Request sent.

```
{
  "items" : [ {
    "block_time" : 305,
    "category" : "long_ip_block",
    "description" : "test",
    "id" : "2c3afdcc982b429da4f72ee483aece3e",
    "policyid" : "2fcbcb23ef0d48d99d24d7dcff00307d",
    "timestamp" : 1668148186106
  } ],
  "total" : 1
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.34 Creating a Known Attack Source Rule

Function

This API is used to create a known attack source rule.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/punishment

Table 4-404 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. In the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-405 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-406 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-407 Request body parameters

Parameter	Mandatory	Type	Description
category	Yes	String	Type of the known attack source rule. Enumeration values: <ul style="list-style-type: none"> • long_ip_block • long_cookie_block • long_params_block • short_ip_block • short_cookie_block • short_params_block
block_time	Yes	Integer	Block duration. If prefix long is selected for the rule type, the value for block_time ranges from 301 to 1800 . If prefix short is selected for the rule type, the value for block_time ranges from 0 to 300 .
description	No	String	Rule description.

Response Parameters

Status code: 200

Table 4-408 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
block_time	Integer	Block duration.
category	String	Type of the known attack source rule.
description	String	Rule description.
timestamp	Long	Timestamp the rule is created.

Status code: 400

Table 4-409 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-410 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-411 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a known attack source rule in a policy. The project ID is specified by `project_id` and the policy ID is specified by `policy_id`. The rule type is `long_ip_block`, the block duration is 1233 seconds, and the rule description is `demo`.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/punishment?
{
  "category": "long_ip_block",
  "block_time": "1233",
  "description": "demo"
}
```

Example Responses

Status code: 200

Request sent.

```
{
  "block_time": 1233,
  "category": "long_ip_block",
  "description": "demo",
```

```

{id" : "2c3afdcc982b429da4f72ee483aece3e",
"policyid" : "2fcbcb23ef0d48d99d24d7dcff00307d",
"timestamp" : 1668148186106
}

```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.35 Querying a Known Attack Source Rule by ID

Function

This API is used to query a known attack source rule by ID.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}

Table 4-412 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of a known attack source rule. You can obtain it by calling the ListPunishmentRules API.

Table 4-413 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-414 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-415 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
block_time	Integer	Block duration.
category	String	Type of the known attack source rule.
description	String	Rule description.
timestamp	Long	Timestamp the rule is created.

Status code: 400

Table 4-416 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-417 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-418 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a known attack source rule. Details about the query are specified by `project_id`, `policy_id`, and `rule_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}?
```

Example Responses

Status code: 200

Request sent.

```
{
  "block_time" : 1233,
  "category" : "long_ip_block",
  "description" : "demo",
  "id" : "2c3afdcc982b429da4f72ee483aece3e",
  "policyid" : "2fcbcb23ef0d48d99d24d7dcff00307d",
  "timestamp" : 1668148186106
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.36 Updating a Known Attack Source Rule

Function

This API is used to update a known attack source rule.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}

Table 4-419 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of a known attack source rule. You can obtain it by calling the ListPunishmentRules API.

Table 4-420 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-421 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-422 Request body parameters

Parameter	Mandatory	Type	Description
category	Yes	String	Type of the known attack source rule. Enumeration values: <ul style="list-style-type: none"> • long_ip_block • long_cookie_block • long_params_block • short_ip_block • short_cookie_block • short_params_block
block_time	Yes	Integer	Block duration. If prefix long is selected for the rule type, the value for block_time ranges from 301 to 1800 . If prefix short is selected for the rule type, the value for block_time ranges from 0 to 300 .
description	No	String	Rule description.

Response Parameters

Status code: 200

Table 4-423 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
block_time	Integer	Block duration.
category	String	Type of the known attack source rule.
description	String	Rule description.

Status code: 400

Table 4-424 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-425 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-426 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a known attack source rule. The project ID is specified by `project_id` and the policy ID is specified by `policy_id`. The rule ID is specified by `rule_id`. The rule type is `long_ip_block`, the block duration is 1233 seconds, and the rule description is update.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}?
{
  "category": "long_ip_block",
  "block_time": "1233",
  "description": "update"
}
```

Example Responses

Status code: 200

Request sent.

```
{
  "block_time": 1233,
  "category": "long_ip_block",
  "description": "update",
  "id": "2c3afdcc982b429da4f72ee483aece3e",
  "policyid": "2fcbcb23ef0d48d99d24d7dcff00307d"
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.37 Deleting a Known Attack Source Rule

Function

This API is used to delete a known attack source rule.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}

Table 4-427 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of a known attack source rule. You can obtain it by calling the ListPunishmentRules API.

Table 4-428 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-429 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-430 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
block_time	Integer	Block duration.
category	String	Type of the known attack source rule.
description	String	Rule description.
timestamp	Long	Timestamp the rule is created.

Status code: 400

Table 4-431 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-432 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-433 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a known attack source rule in a policy. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}?
```

Example Responses

Status code: 200

Request sent.

```
{
  "block_time" : 1233,
  "category" : "long_ip_block",
  "description" : "update",
  "id" : "2c3afdcc982b429da4f72ee483aece3e",
  "policyid" : "2fcbcb23ef0d48d99d24d7dcff00307d",
  "timestamp" : 1668148186106
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.38 Querying the List of Geolocation Access Control Rules

Function

This API is used to query the list of geolocation access control rules.

URI

```
GET /v1/{project_id}/waf/policy/{policy_id}/geoip
```

Table 4-434 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-435 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned. Default: 1
pagesize	No	Integer	Number of results on each page during pagination query. Value range: 1 to 100 . The default value is 10 , indicating that each page contains 10 results. Default: 10

Request Parameters

Table 4-436 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-437 Response body parameters

Parameter	Type	Description
total	Integer	Number of geolocation access control rules in the policy
items	Array of GeOIpItem objects	Array of geolocation access control rules

Table 4-438 GeOIpItem

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
name	String	Name of the geolocation access control rule
geoip	String	Locations that can be configured in the geolocation access control rule: (Countries/Regions outside China: CA : Canada, South Africa : South Africa, Mexico : Mexico, Peru : Peru, Indonesia : Indonesia Cities inside China: GD : Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tibet, NM : Inner Mongolia) For details about the location code, see <i>Appendix - Geographical Location Codes</i> .

Parameter	Type	Description
white	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.
status	Integer	Rule status. <ul style="list-style-type: none"> ● true: enabled. ● false: disabled.
timestamp	Long	Time the rule is created.

Status code: 400

Table 4-439 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-440 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-441 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the geolocation access control rule list in a project. The project ID is specified by `project_id`, and the policy is specified by `policy_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/geoip?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "06f07f6c229141b9a4a78614751bb687",
    "policyid" : "2abeecefb9840e6bf05efbd80d0fcd7",
    "timestamp" : 1636340038062,
    "status" : 1,
    "geoip" : "GD",
    "white" : 1,
    "name" : "demo"
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.39 Creating a Geolocation Access Control Rule

Function

This API is used to create a geolocation access control rule.

URI

```
POST /v1/{project_id}/waf/policy/{policy_id}/geoip
```

Table 4-442 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-443 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-444 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-445 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Name of the geolocation access control rule

Parameter	Mandatory	Type	Description
geoip	Yes	String	Locations that can be configured in the geolocation access control rule: (Countries/ Regions outside China: CA : Canada, South Africa : South Africa, Mexico : Mexico, Peru : Peru, Indonesia : Indonesia Cities inside China: GD : Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tibet, NM : Inner Mongolia) For details about the location code, see <i>Appendix - Geographical Location Codes</i> .
white	Yes	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.
status	No	Integer	Rule status. <ul style="list-style-type: none"> ● true: enabled. ● false: disabled.
description	No	String	Rule Description

Response Parameters

Status code: 200

Table 4-446 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the geolocation access control rule
policyid	String	Policy ID
geoip	String	Locations that can be configured in the geolocation access control rule: (Countries/Regions outside China: CA : Canada, South Africa : South Africa, Mexico : Mexico, Peru : Peru, Indonesia : Indonesia Cities inside China: GD : Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tibet, NM : Inner Mongolia) For details about the location code, see <i>Appendix - Geographical Location Codes</i> .
white	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.
status	Integer	Rule status. <ul style="list-style-type: none"> ● true: enabled. ● false: disabled.
timestamp	Long	Time the rule is created.

Status code: 400

Table 4-447 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-448 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-449 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a geolocation access control rule in a policy. The project ID is specified by `project_id`, and the policy ID is specified by `policy_id`. The protective action is set to block, rule description to demo, rule name to demo, and blocked regions to Shanghai and Afghanistan.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/geoip?enterprise_project_id=0
{
  "white" : 0,
  "description" : "demo",
  "name" : "demo",
  "geoip" : "SH|Afghanistan"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "02dafa406c4941368a1037b020f15a53",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650534513775,
  "status" : 1,
  "geoip" : "SH|Afghanistan",
  "white" : 0
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.40 Querying a Geolocation Access Control Rule by ID.

Function

Querying a Geolocation Access Control Rule by ID.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}

Table 4-450 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of the geolocation access control rule. You can obtain the rule ID by calling ListGeoipRule API which is used to query the list of geolocation access control rules. The rule ID is included the id field in the response body.

Table 4-451 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-452 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-453 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.

Parameter	Type	Description
geoip	String	Locations that can be configured in the geolocation access control rule: (Countries/Regions outside China: CA : Canada, South Africa : South Africa, Mexico : Mexico, Peru : Peru, Indonesia : Indonesia Cities inside China: GD : Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tibet, NM : Inner Mongolia) For details about the location code, see <i>Appendix - Geographical Location Codes</i> .
white	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.
status	Integer	Rule status. <ul style="list-style-type: none"> ● true: enabled. ● false: disabled.
timestamp	Long	Time the rule is created.

Status code: 400

Table 4-454 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-455 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-456 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a geolocation access control rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

Request sent.

```
{
  "id": "02dafa406c4941368a1037b020f15a53",
  "policyid": "38ff0cb9a10e4d5293c642bc0350fa6d",
  "status": 1,
  "geoip": "BJ|Afghanistan",
  "white": 0
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.41 Updating a Geolocation Access Control Rule

Function

This API is used to update a geolocation access control rule.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}

Table 4-457 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API (value of the id field in the response body).
rule_id	Yes	String	ID of the geolocation access control rule. You can obtain the rule ID by calling ListGeoipRule API which is used to query the list of geolocation access control rules. The rule ID is included the id field in the response body.

Table 4-458 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-459 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-460 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Name of the geolocation access control rule
description	No	String	Description
geoip	Yes	String	Locations that can be configured in the geolocation access control rule: (Countries/Regions outside China: CA : Canada, South Africa : South Africa, Mexico : Mexico, Peru : Peru, Indonesia : Indonesia Cities inside China: GD : Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tibet, NM : Inner Mongolia) For details about the location code, see <i>Appendix - Geographical Location Codes</i> .

Parameter	Mandatory	Type	Description
white	Yes	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.

Response Parameters

Status code: 200

Table 4-461 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the geolocation access control rule
description	String	description
policyid	String	Policy ID
geoip	String	Locations that can be configured in the geolocation access control rule: (Countries/Regions outside China: CA : Canada, South Africa : South Africa, Mexico : Mexico, Peru : Peru, Indonesia : Indonesia Cities inside China: GD : Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tibet, NM : Inner Mongolia) For details about the location code, see <i>Appendix - Geographical Location Codes</i> .
white	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.

Status code: 400

Table 4-462 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-463 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-464 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a geolocation access control rule in a policy. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`. The protective action is set to block, rule description to demo, rule name to demo, and blocked regions to Beijing and Afghanistan.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}?enterprise_project_id=0
{
  "white" : 0,
  "name" : "demo",
  "geoip" : "BJ|Afghanistan"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "02dafa406c4941368a1037b020f15a53",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "description" : "demo",
  "geoip" : "BJ|Afghanistan",
  "white" : 0
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.42 Deleting a Geolocation Access Control Rule

Function

This API is used to delete a geolocation access control rule.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}

Table 4-465 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Parameter	Mandatory	Type	Description
rule_id	Yes	String	ID of the geolocation access control rule. You can obtain the rule ID by calling ListGeoipRule API which is used to query the list of geolocation access control rules. The rule ID is included the id field in the response body.

Table 4-466 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-467 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-468 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the geolocation access control rule
policyid	String	Policy ID

Parameter	Type	Description
geoip	String	Locations that can be configured in the geolocation access control rule: (Countries/Regions outside China: CA : Canada, South Africa : South Africa, Mexico : Mexico, Peru : Peru, Indonesia : Indonesia Cities inside China: GD : Guangdong, FJ : Fujian, JL : Jilin, LN : Liaoning, TW : Taiwan (China), GZ : Guizhou, AH : Anhui, HL : Heilongjiang, HA : Henan, SC : Sichuan, HE : Hebei, YN : Yunnan, HB : Hubei, HI : Hainan, QH : Qinghai, HN : Hunan, JX : Jiangxi, SX : Shanxi, SN : Shaanxi, ZJ : Zhejiang, GS : Gansu, JS : Jiangsu, SD : Shandong, BJ : Beijing, SH : Shanghai, TJ : Tianjin, CQ : Chongqing, MO : Macao (China), HK : Hong Kong (China), NX : Ningxia, GX : Guangxi, XJ : Xinjiang, XZ : Tibet, NM : Inner Mongolia) For details about the location code, see <i>Appendix - Geographical Location Codes</i> .
white	Integer	Protective action <ul style="list-style-type: none"> ● 0: WAF blocks requests that hit the rule. ● 1: WAF allows requests that hit the rule. ● 2: WAF only record requests that hit the rule.
status	Integer	Rule status. <ul style="list-style-type: none"> ● true: enabled. ● false: disabled.
description	String	Description
timestamp	Long	Time the rule is created.

Status code: 400

Table 4-469 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-470 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-471 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a geolocation access control rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "02dafa406c4941368a1037b020f15a53",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "timestamp" : 1650534513775,
  "status" : 1,
  "geoip" : "BJ|Afghanistan",
  "white" : 0
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.43 Querying the List of Web Tamper Protection Rules

Function

This API is used to query the list of web tamper protection rules.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/antitamper

Table 4-472 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-473 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned.
pagesize	No	Integer	Number of results on each page during pagination query. Value range: 1 to 100 . The default value is 10 , indicating that each page contains 10 results.

Request Parameters

Table 4-474 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-475 Response body parameters

Parameter	Type	Description
total	Integer	Total number of web tamper protection rules
items	Array of AntiTamperRuleResponseBody objects	Number of web tamper protection rules.

Table 4-476 AntiTamperRuleResponseBody

Parameter	Type	Description
id	String	Rule ID
policyid	String	ID of the protection policy that includes the rule
timestamp	Long	Timestamp the rule was created.
description	String	Rule remarks
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> 0: The rule is disabled. 1: The rule is enabled.
hostname	String	Domain name protected by the web tamper protection rule

Parameter	Type	Description
url	String	URL protected by the web tamper protection rule

Status code: 400

Table 4-477 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-478 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-479 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the web tamper protection rule list in a project. The project ID is specified by `project_id`, and the policy is specified by `policy_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "b77c3182957b46ed8f808a1998245cc4",
    "policyid" : "bdba8e224cbd4d11915f244c991d1720",
    "timestamp" : 1647499571037,
    "description" : "",
    "status" : 0,
    "hostname" : "www.demo.com",
    "url" : "/sdf"
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.44 Creating a Web Tamper Protection Rule

Function

This API is used to create a web tamper protection rule.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/antitamper

Table 4-480 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-481 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-482 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-483 Request body parameters

Parameter	Mandatory	Type	Description
hostname	Yes	String	Protected websites. The list can be obtained by calling the ListHost API in cloud mode (the value of the hostname field in the response body).
url	Yes	String	URL protected by the web tamper protection rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/. The <i>asterisk (*)</i> indicates the path prefix.
description	No	String	Rule Description

Response Parameters

Status code: 200

Table 4-484 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
hostname	String	Domain name protected by the web tamper protection rule
url	String	URL protected by the web tamper protection rule
description	String	Timestamp the rule was created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.

Status code: 400

Table 4-485 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-486 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-487 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a web tamper protection rule in a policy. The project ID is specified by `project_id`, and the policy ID is specified by `policy_id`. The website for the rule is `www.demo.com`, the URL of the rule is `/test`, and the rule description is `demo`.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper?enterprise_project_id=0
{
  "hostname": "www.demo.com",
  "url": "/test",
  "description": "demo"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id": "eed1c1e9c1b04b4bad4ba1186387a5d8",
  "policyid": "38ff0cb9a10e4d5293c642bc0350fa6d",
  "description": "demo",
  "status": 1,
  "hostname": "www.demo.com",
  "url": "/test"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.45 Querying a Web Tamper Protection Rule

Function

This API is used to query a web tamper protection rule.

URI

GET `/v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}`

Table 4-488 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of the anti-tamper rule. It can be obtained by calling the ListAntitamperRule API.

Table 4-489 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-490 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-491 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
hostname	String	Domain name protected by the web tamper protection rule
url	String	URL protected by the web tamper protection rule
description	String	Timestamp the rule is created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none">● 0: The rule is disabled.● 1: The rule is enabled.
timestamp	Long	Timestamp the rule is created.

Status code: 400**Table 4-492** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401**Table 4-493** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500**Table 4-494** Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Example Requests

The following example shows how to query a web tamper protection rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

Request sent.

```
{
  "id" : "b77c3182957b46ed8f808a1998245cc4",
  "policyid" : "bdba8e224cbd4d11915f244c991d1720",
  "timestamp" : 1647499571037,
  "description" : "",
  "status" : 0,
  "hostname" : "www.demo.com",
  "url" : "/sdf"
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.46 Deleting a Web Tamper Protection Rule

Function

This API is used to delete a web tamper protection rule.

URI

```
DELETE /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}
```

Table 4-495 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	ID of the anti-tamper rule. It can be obtained by calling the ListAntitamperRule API.

Table 4-496 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-497 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-498 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
url	String	URL protected by the web tamper protection rule
timestamp	Long	Timestamp the rule was created.

Status code: 400

Table 4-499 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-500 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-501 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a web tamper protection rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}?
enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 1,
  "items" : [ {
    "id" : "b77c3182957b46ed8f808a1998245cc4",
    "policyid" : "bdba8e224cbd4d11915f244c991d1720",
    "policyname" : "demo",
    "timestamp" : 1647499571037,
    "description" : "",
    "status" : 0,
    "hostname" : "www.demo.com",
    "url" : "/sdf"
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.47 Updating the Cache for a Web Tamper Protection Rule

Function

This API is used to updating the cache for a web tamper protection Rule.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}/refresh

Table 4-502 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	Rule ID.

Table 4-503 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-504 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-505 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
hostname	String	Domain name protected by the web tamper protection rule
url	String	URL protected by the web tamper protection rule
description	String	Timestamp the rule was created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none">● 0: The rule is disabled.● 1: The rule is enabled.
timestamp	Long	Timestamp the rule was created.

Status code: 400**Table 4-506** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401**Table 4-507** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500**Table 4-508** Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Example Requests

The following example shows how to update cache for a web tamper protection rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}/refresh?
```

Example Responses

Status code: 200

ok

```
{
  "description" : "",
  "hostname" : "www.domain.com",
  "id" : "0f59185b76c143f884d21cd0d88e6fa8",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1666506256928,
  "url" : "/login"
}
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.48 Querying the List of Information Leakage Prevention Rules

Function

This API is used to query the list of information leakage prevention rules.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/antileakage

Table 4-509 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	ID of a protection policy. You can specify a protection policy ID to query the information leakage prevention rules used in the protection policy. You can obtain the policy ID by calling the ListPolicy API.

Table 4-510 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
offset	Yes	Integer	Offset. The records after the offset are queried.
limit	Yes	Integer	Maximum number of records that can be returned.

Request Parameters

Table 4-511 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-512 Response body parameters

Parameter	Type	Description
total	Integer	The number of information leakage prevention rules
items	Array of LeakageListInfo objects	The list of information leakage prevention rules

Table 4-513 LeakageListInfo

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
url	String	URL to which the rule applies.
category	String	Type
contents	Array of strings	Value
timestamp	Long	Timestamp the rule is created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> 0: The rule is disabled. 1: The rule is enabled.
description	String	Rule description.

Status code: 400

Table 4-514 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-515 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-516 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the information leakage protection rule list in a project. The project ID is specified by `project_id`, and the policy is specified by `policy_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antileakage?offset=0&limit=2
```

Example Responses

Status code: 200

Request sent.

```
{
  "total": 1,
  "items": [ {
    "id": "82c4f04f84fd4b2b9ba4b4ea0df8ee82",
    "policyid": "2fcbcb23ef0d48d99d24d7dcff00307d",
    "timestamp": 1668152426471,
    "description": "demo",
    "status": 1,
    "url": "/attack",
    "category": "sensitive",
    "contents": [ "id_card" ]
  } ]
}
```

```
}]  
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.49 Creating an Information Leakage Prevention Rule

Function

This API is used to create an information leakage prevention rule.

URI

POST /v1/{project_id}/waf/policy/{policy_id}/antileakage

Table 4-517 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-518 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-519 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-520 Request body parameters

Parameter	Mandatory	Type	Description
url	Yes	String	URL to which the rule applies.
category	Yes	String	Type. The value can be code for response code or sensitive for sensitive information. Enumeration values: <ul style="list-style-type: none"> • code • sensitive
contents	Yes	Array of strings	Rule content. The value can be HTTP status code: 400, 401, 402, 403, 404, 405, 500, 501, 502, 503, 504, 507; phone for mobile phone numbers, id_card for personal identity card number, and/or email for email addresses.
description	No	String	Rule description.

Response Parameters

Status code: 200

Table 4-521 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
url	String	URL to which the rule applies.
category	String	Type
contents	Array of strings	Content
timestamp	Long	Timestamp the rule is created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.

Status code: 400

Table 4-522 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-523 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-524 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create an information leakage protection rule in a project. The project ID is specified by `project_id`, and the policy is specified by `policy_id`. The URL for the rule is `/attack`, the content type is sensitive information, and the rule content is ID card number.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antileakage?
{
  "url" : "/attack",
  "category" : "sensitive",
  "contents" : [ "id_card" ]
}
```

Example Responses

Status code: 200

Request sent.

```
{
  "id" : "82c4f04f84fd4b2b9ba4b4ea0df8ee82",
  "policyid" : "2fcbcb23ef0d48d99d24d7dcff00307d",
  "timestamp" : 1668152426471,
  "status" : 1,
  "url" : "/attack",
  "category" : "sensitive",
  "contents" : [ "id_card" ]
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.50 Querying an Information Leakage Prevention Rule

Function

This API is used to query an information leakage prevention rule by ID.

URI

GET /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}

Table 4-525 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	Information leakage prevention rule ID. You can obtain it by calling the ListAntileakageRules API.

Table 4-526 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-527 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-528 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
url	String	URL to which the rule applies.
category	String	Type
contents	Array of strings	Content
timestamp	Long	Timestamp the rule is created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The rule is disabled. ● 1: The rule is enabled.
description	String	Rule description.

Status code: 400

Table 4-529 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-530 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-531 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query an information leakage protection rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}?
```

Example Responses

Status code: 200

Request sent.

```
{
  "id" : "82c4f04f84fd4b2b9ba4b4ea0df8ee82",
  "policyid" : "2fcbcb23ef0d48d99d24d7dcff00307d",
  "timestamp" : 1668152426471,
  "description" : "demo",
  "status" : 1,
  "url" : "/attack",
  "category" : "sensitive",
  "contents" : [ "id_card" ]
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.

Status Code	Description
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.51 Updating an Information Leakage Prevention Rule

Function

This API is used to update an information leakage prevention rule.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}

Table 4-532 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	Information leakage prevention rule ID. You can obtain it by calling the ListAntileakageRules API.

Table 4-533 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-534 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-535 Request body parameters

Parameter	Mandatory	Type	Description
url	Yes	String	URL to which the rule applies.
category	Yes	String	Type. The value can be code for response code or sensitive for sensitive information. Enumeration values: <ul style="list-style-type: none"> • code • sensitive
contents	Yes	Array of strings	Content. The value can be an HTTP status code, phone for mobile phone numbers, id_card for personal identity card number, and/or email for email addresses.
description	No	String	Rule description.

Response Parameters

Status code: 200

Table 4-536 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
url	String	URL to which the rule applies.

Parameter	Type	Description
category	String	Type
contents	Array of strings	Value
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The rule is disabled. • 1: The rule is enabled.
description	String	Rule description.

Status code: 400

Table 4-537 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-538 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-539 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a web tamper protection rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the

rule ID is specified by rule_id. The URL for the rule is /attack, the content type is sensitive information, and the rule content is ID card number.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}?  
  
{  
  "url" : "/login",  
  "category" : "sensitive",  
  "contents" : [ "id_card" ]  
}
```

Example Responses

Status code: 200

Request sent.

```
{  
  "id" : "82c4f04f84fd4b2b9ba4b4ea0df8ee82",  
  "policyid" : "2fcbb23ef0d48d99d24d7dcff00307d",  
  "description" : "demo",  
  "status" : 1,  
  "url" : "/login",  
  "category" : "sensitive",  
  "contents" : [ "id_card" ]  
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.52 Deleting an Information Leakage Prevention Rule

Function

This API is used to delete an information leakage prevention rule.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}

Table 4-540 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.
rule_id	Yes	String	Information leakage prevention rule ID. You can obtain it by calling the ListAntileakageRules API.

Table 4-541 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-542 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-543 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
policyid	String	Policy ID.
url	String	URL to which the rule applies.
category	String	Type
contents	Array of strings	Content
timestamp	Long	Timestamp the rule is created.
status	Integer	Rule status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The rule is disabled. • 1: The rule is enabled.
description	String	Rule description.

Status code: 400

Table 4-544 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-545 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-546 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Example Requests

The following example shows how to delete an information leakage protection rule. The project ID is specified by `project_id`, the policy ID is specified by `policy_id`, and the rule ID is specified by `rule_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}?
```

Example Responses

Status code: 200

Request sent.

```
{
  "id" : "82c4f04f84fd4b2b9ba4b4ea0df8ee82",
  "policyid" : "2fcbbcb23ef0d48d99d24d7dcff00307d",
  "timestamp" : 1668152426471,
  "description" : "demo",
  "status" : 1,
  "url" : "/attack",
  "category" : "sensitive",
  "contents" : [ "id_card" ]
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.53 Querying the Reference Table List

Function

This API is used to query the reference table list.

URI

GET /v1/{project_id}/waf/valuelist

Table 4-547 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-548 Query Parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned.
pagesize	No	Integer	Number of results on each page during pagination query. Value range: 1 to 100 . The default value is 10 , indicating that each page contains 10 results.
name	No	String	Reference table name

Request Parameters

Table 4-549 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-550 Response body parameters

Parameter	Type	Description
total	Integer	Number of reference tables
items	Array of ValueListResponseBody objects	Reference table list

Table 4-551 ValueListResponseBody

Parameter	Type	Description
id	String	ID of the reference table
name	String	Reference table name.
type	String	Reference table type Enumeration values: <ul style="list-style-type: none"> • url • params • ip • cookie • referer • user-agent • header • response_code • response_header • response_body
timestamp	Long	Reference table timestamp
values	Array of strings	Value of the reference table
producer	Integer	Reference table source. The value can be 1 or others. 1: The table is created by you. Other values indicate that the table is automatically generated by moduleX.
description	String	Reference table description

Status code: 400

Table 4-552 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-553 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-554 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the reference table list in a project. The project ID is specified by project_id.

```
GET https://{Endpoint}/v1/{project_id}/waf/valuelist?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total": 1,
  "items": [ {
    "id": "3b03be27a40b45d3b21fe28a351e2021",
    "name": "ip_list848",
    "type": "ip",
    "values": [ "100.100.100.125" ],
    "timestamp": 1650421866870,
    "producer": 1,
    "description": "demo"
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.54 Creating a Reference Table

Function

This API is used to add a reference table. A reference table can be used by CC attack protection rules and precise protection rules.

URI

POST /v1/{project_id}/waf/valuelist

Table 4-555 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-556 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-557 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-558 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Reference table name. The value can contain a maximum of 64 characters. Only digits, letters, hyphens (-), underscores (_), and periods (.) are allowed. Minimum: 2 Maximum: 64
type	Yes	String	Reference table type. For details, see the enumeration list. Minimum: 2 Maximum: 32 Enumeration values: <ul style="list-style-type: none"> • url • params • ip • cookie • referer • user-agent • header • response_code • response_header • response_body
values	Yes	Array of strings	Value of the reference table

Parameter	Mandatory	Type	Description
description	No	String	Reference table description. The value contains a maximum of 128 characters. Minimum: 0 Maximum: 128

Response Parameters

Status code: 200

Table 4-559 Response body parameters

Parameter	Type	Description
id	String	ID of the reference table
name	String	Reference table name.
type	String	Reference table type
description	String	Reference table description
timestamp	Long	Reference table timestamp
values	Array of strings	Value of the reference table
producer	Integer	Source of the reference table. <ul style="list-style-type: none"> 1: The reference table was created by you. 2: The reference table was created by the intelligent access control protection.

Status code: 400

Table 4-560 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-561 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-562 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a reference table in the project. The project ID is specified by `project_id`. The reference table name is `demo`, the reference table type is `url`, the value is `/124`, and the description is `demo`.

```
POST https://{Endpoint}/v1/{project_id}/waf/valuelist?enterprise_project_id=0
{
  "name" : "demo",
  "type" : "url",
  "values" : [ "/124" ],
  "description" : "demo"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "e5d9032d8da64d169269175c3e4c2849",
  "name" : "demo",
  "type" : "url",
  "values" : [ "/124" ],
  "timestamp" : 1650524684892,
  "description" : "demo",
  "producer" : 1
}
```

Status Codes

Status Code	Description
200	Request succeeded.

Status Code	Description
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.55 Querying a Reference Table

Function

This API is used to query a reference table.

URI

GET /v1/{project_id}/waf/valuelist/{valuelistid}

Table 4-563 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
valuelistid	Yes	String	Reference table ID. It can be obtained by calling the ListValueList API.

Table 4-564 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-565 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-566 Response body parameters

Parameter	Type	Description
id	String	ID of the reference table
name	String	Reference table name.
type	String	Reference table type
description	String	Reference table description
values	Array of strings	Value of the reference table
producer	Integer	Source of the reference table. <ul style="list-style-type: none"> • 1: The reference table was created by you. • 2: The reference table was created by the intelligent access control protection.
timestamp	Long	Timestamp the rule is created.

Status code: 400

Table 4-567 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-568 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-569 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a reference table in a project. The project ID is specified by project_id. The reference table ID is valuelistid.

```
GET https://{Endpoint}/v1/{project_id}/waf/valuelist/{valuelistid}?enterprise_project_id=0
```

Example Responses

Status code: 200

Request sent.

```
{
  "id": "63b1d9edf2594743bc7c6ee98527306c",
  "name": "Rpmvp0m4",
  "type": "response_code",
  "values": [ "500" ],
  "description": "demo",
  "producer": 1
}
```

Status Codes

Status Code	Description
200	Request sent.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.56 Modifying a Reference Table

Function

This API is used to modify a reference table.

URI

PUT /v1/{project_id}/waf/valuelist/{valuelistid}

Table 4-570 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
valuelistid	Yes	String	Reference table ID. It can be obtained by calling the ListValueList API.

Table 4-571 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-572 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-573 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Reference table name, which is a string of 2 to 32 characters. Minimum: 2 Maximum: 32
type	Yes	String	Reference table type. For details, see the enumeration list. Minimum: 2 Maximum: 32 Enumeration values: <ul style="list-style-type: none"> • url • params • ip • cookie • referer • user-agent • header • response_code • response_header • resopnse_body
values	No	Array of strings	Value of the reference table

Parameter	Mandatory	Type	Description
description	No	String	Reference table description. The value contains a maximum of 128 characters. Minimum: 0 Maximum: 128

Response Parameters

Status code: 200

Table 4-574 Response body parameters

Parameter	Type	Description
id	String	ID of the reference table
name	String	Reference table name.
type	String	Reference table type
description	String	Reference table description
values	Array of strings	Value of the reference table
producer	Integer	Source of the reference table. <ul style="list-style-type: none"> 1: The reference table was created by you. 2: The reference table was created by the intelligent access control protection.

Status code: 400

Table 4-575 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-576 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-577 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a reference table whose ID is `valuelistid` in the project. The project ID is specified by `project_id`. The reference table name is `RPmvp0m4`, the reference table type is `response_coderl`, the value is 500, and the description is `demo`.

```
PUT https://{Endpoint}/v1/{project_id}/waf/valuelist/{valuelistid}?enterprise_project_id=0
{
  "name": "RPmvp0m4",
  "type": "response_code",
  "values": [ "500" ],
  "description": "demo"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id": "63b1d9edf2594743bc7c6ee98527306c",
  "name": "RPmvp0m4",
  "type": "response_code",
  "values": [ "500" ],
  "description": "demo",
  "producer": 1
}
```

Status Codes

Status Code	Description
200	Request succeeded.

Status Code	Description
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.57 Deleting a Reference Table

Function

This API is used to delete a reference table.

URI

DELETE /v1/{project_id}/waf/valuelist/{valuelistid}

Table 4-578 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
valuelistid	Yes	String	Reference table ID. It can be obtained by calling the ListValueList API.

Table 4-579 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-580 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-581 Response body parameters

Parameter	Type	Description
id	String	ID of a reference table
name	String	Reference table name.
type	String	Reference table type
timestamp	Long	Time the reference table is deleted. The value is a 13-digit timestamp in millisecond.

Status code: 400

Table 4-582 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-583 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-584 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a reference table in a project. The project ID is specified by `project_id`. The reference table ID is `valuelistid`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/valuelist/{valuelistid}?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "63b1d9edf2594743bc7c6ee98527306c",
  "name" : "Rpmvp0m4",
  "type" : "response_code",
  "timestamp" : 1640938602391
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.3 Address Group Management

4.3.1 Querying IP Address Groups

Function

Querying IP Address Groups

URI

GET /v1/{project_id}/waf/ip-groups

Table 4-585 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-586 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number. The default value is 1. Default: 1
pagesize	No	Integer	Number of records on each page. A maximum of 100 records can be displayed on a page. The default value is 10. Default: 10
name	No	String	Name of the IP address group. Fuzzy search is supported.

Parameter	Mandatory	Type	Description
ip	No	String	IP addresses or IP address ranges. If this parameter is specified, the address group that contains the specified IP address or IP address ranges are queried.

Request Parameters

Table 4-587 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-588 Response body parameters

Parameter	Type	Description
total	Integer	Total number of IP address groups in the current enterprise project. Only local address groups are listed.
items	Array of IpGroupBody objects	Details about IP address groups
cloudTotal	Integer	Total number of IP address groups, including local and shared address groups.

Table 4-589 IpGroupBody

Parameter	Type	Description
id	String	ID of the IP address group

Parameter	Type	Description
name	String	IP address group name
ips	String	Address group IP addresses (IP addresses or IP address ranges are separated by commas (,)).
size	Integer	Length of the IP address group
rules	Array of RuleInfo objects	List of rules that use the IP address group
share_info	ShareInfo object	Sharing information
description	String	Address group description

Table 4-590 RuleInfo

Parameter	Type	Description
rule_id	String	Rule ID
rule_name	String	Rule name
policy_id	String	Policy ID
policy_name	String	Policy Name

Table 4-591 ShareInfo

Parameter	Type	Description
share_count	Integer	Total number of the users who share the address group.
accept_count	Integer	Number of users who accept the sharing
process_status	Integer	Status

Status code: 400**Table 4-592** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-593 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-594 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the address group list in a project. The project ID is specified by `project_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/ip-groups?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total": 1,
  "items": [ {
    "description": "",
    "id": "c36e896b18ee486a8102fce8e69fb1a",
    "ips": "xxx.xx.xx.xx",
    "name": "sfddf",
    "rules": [ ],
    "share_info": {
      "accept_count": 0,
      "process_status": 0,
      "share_count": 0
    }
  }
  ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.

Status Code	Description
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.3.2 Creating an IP Address Group

Function

This API is used to create an IP address group.

URI

POST /v1/{project_id}/waf/ip-groups

Table 4-595 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-596 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID.

Request Parameters

Table 4-597 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-598 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Address group name
ips	Yes	String	IP addresses or IP address ranges are separated by commas (,).
description	No	String	Address group description

Response Parameters

Status code: 200

Table 4-599 Response body parameters

Parameter	Type	Description
id	String	ID of the IP address group
name	String	IP address group name
ips	String	Address group IP addresses (IP addresses or IP address ranges are separated by commas (,)).
size	Integer	Length of the IP address group
rules	Array of RuleInfo objects	List of rules that use the IP address group
description	String	Address group description
timestamp	Long	Timestamp

Table 4-600 RuleInfo

Parameter	Type	Description
rule_id	String	Rule ID
rule_name	String	Rule name

Parameter	Type	Description
policy_id	String	Policy ID
policy_name	String	Policy Name

Status code: 400

Table 4-601 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-602 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-603 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create an address group in a project. The project ID is specified by project_id. IP address group name: group3. IP address: xx.xx.xx.xx. Address group description: demo.

```
POST https://{Endpoint}/v1/{project_id}/waf/ip-groups?enterprise_project_id=0
{
  "name" : "group3",
  "ips" : "xx.xx.xx.xx",
  "description" : "demo"
}
```


Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "c36e896b18ee486a81026fce8e69fb1a",
  "ips" : "xx.xx.xx.xx",
  "name" : "group3",
  "rules" : [ ],
  "size" : 1,
  "timestamp" : 1666747418345,
  "description" : "demo"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.3.3 Querying IP Addresses in an Address Group

Function

This API is used to query IP addresses included in an address group.

URI

GET /v1/{project_id}/waf/ip-group/{id}

Table 4-604 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
id	Yes	String	ID of the IP address group.

Table 4-605 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-606 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-607 Response body parameters

Parameter	Type	Description
id	String	ID of the IP address group

Parameter	Type	Description
name	String	IP address group name
ips	String	Address group IP addresses (IP addresses or IP address ranges are separated by commas (,)).
size	Integer	Length of the IP address group
rules	Array of RuleInfo objects	List of rules that use the IP address group
share_info	ShareInfo object	Sharing information
description	String	Address group description

Table 4-608 RuleInfo

Parameter	Type	Description
rule_id	String	Rule ID
rule_name	String	Rule name
policy_id	String	Policy ID
policy_name	String	Policy Name

Table 4-609 ShareInfo

Parameter	Type	Description
share_count	Integer	Total number of the users who share the address group.
accept_count	Integer	Number of users who accept the sharing
process_status	Integer	Status

Status code: 400

Table 4-610 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-611 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-612 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query an address group in a project. The project ID is specified by project_id. The address group ID is id.

GET https://{Endpoint}/v1/{project_id}/waf/ip-group/{id}?enterprise_project_id=0

Example Responses

Status code: 200

Request succeeded.

```
{
  "description" : "",
  "id" : "c36e896b18ee486a81026fce8e69fb1a",
  "ips" : "xx.xx.xx.xx",
  "name" : "sfddf",
  "rules" : [ ],
  "size" : 1
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.3.4 Modifying an IP Address Group

Function

This API is used to modify an IP address group.

URI

PUT /v1/{project_id}/waf/ip-group/{id}

Table 4-613 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
id	Yes	String	ID of the IP address group.

Table 4-614 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-615 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-616 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Group Name
ips	Yes	String	IP addresses or IP address ranges are separated by commas (,).
description	No	String	Address group description

Response Parameters

Status code: 200

Table 4-617 Response body parameters

Parameter	Type	Description
id	String	ID of the IP address group
name	String	IP address group name
ips	String	Address group IP addresses (IP addresses or IP address ranges are separated by commas (,)).
size	Integer	Length of the IP address group
rules	Array of RuleInfo objects	List of rules that use the IP address group
description	String	Address group description

Table 4-618 RuleInfo

Parameter	Type	Description
rule_id	String	Rule ID
rule_name	String	Rule name
policy_id	String	Policy ID

Parameter	Type	Description
policy_name	String	Policy Name

Status code: 400

Table 4-619 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-620 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-621 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update an address group in a project. The project ID is specified by project_id. The address group ID is ip. IP address group name: demo. IP address: xx.xx.xx.xx. The address group description is empty.

```
PUT https://{Endpoint}/v1/{project_id}/waf/ip-group/{id}?enterprise_project_id=0
{
  "ips": "xx.xx.xx.xx",
  "name": "demo",
  "description": ""
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "description": "",
  "id": "c36e896b18ee486a81026fce8e69fb1a",
  "ips": "xx.xx.xx.xx",
  "name": "demo",
  "size": 1,
  "rules": [ ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.3.5 Deleting an IP Address Group

Function

This API is used to delete an IP address group.

URI

DELETE /v1/{project_id}/waf/ip-group/{id}

Table 4-622 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the IP address group.

Table 4-623 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-624 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-625 Response body parameters

Parameter	Type	Description
id	String	ID of the IP address group
name	String	IP address group name
ips	String	Address group IP addresses (IP addresses or IP address ranges are separated by commas (,)).
size	Integer	Length of the IP address group
rules	Array of RuleInfo objects	List of rules that use the IP address group

Table 4-626 RuleInfo

Parameter	Type	Description
rule_id	String	Rule ID
rule_name	String	Rule name
policy_id	String	Policy ID
policy_name	String	Policy Name

Status code: 400

Table 4-627 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-628 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-629 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete an address group in a project. The project ID is specified by project_id. The address group ID is id.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/ip-group/{id}?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "description" : "",
  "id" : "c36e896b18ee486a81026fce8e69fb1a",
  "ips" : "xx.xx.xx.xx",
  "name" : "demo",
  "size" : 1,
  "rules" : [ ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request Failed
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.4 Certificate Management

4.4.1 Querying the List of Certificates

Function

This API is used to query the list of certificates.

URI

GET /v1/{project_id}/waf/certificate

Table 4-630 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-631 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned. Default: 1
pagesize	No	Integer	Number of results on each page during pagination query. Value range: 1 to 100 . The default value is 10 , indicating that each page contains 10 results. Default: 10
name	No	String	Certificate name
host	No	Boolean	Whether to obtain the domain name for which the certificate is used. The default value is false . <ul style="list-style-type: none"> • true: Obtain the certificates that have been used for domain names. • false: Obtain the certificates that have not been used for any domain name. Default: false

Parameter	Mandatory	Type	Description
exp_status	No	Integer	Certificate status. The options are as follows: 0: not expired; 1: expired; 2: about to expire (The certificate will expire within one month.)

Request Parameters

Table 4-632 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-633 Response body parameters

Parameter	Type	Description
items	Array of CertificateBody objects	Certificates
total	Integer	Total number of certificates

Table 4-634 CertificateBody

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name
expire_time	Long	Certificate expiration timestamp.

Parameter	Type	Description
exp_status	Integer	Certificate status. The value can be: 0 : The certificate is valid. 1 : The certificate has expired. 2 : The certificate will expire within one month.
timestamp	Long	Certificate upload timestamp.
bind_host	Array of BindHost objects	Domain name associated with the certificate

Table 4-635 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-636 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-637 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-638 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the certificate list in a project. The project ID is specified by `project_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/certificate?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "items": [ {
    "id": "dc443ca4f29c4f7e8d4adaf485be317b",
    "name": "demo",
    "timestamp": 1643181401751,
    "expire_time": 1650794100000,
    "bind_host": [ ],
    "exp_status": 2
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.4.2 Uploading a Certificate

Function

This API is used to upload a certificate.

URI

POST /v1/{project_id}/waf/certificate

Table 4-639 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-640 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-641 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-642 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Certificate name. The value can contain a maximum of 64 characters. Only digits, letters, hyphens (-), underscores (_), and periods (.) are allowed.
content	Yes	String	Certificate file. Only certificates and private key files in PEM format are supported, and the newline characters in the file must be replaced with \n.
key	Yes	String	Certificate private key. Only certificates and private key files in PEM format are supported, and the newline characters in the files must be replaced with \n.

Response Parameters

Status code: 200

Table 4-643 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
content	String	Certificate file, PEM encoding
key	String	Private key of the certificate, which is in PEM format.
expire_time	Long	Certificate expiration timestamp
exp_status	Integer	Certificate status. The options can be: 0 : The certificate has not expired. 1 : The certificate expired. 2 : The certificate is about to expire.
timestamp	Long	Certificate upload timestamp
bind_host	Array of BindHost objects	Domain name associated with the certificate

Table 4-644 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-645 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-646 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-647 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a certificate in the project whose project ID is `project_id`. The certificate name is `demo`, the certificate content is -----BEGIN CERTIFICATE-----..., and the certificate key is -----BEGIN Private KEY-----.....

```
POST https://{Endpoint}/v1/{project_id}/waf/certificate?enterprise_project_id=0
{
  "name" : "demo",
  "content" : "-----BEGIN CERTIFICATE----- \
\nMIIIDyzCCArOgAwIBAgIJAN5U0Z4Bh5ccMA0GCSqGSIb3DQEBCwUAMHwxCzAJBgNV
BAYTAlpMRiWEAYDVQQLDAIHVUFOR0RPTkcETAPBgNVBACmCERPTkdHVUFOMQ0w
CwYDVQQKDARERUUFMqswCQYDVQQLDAJESzELMAKGA1UEAwwCT0QxHTAbBgkqhkiG
9w0BCQEWdK8lZC5odWF3ZWkuY29tMB4XDTEwMTEwMTEwMTEwMTEwMTEwMTEwMTEw
MTk0M0VowfDELMAGKGA1UEBhMCWkgxYjEwMTEwMTEwMTEwMTEwMTEwMTEwMTEw
BwY*****VQQD
DAJPRDEdMBsGCSqGSIb3DQEJARYOTwhkLmh1YXdlas5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDcoLfk62//r0RHFyweYBj9754NsJ8Qj0RG+Y02
OgwhQmRiNNjubJwP8NqqyD86zr+fsSQxKBAcCosn1PcN2Pj2vPD6NEk4I6VdOWr /
kFYMlOcmhSfW4wt6VakniOKIYGrCxxvQe1X2OyBxT+ocTLRgEIB8ZbvJyPNseg
feLE*****SusXo FQ/WRbBRH7DrQmxGiXsq4VELER9Nnc/Kyww+9pYi8L
+mKeRL+lCMMbXC/3k6OfMB tVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9sE
+tmJZTPH6lYtAgMBAAGjUDBOMB0G A1UdDgQWBBQprUUFxw
+gIkpzXdrYlsWjSahWjAfBgNVHSMEGDAWgBQprUUFxw+g lkpzXdrYlsWjSahWjAMBgNVHRMEBTADAQH/
MA0GCSqGSIb3DQEBCwUAA4IBAQA2 603K*****iOhU o/
kVwkiUlCw4t7RwP0hVms0OZw59MuqKd3oCSWkYO4vEHs3t40JDWnGDnmQ4sol
RkOWJwL4w8tnPe3qY9JSupjlsu6Y1hlvKtEfn2vEKFnsuMhidkUpUAJWodHhWBQH
wglDo4/6yTnWZNGK8JDal86Dm5lchXea1EoYBjsHxiJb7HeWQlkre+Mcyi1RH0in 4miXTr0oT4/jWlglkSz6/
ZhGRq+7W7tl7cvzCe+4XsVZlenAcYoNd/WLfo91PD4 yAsRxoJw1so1Bj0BkdZ\n -----END CERTIFICATE-----",
  "key" : "-----BEGIN PRIVATE KEY----- \
\nMIIEEwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDcoLfk62//r0RH FyweYBj9754NsJ8Qj0RG
+Y02OgwhQmRiNNjubJwP8NqqyD86zr+fsSQxKBAcCosn 1PcN2Pj2vPD6NEk4I6VdOWr/
kFYMlOcmhSfW4wt6VakniOKIYGrCxxvQe1X2Oy BxT
+ocTLRgEIB8ZbvJyPNsegfeLEUuPYRpQ5kXlgJH2/3NwZFogBHvV/b07l4fR+ sWJMniA2yIjSBQ0DEAOSusXoFQ/
WRbBRH7DrQmxGiXsq4VELER9Nnc/Kyww+9pYi 8L+mKeRL+lCMMbXC/
3k6OfMBtVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9sE+tmJ ZTPH6lYtAgMBAEcgEBAL+xZxm/QoqXT
+2stoqV2GEyAMFASpRqxlOzjMmEE/9 jZa+cBWIjHhVpsjRqYfBDcHEebu0JwlrjclAvgnlVn05XgXm1A9Q
+WbsocmX1 xCypHgc+MDVn+uWdCd4KW5kEk4EnSsFN5iNSf+1VxNURN+gwsSp/0E+muwA5IISO
G6*****lcGO1n 4urPBHuNly04GgGw
+vkaqjOvZrNLVOMMaFWBxsDWBhgSSBQTj+f3NCxneGYtt8 3SCTZQI5nlkb+r/
M455EwKTSXuEsNHolwx7L6GEPbQECgYEA8lxgK2fYyKloIcOh
TFJaRAVvyjKa2+Aza4qT9SGY9Y30VPCIPjBB1vUu5M9KrFufzlv06nGecHmpEwOe
8vbRu7nLAQTGYFi8VK63q8w6FIFdAyCG6Sx+BWCfWxJzXsZLAJTFklwi8HsOSlqh
6QN*****fvx mTbLg52Z21OyocNq3Tf/
b1Zwolc1ik6cyBzY6z1blrbSzArCqm0sb2iD+kjL8100 /qqdXjBxZukKiVAMNnp7xjGZHHFKWUxT2+UX/
tlyx4T4dzrFlkdDXcMmqfsRxd 1NEVaAaT8SECgYAOu7BPtplun43YTpUfr3pSIN6oZeKoxSbw9i4MNC
+4fSDRPC+ 80ImcmZRL7taF+Y7p0jxAOTulkdJC8NbAiv5J9WzrwQ+5MF2BPB/2bYnRa6tNofH
kZD*****QC9 ihZTj/bTHtRiHZppzCvyYm/lgd
+Uwtsy0uXR1n0G1SQENgrTBD/J6AzdfJae6tE P0U8YIM5Oqxf2i/as9ay+IPRecMI4eSxz7JWAGx6Yx/3AZ
+hAB1ZbNbnqniCLYNk d0MvjwmA25ATO+ro4OZ7AdEpqbk3l9aG/WFyYBz9AQKBgQCucFPA115esL8196V
WMr2Qo0tqzL7CGSoWQk2Sa2HZtZdfofXAaaqo+zvJ6RPHUh0jgJtx536DvV3egI
37YrdQyJbCPZXQ3SPgqWCORUnXBWq/nxS06uwu6JBxUfC57ijmMU4fWYNrvkkmWb 7keAg/
r5Uy1joMAvBN1I6lB8pg==\n -----END PRIVATE KEY-----"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "64af92e2087d49cbabc233e9bdc761b7",
  "name" : "testly",
  "timestamp" : 1658994431596,
}
```

```
"expire_time" : 1682394560000
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.4.3 Querying a Certificate

Function

This API is used to query a certificate.

URI

GET /v1/{project_id}/waf/certificate/{certificate_id}

Table 4-648 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
certificate_id	Yes	String	HTTPS certificate ID. It can be obtained by calling the ListCertificates API.

Table 4-649 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-650 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-651 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
content	String	Certificate file, PEM encoding
key	String	Private key of the certificate, which is in PEM format.
expire_time	Long	Certificate expiration timestamp.
exp_status	Integer	Certificate status. The options can be: 0 : The certificate has not expired. 1 : The certificate expired. 2 : The certificate is about to expire.
timestamp	Long	Certificate upload timestamp
bind_host	Array of BindHost objects	Domain name associated with the certificate

Table 4-652 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-653 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-654 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-655 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a certificate in a project. The project ID is specified by `project_id`, and the certificate ID is specified by `certificate_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "id": "6e2be127b79f4a418414952ad5d8c59f",
  "name": "certificatename94319",
  "content": "-----BEGIN CERTIFICATE-----\nMIIB
+TCCAaOgAwIBAgIUJP9I8OupQ77w0bGL2yWOOQXreM4kwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMC
QVUxEzARBgNVBAGMClNvbWUtU3RhdGUxLzANBgNVBAoMBkx1YXdlTEcMBoGA1UEAwwTd2FmLmh1YXdl
aW*****MRMwEQYDVQQLIDApTb21lLVN0YXRIMQ8wDQYDVQQKDAZlWF3ZWkxH
DAaBgNVBAMME3dhZi5odWF3ZljbG91ZC5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIaEA0UEBmZbvgOJ
TKrKcDUw9xjFqxM7BaQFM3SLsQlmd5hkzygyL1ra
+cWajPJlTCxz9Ph6qldna2+Orl*****wYDV
R0jBBgwFoAUE7ZQNcgI3lmryx1s5gy9mnC1rsYwDwYDVR0TAQH/BAUwAwEB/
zANBgkqhkiG9w0BAQsFAANBAM5wGi88jYwLgOnGbae5hH3I9lMBKxGqv17Cbm1tjWuUogVINz86lqvCpuhZL
D/vzJAqPluDwgM8uvzjgRfZs8=\n-----END CERTIFICATE-----",
  "key": "-----BEGIN RSA PRIVATE KEY-----
\nMIIBOQIBAAJBANFBGzM274DiUyqynA1MPcYxasTOwWkBTN0i7EJZg+YZM8oMi9a2vnFmozyZUwsc/
T4eqpXZ2tvjqyLk3bwnKY8CAwEAAQJBAI7LMPaH/HQk/b/bVmY0qsr
+me9nb9BqFLuqzKbx0hSmWPOWf3rOFISopyHqgYtAsPfvPumEdGbdnCyU8zAECIQD71768K1ejb
+ei2lqZqHaczqUNQxMh54yot9F2yVWjwIhANS1Y1Jv89WEU/ZvMS9a4638Msv2c4GGp08RtXNyn0BAiA0H4b
+cwoEbZjHf+HYg6Fo+uxu5TvSaw8287a6Qo0LyQlFVZSIYwPlT6oiX5rdLzBiap4N0gJWdsa2ihmV59LAQlgK8N
+j1daq63b0bJ9k4HruhQtgxl6U9nFBemH4zTRYM=\n-----END RSA PRIVATE KEY-----",
  "timestamp": 1650595334578,
  "expire_time": 1596865564000,
  "bind_host": [ {
    "id": "978b411657624c2db069cd5484195d1c",
    "hostname": "www.demo.com",
    "waf_type": "cloud"
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.4.4 Modifying a Certificate

Function

This API is used to modify a certificate.

URI

PUT /v1/{project_id}/waf/certificate/{certificate_id}

Table 4-656 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
certificate_id	Yes	String	HTTPS certificate ID. It can be obtained by calling the ListCertificates API.

Table 4-657 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-658 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-659 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Certificate name. The value can contain a maximum of 64 characters. Only digits, letters, hyphens (-), underscores (_), and periods (.) are allowed.
content	No	String	Certificate file. Only certificates and private key files in PEM format are supported, and the newline characters in the file must be replaced with \n.
key	No	String	Certificate private key. Only certificates and private key files in PEM format are supported, and the newline characters in the files must be replaced with \n.

Response Parameters

Status code: 200

Table 4-660 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
expire_time	Long	Timestamp when the certificate expires
timestamp	Long	Timestamp.

Status code: 400

Table 4-661 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-662 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-663 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a certificate name in a project. The project ID is specified by `project_id`, and the certificate ID is specified by `certificate_id`. The certificate name is updated to `demo`.

```
PUT https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?enterprise_project_id=0
{
  "name" : "demo"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "360f992501a64de0a65c50a64d1ca7b3",
  "name" : "demo",
  "timestamp" : 1650593797892,
  "expire_time" : 1596865564000
}
```

Status Codes

Status Code	Description
200	OK

Status Code	Description
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.4.5 Deleting a Certificate

Function

This API is used to delete a certificate.

URI

DELETE /v1/{project_id}/waf/certificate/{certificate_id}

Table 4-664 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
certificate_id	Yes	String	HTTPS certificate ID. It can be obtained by calling the ListCertificates API.

Table 4-665 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-666 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-667 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
content	String	Certificate file, PEM encoding
key	String	Private key of the certificate in PEM format
expire_time	Long	Certificate expiration timestamp
exp_status	Integer	Certificate status. The options can be: 0 : The certificate has not expired. 1 : The certificate expired. 2 : The certificate is about to expire.
timestamp	Long	Certificate upload timestamp
bind_host	Array of BindHost objects	Domain name associated with the certificate

Table 4-668 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name

Parameter	Type	Description
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-669 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-670 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-671 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a certificate in a project. The project ID is specified by `project_id`, and the certificate ID is specified by `certificate_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "id" : "e1d87ba2d88d4ee4a3b0c829e935e5e0",
  "name" : "certificatename29556",
  "timestamp" : 1650594410630,
  "expire_time" : 1596865564000
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.4.6 Applying a Certificate to a Domain Name

Function

This API is used to apply a certificate to a domain name.

URI

POST /v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts

Table 4-672 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	HTTPS certificate ID. It can be obtained by calling the ListCertificates API.

Table 4-673 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-674 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-675 Request body parameters

Parameter	Mandatory	Type	Description
cloud_host_ids	No	Array of strings	ID of HTTPS domain name in cloud mode. You can obtain it by calling the ListHost API.
premium_host_ids	No	Array of strings	ID of the HTTPS domain name in dedicated mode. You can obtain it by calling the ListPremiumHost API.

Response Parameters

Status code: 200

Table 4-676 Response body parameters

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name
timestamp	Long	Timestamp.
expire_time	Long	Expiration date
bind_host	Array of CertificateBundlingHostBody objects	Domain name list

Table 4-677 CertificateBundlingHostBody

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF mode (Cloud: cloud; Dedicated: premium) Enumeration values: <ul style="list-style-type: none">• cloud• premium

Status code: 400**Table 4-678** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401**Table 4-679** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-680 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to use a certificate for two domain names in a project. The project ID is specified by `project_id`, and certificate ID is specified by `certificate_id`. The ID of the domain name protected in cloud mode is `85e554189d494c0f97789e93531c9f90`, and the ID of the domain name protected in dedicated mode is `4e9e97c425fc463c8f374b90124e8392`.

```
POST https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts?
enterprise_project_id=0
```

```
{
  "cloud_host_ids" : [ "85e554189d494c0f97789e93531c9f90" ],
  "premium_host_ids" : [ "4e9e97c425fc463c8f374b90124e8392" ]
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "3ac1402300374a63a05be68c641e92c8",
  "name" : "www.abc.com",
  "timestamp" : 1636343349139,
  "expire_time" : 1650794100000,
  "bind_host" : [ {
    "id" : "e350cf556da34adab1f017523d1c05ed",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud"
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.5 Event Management

4.5.1 This API is used to query details about an event of a specified ID

Function

Querying Details About an Event of a Specified ID

URI

GET /v1/{project_id}/waf/event/{eventid}

Table 4-681 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
eventid	Yes	String	Event ID. It can be obtained by calling the ListEvent API.

Table 4-682 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-683 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
X-Language	No	String	Language. The default value is en-us. zh-cn (Chinese)/en-us (English)

Response Parameters

Status code: 200

Table 4-684 Response body parameters

Parameter	Type	Description
total	Integer	Number of attack events
items	Array of ShowEventItems objects	Details about an attack event

Table 4-685 ShowEventItems

Parameter	Type	Description
time	Long	Timestamp when the attack occurs, in milliseconds.
policyid	String	ID of the policy
sip	String	Source IP address
host	String	Domain name
url	String	Attacked URL
attack	String	Attack type
rule	String	ID of the hit rule

Parameter	Type	Description
action	String	Protective action
cookie	String	Cookie of the attack request
headers	Object	Header of the attack request
host_id	String	ID of the attacked domain name
id	String	Event ID
payload	String	Malicious load
payload_location	String	Malicious load location
region	String	Geographical location of the source IP address
process_time	Integer	Processing time
request_line	String	Body of the attack request
response_size	Integer	Response body size (byte)
response_time	Long	Response time (ms)
status	String	Response code
request_body	String	Request body

Status code: 400

Table 4-686 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-687 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-688 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query details about an event in a project. The event ID is specified by event_id, and the project ID is specified by project_id.

```
GET https://{Endpoint}/v1/{project_id}/waf/event/{event_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

ok

```
{
  "total": 1,
  "items": [ {
    "id": "09-0000-0000-0000-12120220421093806-a60a6166",
    "time": 1650505086000,
    "policyid": "173ed802272a4b0798049d7edffeff03",
    "host": "x.x.x.x:xxxxxx-xxx-xxx-xxx-xxxxxxxx",
    "url": "/mobile/DBconfigReader.jsp",
    "attack": "vuln",
    "rule": "091004",
    "payload": " /mobile/dbconfigreader.jsp",
    "payload_location": "uri",
    "sip": "x.x.x.x",
    "action": "block",
    "request_line": "GET /mobile/DBconfigReader.jsp",
    "headers": {
      "ls-id": "c0d957e6-26a8-4f2e-8216-7fc9332a250f",
      "host": "x.x.x.x:81",
      "lb-id": "68d3c435-2607-45e0-a5e2-38980544dd45",
      "accept-encoding": "gzip",
      "user-agent": "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 CSIRTx/2022"
    },
    "cookie": "HWWAFSESID=2a0bf76a111c93926d; HWWAFSESTIME=1650505086260",
    "status": "418",
    "region": "Reserved IP",
    "host_id": "e093a352fd3a4ddd994c585e2e1dda59",
    "response_time": 0,
    "response_size": 3318,
    "process_time": 0,
    "request_body": "{}"
  } ]
}
```

Status Codes

Status Code	Description
200	ok

Status Code	Description
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.5.2 Querying the List of Attack Events

Function

This API is used to query the attack event list. Currently, this API does not support query of all protection events. The **pagesize** parameter cannot be set to **-1**. The larger the data volume, the larger the memory consumption. A maximum of 10,000 data records can be queried. For example, if the number of data records in a user-defined period exceeds 10,000, the data whose page is 101 (or **pagesize** is greater than 100) cannot be queried. You need to adjust the time range to a longer period and then query the data.

URI

GET /v1/{project_id}/waf/event

Table 4-689 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-690 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Parameter	Mandatory	Type	Description
recent	No	String	Time range for querying logs. This parameter cannot be used together with from or to at the same time. Parameter recent must be used with either from or to . Enumeration values: <ul style="list-style-type: none"> • yesterday • today • 3days • 1week • 1month
from	No	Long	Start time (13-digit timestamp). This parameter must be used together with to, but cannot be used together with recent.
to	No	Long	End time (13-digit timestamp). This parameter must be used together with from but cannot be used together with recent.

Parameter	Mandatory	Type	Description
attacks	No	Array	<p>Attack type</p> <ul style="list-style-type: none"> • vuln: other attack types • sqli: SQL injection attacks • lfi: local file inclusion • cmdi: command injection attacks • xss: XSS attacks • robot: malicious crawler • rfi: remote file inclusion • custom_custom: attack hit the precision protection rule • cc: CC attacks • webshell: website Trojan • custom_whiteblackip: attacks that hit the blocklist and trustlist rule • custom_geoip: attacks that hit the geolocation access control rule • antitamper: attacks that hit the web tamper prevention rule • anticrawler: attacks that hit the anti-crawler rules • leakage: attacks that hit the information leakage prevention rule • illegal: illegal requests
hosts	No	Array	Domain name ID. It can be obtained by calling the **ListHost API.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned.
pagesize	No	Integer	Number of records on each page during pagination query. The default value is 10 , indicating that each page contains 10 records.

Request Parameters

Table 4-691 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
X-Language	No	String	Language. The default value is en-us. zh-cn (Chinese)/en-us (English)

Response Parameters

Status code: 200

Table 4-692 Response body parameters

Parameter	Type	Description
total	Integer	Number of attack events
items	Array of ListEventItems objects	Details about an attack event

Table 4-693 ListEventItems

Parameter	Type	Description
id	String	Event ID
time	Long	Count
policyid	String	Policy ID
sip	String	Source IP address, which is the IP address of the web visitor (attacker's IP address).
host	String	Attacked domain name
url	String	Attacked URL

Parameter	Type	Description
attack	String	Attack type <ul style="list-style-type: none"> • vuln: other attack types • sqli: SQL injection attack • lfi: local file inclusion • cmdi: command injection attacks • XSS: XSS attacks • robot: malicious crawler • rfi: remote file inclusion • custom_custom: attacks hit a precise protection rule • webshell: Trojan • custom_whiteblackip: attacks hit a blacklist or whitelist rule • custom_geoip: attacks hit a geolocation access control rule • antitamper: attacks hit a web tamper prevention rule • anticrawler: attacks hit an anti-crawler rule • leakage: attacks hit an information leakage prevention rule • illegal: invalid requests
rule	String	ID of the matched rule
payload	String	Hit payload
payload_location	String	Hit Load Position
action	String	Protective action
request_line	String	Request method and path
headers	Object	HTTP request header
cookie	String	Request cookie
status	String	Response code status
process_time	Integer	Processing time
region	String	Geographical location
host_id	String	Domain name ID
response_time	Long	Time to response
response_size	Integer	Response body size

Parameter	Type	Description
response_body	String	Response body
request_body	String	Request body

Status code: 400

Table 4-694 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-695 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-696 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the event list for the current day in a project. The project ID is specified by `project_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/event?
enterprise_project_id=0&page=1&pagesize=10&recent=today
```

Example Responses

Status code: 200

ok

```
{
  "total": 1,
  "items": [ {
    "id": "04-0000-0000-0000-21120220421152601-2f7a5ceb",
    "time": 1650525961000,
    "policyid": "25f1d179896e4e3d87ceac0598f48d00",
    "host": "x.x.x.x:xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx",
    "url": "/osclass/oc-admin/index.php",
    "attack": "lfi",
    "rule": "040002",
    "payload": " file=../../../../../../../../etc/passwd",
    "payload_location": "params",
    "sip": "x.x.x.x",
    "action": "block",
    "request_line": "GET /osclass/oc-admin/index.php?
page=appearance&action=render&file=../../../../../../../../etc/passwd",
    "headers": {
      "accept-language": "en",
      "ls-id": "xxxxx-xxxxx-xxxx-xxxx-9c302cb7c54a",
      "host": "x.x.x.x",
      "lb-id": "2f5f15ce-08f4-4df0-9899-ec0cc1fcdc52",
      "accept-encoding": "gzip",
      "accept": "*/*",
      "user-agent": "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
35.0.2309.372 Safari/537.36"
    },
    "cookie": "HWWAFSESID=2a1d773f9199d40a53; HWWAFSESTIME=1650525961805",
    "status": "418",
    "host_id": "6fbe595e7b874dbbb1505da3e8579b54",
    "response_time": 0,
    "response_size": 3318,
    "response_body": "",
    "process_time": 2,
    "request_body": "{}"
  } ]
}
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.6 Dashboard

4.6.1 Querying the QPS Statistics

Function

This API is used to query the website QPS.

URI

GET /v1/{project_id}/waf/overviews/qps/timeline

Table 4-697 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-698 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project. It can be obtained by calling the ListEnterpriseProject API of EPS.
from	Yes	Long	Start time (13-digit timestamp in millisecond). This parameter must be used together with to .
to	Yes	Long	End time (13-digit timestamp in millisecond). This parameter must be used together with from .

Parameter	Mandatory	Type	Description
hosts	No	String	Domain name IDs. In the cloud mode, domain name IDs can be obtained by calling the ListHost API. In the dedicated mode, domain name IDs can be obtained by calling the ListPremiumHost API. By default, this parameter is not specified, and the QPS data of every protected domain name in the project is queried.
instances	No	String	Instance IDs you want to query. This parameter is required only for dedicated WAF instances and load-balancing instances (ELB mode).
group_by	No	String	Display dimension. For example, the value is DAY if data is displayed by the day.

Request Parameters

Table 4-699 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-700 Response body parameters

Parameter	Type	Description
[items]	Array of StatisticsTimelineItem objects	QPS statistics over time on the dashboard

Table 4-701 StatisticsTimelineItem

Parameter	Type	Description
key	String	Key value. The options are ACCESS for total requests, CRAWLER for bot mitigation, ATTACK for total attacks, WEB_ATTACK for basic web protection, PRECISE for precise protection, and CC for CC attack protection.
timeline	Array of TimeLineItem objects	Statistics data over time for the corresponding key value

Table 4-702 TimeLineItem

Parameter	Type	Description
time	Long	Time point
num	Integer	Statistics for the time range from the previous time point to the point specified by the time field.

Status code: 400

Table 4-703 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-704 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-705 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the QPS. The project ID is specified by `project_id` and the time is from 2022-04-21 00:00:00 to 2022-04-21 14:35:36.

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/qps/timeline?
enterprise_project_id=0&from=1650470400196&to=1650522936196
```

Example Responses

Status code: 200

ok

```
[ {
  "key": "ACCESS",
  "timeline": [ {
    "time": 1650470400000,
    "num": 0
  } ]
}, {
  "key": "PRECISE",
  "timeline": [ {
    "time": 1650470400000,
    "num": 0
  } ]
}, {
  "key": "CRAWLER",
  "timeline": [ {
    "time": 1650470400000,
    "num": 0
  } ]
}, {
  "key": "CC",
  "timeline": [ {
    "time": 1650470400000,
    "num": 0
  } ]
}, {
  "key": "ATTACK",
  "timeline": [ {
```



```

    "time" : 1650470400000,
    "num" : 0
  } ]
}, {
  "key" : "WEB_ATTACK",
  "timeline" : [ {
    "time" : 1650470400000,
    "num" : 0
  } ]
} ]
} ]

```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.6.2 Querying Statistics of Requests and Attacks

Function

Querying Statistics of Requests and Attacks Note that APIs related to the dashboard cannot be used to query data for custom time. Only data displayed on the console for yesterday, today, past 3 days, past 7 days, and past 30 days can be queried.

URI

GET /v1/{project_id}/waf/overviews/statistics

Table 4-706 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-707 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
from	Yes	Long	Start time (13-digit timestamp). This parameter must be used together with to .
to	Yes	Long	End time (13-digit timestamp). This parameter must be used together with from .
hosts	No	String	Domain name IDs. In the cloud mode, domain name IDs can be obtained by calling the ListHost API. In the dedicated mode, domain name IDs can be obtained by calling the ListPremiumHost API. By default, this parameter is not specified, and the number of requests and attacks of all protected domain names in the project is queried.
instances	No	String	Instance IDs you want to query. This parameter is required only for dedicated WAF instances and load-balancing instances (ELB mode).

Request Parameters

Table 4-708 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-709 Response body parameters

Parameter	Type	Description
[items]	Array of CountItem objects	Statistics about requests and attacks on the WAF console

Table 4-710 CountItem

Parameter	Type	Description
key	String	Type. The options are ACCESS for total requests, CRAWLER for bot mitigation, ATTACK for total attacks, WEB_ATTACK for basic web protection, PRECISE for precise protection, and CC for CC attack protection.
num	Integer	Quantity.

Status code: 400

Table 4-711 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-712 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 403

Table 4-713 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-714 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the number of security overview requests and attacks. The project ID is specified by `project_id` and the time is from 2022-04-21 00:00:00 to 2022-04-21 14:35:36.

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/statistics?
enterprise_project_id=0&from=1650470400196&to=1650522936196
```

Example Responses

Status code: 200

Request succeeded.

```
[ {
  "key": "ACCESS",
  "num": 1190
}, {
  "key": "PRECISE",
  "num": 0
}, {
  "key": "CRAWLER",
  "num": 10
}, {
  "key": "WEB_ATTACK",
  "num": 22
}, {
  "key": "CC",
  "num": 0
}, {
  "key": "ATTACK",
  "num": 32
} ]
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
403	The resource quota is insufficient.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.6.3 Querying Bandwidth Usage Statistics

Function

This API is used to query average bandwidth usage (in bit/s) for a specific time range.

URI

GET /v1/{project_id}/waf/overviews/bandwidth/timeline

Table 4-715 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-716 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Parameter	Mandatory	Type	Description
from	Yes	Long	Start time (13-digit timestamp in millisecond) of the time range for which you want to query the average bandwidth usage. This parameter must be used together with to .
to	Yes	Long	End time (13-digit timestamp in millisecond) of the time range for which you want to query the average bandwidth usage. This parameter must be used together with from .
hosts	No	String	IDs of the domain names for which you want to query the bandwidth usage for a time range that is specified by from and to . In the cloud mode, domain name IDs can be obtained by calling the ListHost API. In the dedicated mode, domain name IDs can be obtained by calling the ListPremiumHost API.
instances	No	String	IDs of dedicated WAF instances. This parameter is used to query the average bandwidth usage of domain names protected by those dedicated WAF instances for a time range that is specified by from and to .
group_by	No	String	How data is displayed. For example, if the value is DAY , data is displayed by the day. If this parameter is not specified, the data is displayed by the minute.

Request Parameters

Table 4-717 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-718 Response body parameters

Parameter	Type	Description
[items]	Array of BandwidthStatisticsTimelineItem objects	Bandwidth statistics over the time, including BANDWIDTH , IN_BANDWIDTH , and OUT_BANDWIDTH .

Table 4-719 BandwidthStatisticsTimelineItem

Parameter	Type	Description
key	String	Key value. The options are BANDWIDTH , IN_BANDWIDTH , and OUT_BANDWIDTH .
timeline	Array of TimeLineItem objects	Statistics of the corresponding key value over time. This parameter includes the time field for the time point and the num field for statistics between the previous time point and the time point specified by the time field.

Table 4-720 TimeLineItem

Parameter	Type	Description
time	Long	Time point

Parameter	Type	Description
num	Integer	Statistics for the time range from the previous time point to the point specified by the time field.

Status code: 400

Table 4-721 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-722 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-723 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the bandwidth usage. The project ID is specified by `project_id` and the time is from 2022-04-21 00:00:00 to 2022-04-21 14:35:36.

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/bandwidth/timeline?
enterprise_project_id=0&from=1650470400196&to=1650522936196
```

Example Responses

Status code: 200

ok

```
[ {
  "key": "IN_BANDWIDTH",
  "timeline": [ {
    "time": 1650470400000,
    "num": 0
  } ]
}, {
  "key": "OUT_BANDWIDTH",
  "timeline": [ {
    "time": 1650470400000,
    "num": 0
  } ]
}, {
  "key": "BANDWIDTH",
  "timeline": [ {
    "time": 1650470400000,
    "num": 0
  } ]
} ]
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.6.4 Querying Statistics of Top Exceptions

Function

This API is used to query top service exceptions, such as abnormal requests or errors.

URI

GET /v1/{project_id}/waf/overviews/abnormal

Table 4-724 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-725 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
from	Yes	Long	Start time (13-digit timestamp in millisecond). This parameter must be used together with to .
to	Yes	Long	End time (13-digit timestamp in millisecond). This parameter must be used together with from .
top	No	Integer	Top N results to be queried. The default value is 5, and the maximum value is 10.
code	No	Integer	Error code to be queried. Currently, 404, 500, and 502 are supported. If this parameter is not specified, status code 404 is queried by default.

Parameter	Mandatory	Type	Description
hosts	No	String	Domain name IDs. In the cloud mode, domain name IDs can be obtained by calling the ListHost API. In the dedicated mode, domain name IDs can be obtained by calling the ListPremiumHost API. By default, this parameter is not required, and the statistics data of all protected domain names in the project is queried.
instances	No	String	Instance IDs you want to query. This parameter is required only for dedicated WAF instances and load-balancing instances (ELB mode).

Request Parameters

Table 4-726 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-727 Response body parameters

Parameter	Type	Description
total	Integer	Number of abnormal requests

Parameter	Type	Description
items	Array of UrlCountItem objects	Array of abnormal request information.

Table 4-728 UrlCountItem

Parameter	Type	Description
key	String	Attack Type.
num	Integer	Quantity.
host	String	Protected domain names

Status code: 400

Table 4-729 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-730 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-731 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the number of 404 errors and top exceptions. The project ID is specified by `project_id` and the time is from 2022-04-21 00:00:00 to 2022-04-21 14:35:36.

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/abnormal?
enterprise_project_id=0&from=1650470400089&to=1650523520089&top=10&code=404
```

Example Responses

Status code: 200

ok

```
{
  "total" : 2,
  "items" : [ {
    "key" : "/",
    "num" : 6,
    "host" : "hkh4.test.418lab.cn"
  }, {
    "key" : "/",
    "num" : 6,
    "host" : "ces_after.test.418lab.cn"
  } ]
}
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.6.5 Querying Top Security Statistics by Category

Function

This API is used to query statistics by category, including the attacked domain name, attack source IP address, attacked URL, attack source region, and attack event distribution.

URI

```
GET /v1/{project_id}/waf/overviews/classification
```

Table 4-732 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-733 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
from	Yes	Long	Start time (13-digit timestamp in millisecond). This parameter must be used together with to .
to	Yes	Long	End time (13-digit timestamp in millisecond). This parameter must be used together with from .
top	No	Integer	The first several results you want to query. Maximum value: 10 . Default value: 5 .
hosts	No	String	Domain name IDs. In the cloud mode, domain name IDs can be obtained by calling the ListHost API. In the dedicated mode, domain name IDs can be obtained by calling the ListPremiumHost API. By default, this parameter is not required, and the statistics data of all protected domain names in the project is queried. To query data about several specified domain names, refer to the request example.

Parameter	Mandatory	Type	Description
instances	No	String	Instance IDs you want to query. This parameter is required only for dedicated WAF instances and load-balancing instances (ELB mode).

Request Parameters

Table 4-734 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
X-Language	No	String	Language. The default value is en-us. zh-cn (Chinese)/en-us (English)

Response Parameters

Status code: 200

Table 4-735 Response body parameters

Parameter	Type	Description
domain	DomainClassificationItem object	Attacked domain name
attack_type	AttackTypeClassificationItem object	Attack event distribution
ip	IpClassificationItem object	Attacking source IP address
url	UrlClassificationItem object	Attacking URL

Parameter	Type	Description
geo	GeoClassificationItem object	Source region

Table 4-736 DomainClassificationItem

Parameter	Type	Description
total	Integer	Total number of DomainItem
items	Array of DomainItem objects	DomainItem details

Table 4-737 DomainItem

Parameter	Type	Description
key	String	Domain name
num	Integer	Quantity.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.

Table 4-738 AttackTypeClassificationItem

Parameter	Type	Description
total	Integer	Total number of AttackTypeItem
items	Array of AttackTypeItem objects	AttackTypeItem details

Table 4-739 AttackTypeItem

Parameter	Type	Description
key	String	Attack type
num	Integer	Quantity.

Table 4-740 IpClassificationItem

Parameter	Type	Description
total	Integer	Total number of IpItem
items	Array of IpItem objects	IpItem Details

Table 4-741 IpItem

Parameter	Type	Description
key	String	IP address.
num	Integer	Quantity.

Table 4-742 UrlClassificationItem

Parameter	Type	Description
total	Integer	Total number of UrlItem
items	Array of UrlItem objects	UrlItem Details

Table 4-743 UrlItem

Parameter	Type	Description
key	String	URL path.
num	Integer	Quantity.
host	String	Domain name

Table 4-744 GeoClassificationItem

Parameter	Type	Description
total	Integer	Total number of GeoItem
items	Array of GeoItem objects	GeoItem details

Table 4-745 Geoltem

Parameter	Type	Description
key	String	Source region
num	Integer	Quantity.

Status code: 400

Table 4-746 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-747 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-748 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the top 10 security overview statistics in a project. The project ID is specified by `project_id`. The time is from 2022-05-19 00:00:00 to 2022-06-17 11:14:41. The domain name ID is 1bac09440a814aa98ed08302c580a48b, and engine instance ID is 5a532f83a2fb476ba51ca1de7b1ebc43.

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/classification?
enterprise_project_id=0&from=1652889600354&to=1655435681354&top=10&hosts=1bac09440a814aa98ed0
8302c580a48b&instances=5a532f83a2fb476ba51ca1de7b1ebc43
```

Example Responses

Status code: 200

ok

```
{
  "attack_type": {
    "total": 1,
    "items": [ {
      "key": "custom_custom",
      "num": 2
    } ]
  },
  "domain": {
    "total": 2,
    "items": [ {
      "key": "www.whitelist.com",
      "num": 2,
      "web_tag": "www.whitelist.com"
    }, {
      "key": "zbx002.apayaduo.cn",
      "num": 2,
      "web_tag": ""
    } ]
  },
  "geo": {
    "total": 1,
    "items": [ {
      "key": "Shanghai",
      "num": 2
    } ]
  },
  "ip": {
    "total": 1,
    "items": [ {
      "key": "10.142.4.15",
      "num": 2
    } ]
  },
  "url": {
    "total": 1,
    "items": [ {
      "key": "/attack",
      "num": 2,
      "host": "www.whitelist.com"
    } ]
  }
}
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.6.6 Querying Website Requests

Function

This API is used to query website requests.

URI

GET /v1/{project_id}/waf/overviews/request/timeline

Table 4-749 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-750 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
from	Yes	Long	Start time (13-digit timestamp in millisecond). This parameter must be used together with to .
to	Yes	Long	End time (13-digit timestamp in millisecond). This parameter must be used together with from .

Parameter	Mandatory	Type	Description
hosts	No	Array	Domain name IDs. In the cloud mode, domain name IDs can be obtained by calling the ListHost API. In the dedicated mode, domain name IDs can be obtained by calling the ListPremiumHost API. By default, this parameter is not required, and the statistics data of all protected domain names in the project is queried. To query data about several specified domain names, refer to the request example.
instances	No	Array	Instance IDs you want to query. This parameter is required only for dedicated WAF instances and load-balancing instances (ELB mode).
group_by	No	String	How data is displayed. To display data by the day, set the parameter to DAY . By default, this parameter is not specified, and data is displayed by the minute.

Request Parameters

Table 4-751 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-752 Response body parameters

Parameter	Type	Description
[items]	Array of StatisticsTimelineItem objects	Request Timeline Data for Security Statistics.

Table 4-753 StatisticsTimelineItem

Parameter	Type	Description
key	String	Key value. The options are ACCESS for total requests, CRAWLER for bot mitigation, ATTACK for total attacks, WEB_ATTACK for basic web protection, PRECISE for precise protection, and CC for CC attack protection.
timeline	Array of TimeLineItem objects	Statistics data over time for the corresponding key value

Table 4-754 TimeLineItem

Parameter	Type	Description
time	Long	Time point
num	Integer	Statistics for the time range from the previous time point to the point specified by the time field.

Status code: 400

Table 4-755 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-756 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-757 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the number of requests in security overview in a project. The project ID is specified by `project_id` and the time is from 2022-04-21 00:00:00 to 2022-04-21 00:00:50.

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/request/timeline?
enterprise_project_id=0&from=1650470400196&to=1650470450000
```

Example Responses

Status code: 200

ok

```
[ {
  "key": "ACCESS",
  "timeline": [ {
    "time": 1650470400196,
    "num": 0
  } ]
}, {
  "key": "PRECISE",
  "timeline": [ {
    "time": 1650470400196,
    "num": 0
  } ]
}, {
  "key": "CRAWLER",
  "timeline": [ {
    "time": 1650470400196,
    "num": 0
  } ]
}, {
  "key": "CC",
  "timeline": [ {
    "time": 1650470400196,
    "num": 0
  } ]
}, {
```

```
"key" : "ATTACK",
"timeline" : [ {
  "time" : 1650470400000,
  "num" : 0
} ]
}, {
"key" : "WEB_ATTACK",
"timeline" : [ {
  "time" : 1650470400196,
  "num" : 0
} ]
} ]
```

Status Codes

Status Code	Description
200	ok
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.7 Dedicated Instance Management

4.7.1 Querying Dedicated WAF Instances

Function

This API is used to query the list of dedicated WAF instances. Dedicated WAF instances are supported only in some regions, including: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN-Hong Kong, AP-Bangkok, and AP-Singapore

URI

GET /v1/{project_id}/premium-waf/instance

Table 4-758 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-759 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project. It can be obtained by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number for pagination query. The default value is 1.
pagesize	No	Integer	Records that can be displayed on each page. The default value is 10.
instancename	No	String	Fuzzy query of dedicated WAF engine names

Request Parameters

Table 4-760 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-761 Response body parameters

Parameter	Type	Description
total	Integer	Number of the dedicated WAF instance.
purchased	Boolean	Whether any dedicated WAF instance has been purchased.
items	Array of ListInstance objects	Details about the dedicated WAF instance.

Table 4-762 ListInstance

Parameter	Type	Description
id	String	IDs of the dedicated WAF instance.
instancename	String	Names of the dedicated WAF instance.
region	String	ID of the region where the dedicated WAF instance is deployed.
zone	String	AZ ID
arch	String	CPU architecture.
cpu_flavor	String	ECS specifications.
vpc_id	String	ID of the VPC where the dedicated WAF instance locates.
subnet_id	String	ID of the VPC subnet where the dedicated WAF instance locates.
service_ip	String	Service plane IP address of the dedicated WAF instance.
security_group_ids	Array of strings	Security group where the dedicated WAF instance is added.
status	Integer	Billing status of the dedicated WAF instance. <ul style="list-style-type: none"> ● 0: Normal. ● 1: Frozen. Resources and data will be retained, but the instance cannot be used. ● 2: Terminated. Resources and data will be cleared.

Parameter	Type	Description
run_status	Integer	Running status of the dedicated instance. The value can be any of the following: <ul style="list-style-type: none"> ● 0: Creating ● 1: Running ● 2: Deleting ● 3: Deleted ● 4: Creation failed ● 5: Frozen ● 6: Abnormal ● 7: Updating ● 8: Update failed
access_status	Integer	Access status of the domain names protected with the dedicated WAF instance. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: the domain name is not connected with the dedicated WAF instance. ● 1: The domain name is connected with the dedicated WAF instance.
upgradable	Integer	Whether the dedicated WAF instance can be upgraded. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The instance cannot be upgraded. ● 1: The instance can be upgraded.
cloudServiceType	String	Cloud service code This parameter is used as an identifier only. You can ignore this parameter.
resourceType	String	Cloud service resource type, which is used as an identifier only. You can ignore this parameter.
resourceSpecCode	String	Cloud service resource code This parameter is used as an identifier only. You can ignore this parameter.
specification	String	Dedicated engine ECS specifications, for example, 8 vCPUs 16 GB
hosts	Array of IdHostnameEntry objects	Domain name protected by the dedicated engine
serverId	String	ID of the ECS hosting the dedicated engine
create_time	Long	Time the dedicated WAF instance is created.

Parameter	Type	Description
instance_name	String	Names of the dedicated WAF instance.

Table 4-763 IdHostnameEntry

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Protected Domain Name

Status code: 400

Table 4-764 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-765 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-766 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the dedicated WAF instance list in a project. The project ID is specified by `project_id`.

```
GET https://{endpoint}/v1/{project_id}/premium-waf/instance
```

Example Responses

Status code: 200

Lists of dedicated WAF instances

```
{
  "purchased" : true,
  "total" : 1,
  "items" : [ {
    "id" : "0619871acb764d48a112695e8f7cbb10",
    "region" : "region-01-7",
    "zone" : "region-01-7a",
    "specification" : "8vCPUs | 16GB",
    "arch" : "x86",
    "upgradable" : 0,
    "status" : 0,
    "serverId" : "477353dc-8687-4bf4-b45b-1d7fee74fa63",
    "cloudServiceType" : "hws.service.type.waf",
    "resourceType" : "hws.resource.type.waf.instance",
    "resourceSpecCode" : "waf.instance.enterprise",
    "vpc_id" : "13718074-a3f9-408d-82aa-3c41ef55e589",
    "subnet_id" : "74d1b5a6-c7eb-4e9a-8372-181212552fcc",
    "service_ip" : "192.168.10.68",
    "security_group_ids" : [ "34287bdb-7aba-471a-b041-27427f1af76a" ],
    "cpu_flavor" : "Si2.2xlarge.2",
    "run_status" : 2,
    "access_status" : 1,
    "hosts" : [ {
      "id" : "c3be17bbe3a641c7a1ded6019c377402",
      "hostname" : "demo.www.com"
    } ],
    "instance_name" : "0412elb"
  } ]
}
```

Status Codes

Status Code	Description
200	Lists of dedicated WAF instances
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.7.2 Creating a Dedicated WAF Instance

Function

This API is used to create a dedicated WAF instance. Dedicated WAF instances are supported only in some regions, including CN East-Qingdao, ME-Riyadh, CN North-Beijing1, CN North-Beijing4, CN North-Ulanqab1, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN South-Shenzhen, and CN-Hong Kong, CN Southwest - Guiyang 1, AP-Bangkok, AP-Singapore, AP-Johannesburg, and TR-Istanbul. Dedicated instances of the ECS type are supported in the following regions: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN-Hong Kong, AP-Bangkok, and AP-Singapore.

URI

POST /v1/{project_id}/premium-waf/instance

Table 4-767 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-768 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project. It can be obtained by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-769 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-770 Request body parameters

Parameter	Mandatory	Type	Description
chargemode	No	Integer	Billing mode. Currently, only pay-per-use (30) is supported.
region	Yes	String	Region where a dedicated engine is to be created, for example, cn-north-4.
available_zone	Yes	String	AZ where the dedicated engine is to be created, for example, AZ 1 of CN North-Beijing4 (cn-north-4a)
arch	Yes	String	CPU architecture of the dedicated WAF instance, supporting only x86
instancename	Yes	String	Prefix of dedicated WAF engine names
specification	Yes	String	Specifications of the dedicated WAF instance <ul style="list-style-type: none"> • waf.instance.enterprise: the enterprise edition, corresponding to WI-500 on the console. • waf.instance.enterprise: the professional edition, corresponding to WI-100 on the console.

Parameter	Mandatory	Type	Description
cpu_flavor	No	String	Flavor of the ECS used for the dedicated WAF instance. This parameter is optional when you create the WAF instances of the network interface type. This parameter is mandatory when you create the WAF instances of the ECS type. For WAF instances of the ECS type, select a flavor based on what are available on the console.
vpc_id	Yes	String	ID of the VPC where the dedicated engine is located.
subnet_id	Yes	String	ID of the VPC subnet where the dedicated engine is located.
security_group	Yes	Array of strings	ID of the security group where the dedicated engine is located.
count	Yes	Integer	Number of dedicated WAF instance applied for
res_tenant	No	Boolean	Whether this is resource tenant. The default value is false. <ul style="list-style-type: none"> ● false: common tenant. ● true: resource tenant.
anti_affinity	No	Boolean	Whether to enable anti-affinity. Only the WAF instances of the network interface type support this feature.

Response Parameters

Status code: 200

Table 4-771 Response body parameters

Parameter	Type	Description
instances	Array of instanceInfo objects	instances

Table 4-772 instanceInfo

Parameter	Type	Description
id	String	ID of the dedicated WAF instance.
name	String	Name of the dedicated WAF instance.

Status code: 400

Table 4-773 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-774 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-775 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a WAF dedicated instance. The project ID is specified by project_id. Billing mode: pay-per-use. Region: region-01-4. AZ: region-01-4a. CPU architecture: x86. Prefix of the instance name: demo. Edition: Enterprise. VPC ID: d7b6a5ff-6c53-4cd4-9d57-f20ee8753056. Subnet ID: e59ccd18-7e15-4588-b689-04b856f4e78b. Security group ID: 09b156a2-f0f0-41fd-9891-60e594601cfd. Quantity: one. Instance type: ECS.

```
POST https://{endpoint}/v1/{project_id}/premium-waf/instance
```

```
{
  "chargemode" : 30,
  "region" : "region-01-4",
  "available_zone" : "region-01-4a",
  "arch" : "x86",
  "instancename" : "demo",
  "specification" : "waf.instance.enterprise",
  "vpc_id" : "d7b6a5ff-6c53-4cd4-9d57-f20ee8753056",
  "subnet_id" : "e59ccd18-7e15-4588-b689-04b856f4e78b",
  "security_group" : [ "09b156a2-f0f0-41fd-9891-60e594601cfd" ],
  "count" : 1,
  "res_tenant" : true
}
```

Example Responses

Status code: 200

Dedicated WAF instance information

```
{
  "instances" : [ {
    "id" : "50a6b6c9bdb643f9a8038976fc58ad02",
    "name" : "demo-6wvl"
  } ]
}
```

Status Codes

Status Code	Description
200	Dedicated WAF instance information
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.7.3 Querying Details about a Dedicated WAF Instance

Function

This API is used to query details about a dedicated WAF instance. Dedicated WAF instances are supported only in some regions, including: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN-Hong Kong, AP-Bangkok, AP-Singapore

URI

GET /v1/{project_id}/premium-waf/instance/{instance_id}

Table 4-776 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
instance_id	Yes	String	ID of the dedicated WAF instance. It can be obtained by calling the WAF ListInstance API

Table 4-777 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project. It can be obtained by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-778 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-779 Response body parameters

Parameter	Type	Description
id	String	ID of the dedicated WAF instance.
instancename	String	Name of the dedicated WAF instance.
region	String	ID of the region where the dedicated WAF instance is deployed.
zone	String	AZ ID
arch	String	CPU Architecture
cpu_flavor	String	ECS Specifications
vpc_id	String	ID of the VPC where the dedicated WAF instance locates.
subnet_id	String	ID of the VPC subnet where the dedicated WAF instance locates.
service_ip	String	Service plane IP address of the dedicated WAF instance.
security_group_ids	Array of strings	Security group where the dedicated WAF instance is added.
status	Integer	Billing status of the dedicated WAF instance. <ul style="list-style-type: none"> ● 0: Normal. ● 1: Frozen. Resources and data will be retained, but the instance cannot be used. ● 2: Terminated. Resources and data will be cleared.
run_status	Integer	Running status of the dedicated instance. The value can be any of the following: <ul style="list-style-type: none"> ● 0: Creating ● 1: Running ● 2: Deleting ● 3: Deleted ● 4: Creation failed ● 5: Frozen ● 6: Abnormal ● 7: Updating ● 8: Update failed
access_status	Integer	Access status of the dedicated engine. The value 0 indicates that the dedicated engine is not connected, and the value 1 indicates that the dedicated engine is connected.

Parameter	Type	Description
upgradable	Integer	Whether the dedicated engine can be upgraded (0: no; 1: yes)
cloudServiceType	String	Cloud service code This parameter is used as an identifier only. You can ignore this parameter.
resourceType	String	Cloud service resource type, which is used as an identifier only. You can ignore this parameter.
resourceSpecCode	String	Cloud service resource code This parameter is used as an identifier only. You can ignore this parameter.
specification	String	Dedicated engine ECS specifications, for example, 8 vCPUs 16 GB
serverId	String	ID of the ECS hosting the dedicated engine
create_time	Long	Time the dedicated WAF instance is created.

Status code: 400

Table 4-780 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-781 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-782 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query a dedicated WAF instance in a project. The project ID is specified by `project_id`, and the instance ID is specified by `instance_id`.

```
GET https://{endpoint}/v1/{project_id}/premium-waf/instance/{instance_id}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id": "0619871acb764d48a112695e8f7cbb10",
  "region": "region-01-7",
  "zone": "region-01-7a",
  "specification": "8vCPUs | 16GB",
  "arch": "x86",
  "upgradable": 0,
  "status": 0,
  "serverId": "477353dc-8687-4bf4-b45b-1d7fee74fa63",
  "cloudServiceType": "hws.service.type.waf",
  "resourceType": "hws.resource.type.waf.instance",
  "resourceSpecCode": "waf.instance.enterprise",
  "vpc_id": "13718074-a3f9-408d-82aa-3c41ef55e589",
  "subnet_id": "74d1b5a6-c7eb-4e9a-8372-181212552fcc",
  "service_ip": "192.168.10.68",
  "security_group_ids": [ "34287bdb-7aba-471a-b041-27427f1af76a" ],
  "cpu_flavor": "Si2.2xlarge.2",
  "run_status": 2,
  "access_status": 1,
  "instancename": "0412elb",
  "create_time": 1649217360674
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.7.4 Renaming a Dedicated WAF Instance

Function

This API is used to rename a dedicated WAF engine. Dedicated WAF instances are supported only in some regions, including: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN-Hong Kong, AP-Bangkok, AP-Singapore

URI

PUT /v1/{project_id}/premium-waf/instance/{instance_id}

Table 4-783 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
instance_id	Yes	String	ID of the dedicated WAF instance. It can be obtained by calling the WAF ListInstance API

Table 4-784 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project. It can be obtained by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-785 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-786 Request body parameters

Parameter	Mandatory	Type	Description
instancename	Yes	String	New name of the dedicated WAF engine

Response Parameters

Status code: 200

Table 4-787 Response body parameters

Parameter	Type	Description
id	String	ID of the dedicated WAF instance.
instancename	String	Name of the dedicated WAF instance.
region	String	ID of the region where the dedicated WAF instance is deployed.
zone	String	AZ ID
arch	String	CPU Architecture
cpu_flavor	String	ECS Specifications
vpc_id	String	ID of the VPC where the dedicated WAF instance locates.
subnet_id	String	ID of the VPC subnet where the dedicated WAF instance locates.
service_ip	String	Service plane IP address of the dedicated WAF instance.

Parameter	Type	Description
security_group_ids	Array of strings	Security group where the dedicated WAF instance is added.
status	Integer	Billing status of the dedicated WAF instance. <ul style="list-style-type: none"> ● 0: Normal. ● 1: Frozen. Resources and data will be retained, but the instance cannot be used. ● 2: Terminated. Resources and data will be cleared.
run_status	Integer	Running status of the dedicated instance. The value can be any of the following: <ul style="list-style-type: none"> ● 0: Creating ● 1: Running ● 2: Deleting ● 3: Deleted ● 4: Creation failed ● 5: Frozen ● 6: Abnormal ● 7: Updating ● 8: Update failed
access_status	Integer	Access status of the dedicated engine. The value 0 indicates that the dedicated engine is not connected, and the value 1 indicates that the dedicated engine is connected.
upgradable	Integer	Whether the dedicated engine can be upgraded (0: no; 1: yes)
cloudServiceType	String	Cloud service code This parameter is used as an identifier only. You can ignore this parameter.
resourceType	String	Cloud service resource type, which is used as an identifier only. You can ignore this parameter.
resourceSpecCode	String	Cloud service resource code This parameter is used as an identifier only. You can ignore this parameter.
specification	String	Dedicated engine ECS specifications, for example, 8 vCPUs 16 GB
serverId	String	ID of the ECS hosting the dedicated engine
create_time	Long	Time the dedicated WAF instance is created.

Status code: 400

Table 4-788 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-789 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-790 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update a dedicated WAF instance in a project. The project ID is specified by `project_id`, and the instance ID is specified by `instance_id`. The new instance name is `0412elb`.

```
PUT https://{endpoint}/v1/{project_id}/premium-waf/instance/{instance_id}
{
  "instancename" : "0412elb"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "0619871acb764d48a112695e8f7cbb10",
  "region" : "region-01-7",
  "zone" : "region-01-7a",
```

```
"specification" : "8vCPUs | 16GB",  
"arch" : "x86",  
"upgradable" : 0,  
"status" : 0,  
"serverId" : "477353dc-8687-4bf4-b45b-1d7fee74fa63",  
"cloudServiceType" : "hws.service.type.waf",  
"resourceType" : "hws.resource.type.waf.instance",  
"resourceSpecCode" : "waf.instance.enterprise",  
"vpc_id" : "13718074-a3f9-408d-82aa-3c41ef55e589",  
"subnet_id" : "74d1b5a6-c7eb-4e9a-8372-181212552fcc",  
"service_ip" : "192.168.10.68",  
"security_group_ids" : [ "34287bdb-7aba-471a-b041-27427f1af76a" ],  
"cpu_flavor" : "Si2.2xlarge.2",  
"run_status" : 2,  
"access_status" : 1,  
"instancename" : "0412elb"  
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.7.5 Deleting a Dedicated WAF Instance

Function

This API is used to delete a dedicated WAF instance. Dedicated WAF instances are supported only in some regions, including: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN South-Shenzhen, CN-Hong Kong, AP-Bangkok, AP-Singapore

URI

DELETE /v1/{project_id}/premium-waf/instance/{instance_id}

Table 4-791 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
instance_id	Yes	String	ID of the dedicated WAF instance. It can be obtained by calling the WAF ListInstance API

Table 4-792 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project. It can be obtained by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-793 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-794 Response body parameters

Parameter	Type	Description
id	String	ID of the dedicated WAF instance.
instancename	String	Name of the dedicated WAF instance.
region	String	ID of the region where the dedicated WAF instance is deployed.
zone	String	AZ ID
arch	String	CPU Architecture
cpu_flavor	String	ECS Specifications
vpc_id	String	ID of the VPC where the dedicated WAF instance locates.
subnet_id	String	ID of the VPC subnet where the dedicated WAF instance locates.
service_ip	String	Service plane IP address of the dedicated WAF instance.
security_group_ids	Array of strings	Security group where the dedicated WAF instance is added.
status	Integer	Billing status of the dedicated WAF instance. <ul style="list-style-type: none"> ● 0: Normal. ● 1: Frozen. Resources and data will be retained, but the instance cannot be used. ● 2: Terminated. Resources and data will be cleared.
run_status	Integer	Running status of the dedicated instance. The value can be any of the following: <ul style="list-style-type: none"> ● 0: Creating ● 1: Running ● 2: Deleting ● 3: Deleted ● 4: Creation failed ● 5: Frozen ● 6: Abnormal ● 7: Updating ● 8: Update failed
access_status	Integer	Access status of the dedicated engine. The value 0 indicates that the dedicated engine is not connected, and the value 1 indicates that the dedicated engine is connected.

Parameter	Type	Description
upgradable	Integer	Whether the dedicated engine can be upgraded (0: no; 1: yes)
cloudServiceType	String	Cloud service code This parameter is used as an identifier only. You can ignore this parameter.
resourceType	String	Cloud service resource type, which is used as an identifier only. You can ignore this parameter.
resourceSpecCode	String	Cloud service resource code This parameter is used as an identifier only. You can ignore this parameter.
specification	String	Dedicated engine ECS specifications, for example, 8 vCPUs 16 GB
serverId	String	ID of the ECS hosting the dedicated engine
create_time	Long	Time the dedicated WAF instance is created.

Status code: 400

Table 4-795 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-796 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-797 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a dedicated WAF instance in a project. The project ID is specified by `project_id`, and the instance ID is specified by `instance_id`.

```
DELETE https://{endpoint}z/v1/{project_id}/premium-waf/instance/{instance_id}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id": "0619871acb764d48a112695e8f7cbb10",
  "region": "region-01-7",
  "zone": "region-01-7a",
  "specification": "8vCPUs | 16GB",
  "arch": "x86",
  "upgradable": 0,
  "status": 0,
  "serverId": "477353dc-8687-4bf4-b45b-1d7fee74fa63",
  "cloudServiceType": "hws.service.type.waf",
  "resourceType": "hws.resource.type.waf.instance",
  "resourceSpecCode": "waf.instance.enterprise",
  "vpc_id": "13718074-a3f9-408d-82aa-3c41ef55e589",
  "subnet_id": "74d1b5a6-c7eb-4e9a-8372-181212552fcc",
  "service_ip": "192.168.10.68",
  "security_group_ids": [ "34287bdb-7aba-471a-b041-27427f1af76a" ],
  "cpu_flavor": "Si2.2xlarge.2",
  "run_status": 2,
  "access_status": 1,
  "instancename": "0412elb"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.8 Log Reporting

4.8.1 Querying LTS Settings

Function

This API is used to query the LTS settings.

URI

GET /v1/{project_id}/waf/config/lts

Table 4-798 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-799 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-800 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-801 Response body parameters

Parameter	Type	Description
id	String	LTS configuration information ID. Each enterprise project has a unique ID.
enabled	Boolean	Whether to enable LTS for WAF logging - false : LTS is disabled for WAF. - true : LTS is enabled for WAF.
ltsIdInfo	LtsIdInfo object	Log group and log stream IDs.
enabale	Boolean	This parameter has been discarded. Ignore it.

Table 4-802 LtsIdInfo

Parameter	Type	Description
ltsGroupId	String	Log group ID.
ltsAccessStreamID	String	Log stream ID for access logs
ltsAttackStreamID	String	Log stream ID for attack logs

Status code: 400

Table 4-803 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-804 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-805 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the LTS configuration in a project. The project ID is specified by project_id.

```
GET https://{Endpoint}/v1/{project_id}/waf/config/lts?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "enabled": true,
  "id": "c89a667487734f6a95e9967d1f373c77",
  "ltsIdInfo": {
    "ltsAccessStreamID": "4bcff74d-f649-41c8-8325-1b0a264ff683",
    "ltsAttackStreamID": "0a7ef713-cc3e-418d-abda-85df04db1a3c",
    "ltsGroupId": "f4fa07f6-277b-4e4a-a257-26508ece81e6"
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.

Status Code	Description
500	Internal server error.

Error Codes

See [Error Codes](#).

4.8.2 Configuring LTS for WAF Logging

Function

This API is used to enable or disable Log Tank Service (LTS) for WAF logging and to configure log groups and streams. You can obtain the log group ID and log stream ID from LTS. The log stream ID must belong to the log group you configure.

URI

PUT /v1/{project_id}/waf/config/lts/{ltsconfig_id}

Table 4-806 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
ltsconfig_id	Yes	String	ID of the LTS configuration. The ID can be obtained by calling the ShowLtsInfoConfig API.

Table 4-807 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-808 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-809 Request body parameters

Parameter	Mandatory	Type	Description
enabled	No	Boolean	Whether to enable LTS for WAF logging - false : LTS is disabled for WAF. - true : LTS is enabled for WAF.
ltsIdInfo	No	LtsIdInfo object	Log group and log stream IDs.
enabale	No	Boolean	This parameter has been discarded. Ignore it.

Table 4-810 LtsIdInfo

Parameter	Mandatory	Type	Description
ltsGroupId	No	String	Log group ID.
ltsAccessStreamID	No	String	Log stream ID for access logs
ltsAttackStreamID	No	String	Log stream ID for attack logs

Response Parameters

Status code: 200

Table 4-811 Response body parameters

Parameter	Type	Description
id	String	LTS configuration information ID. Each enterprise project has a unique ID.
enabled	Boolean	Whether to enable LTS for WAF logging - false : LTS is disabled for WAF. - true : LTS is enabled for WAF.
ltsIdInfo	LtsIdInfo object	Log group and log stream IDs.
enable	Boolean	This parameter has been discarded. Ignore it.

Table 4-812 LtsIdInfo

Parameter	Type	Description
ltsGroupId	String	Log group ID.
ltsAccessStreamId	String	Log stream ID for access logs
ltsAttackStreamId	String	Log stream ID for attack logs

Status code: 400**Table 4-813** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401**Table 4-814** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-815 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update the LTS configuration in a project. The project ID is specified by `project_id`. The new LTS configuration ID is `c89a667487734f6a95e9967d1f373c77`. LTS for WAF logging is enabled. Log group ID: `4bcff74d-f649-41c8-8325-1b0a264ff683`. Access og stream ID: `0a7ef713-cc3e-418d-abda-85df04db1a3c`. Attack log stream ID: `f4fa07f6-277b-4e4a-a257-26508ece81e6`

```
GET https://{Endpoint}/v1/{project_id}/waf/config/lts/c89a667487734f6a95e9967d1f373c77?enterprise_project_id=0
```

```
{
  "enabled" : true,
  "ltsIdInfo" : {
    "ltsAccessStreamID" : "4bcff74d-f649-41c8-8325-1b0a264ff683",
    "ltsAttackStreamID" : "0a7ef713-cc3e-418d-abda-85df04db1a3c",
    "ltsGroupId" : "f4fa07f6-277b-4e4a-a257-26508ece81e6"
  }
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "enabled" : true,
  "id" : "c89a667487734f6a95e9967d1f373c77",
  "ltsIdInfo" : {
    "ltsAccessStreamID" : "4bcff74d-f649-41c8-8325-1b0a264ff683",
    "ltsAttackStreamID" : "0a7ef713-cc3e-418d-abda-85df04db1a3c",
    "ltsGroupId" : "f4fa07f6-277b-4e4a-a257-26508ece81e6"
  }
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.9 Managing Your Subscriptions

4.9.1 Request body for buying a yearly/monthly-billed cloud WAF instance

Function

Request body for buying a yearly/monthly-billed cloud WAF instance. Expansion packages are not supported by the starter edition.

Constraints

If the payment fails, the system automatically generates a pending payment order. You can select another payment method on the console. The Starter edition is available only in CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Guangzhou-InvitationOnly regions.

URI

POST /v1/{project_id}/waf/subscription/purchase/prepaid-cloud-waf

Table 4-816 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain the value, go to the Cloud management console first. Then, click your username, select My Credentials , and view the Project ID column in the Projects area.

Table 4-817 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-818 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-819 Request body parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
is_auto_pay	Yes	Boolean	Whether automatic payment is enabled. <ul style="list-style-type: none"> false: Automatic payment is not enabled. You need to complete payment manually. **: Automatic payment is enabled.
is_auto_renew	Yes	Boolean	Whether auto-renewal is enabled. <ul style="list-style-type: none"> true: Auto-renewal is enabled for the instance. false: Auto-renewal is disabled for the instance.
region_id	Yes	String	region Id
waf_product_info	No	WafProductInfo object	Details about purchased WAF instances
domain_expansion_product_info	No	ExpackProductInfo object	Domain name expansion packages purchased
bandwidth_expansion_product_info	No	ExpackProductInfo object	Bandwidth expansion packages purchased
rule_expansion_product_info	No	ExpackProductInfo object	Rule expansion packages purchased

Table 4-820 WafProductInfo

Parameter	Mandatory	Type	Description
resource_spec_code	No	String	WAF editions <ul style="list-style-type: none">• detection: The Starter edition. (This edition is available only in CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, and CN South-Guangzhou-InvitationOnly regions.)• professional: The Standard edition.• enterprise: The Professional edition.• ultimate: The Platinum edition.
period_type	No	String	Period type in yearly/monthly billing. month (2) is for monthly billing and year(3) for yearly billing.
period_num	No	Integer	Number of subscription periods

Table 4-821 ExpackProductInfo

Parameter	Mandatory	Type	Description
resource_size	No	Integer	Number of expansion packages

Response Parameters

Status code: 200

Table 4-822 Response body parameters

Parameter	Type	Description
orderId	String	Order ID.

Status code: 400

Table 4-823 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-824 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-825 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to purchase yearly/monthly billed cloud WAF. Project Id:550500b49078408682d0d4f7d923f3e1. Auto-renewal: Disabled. Region ID: cn-north-7. Quantity of bandwidth expansion packages: 1.

```
POST https://{Endpoint}/v1/{project_id}/waf/subscription/purchase/prepaid-cloud-waf?
enterprise_project_id=0

{
  "project_id": "550500b49078408682d0d4f7d923f3e1",
  "is_auto_renew": false,
  "is_auto_pay": false,
  "region_id": "cn-north-7",
  "bandwidth_expack_product_info": {
    "resource_size": 1
  }
}
```

Example Responses

Status code: 200

Request succeeded.

```
{  
  "orderId" : "38ff0cb9a10e4d5293c642bc0350fa6d"  
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.9.2 Changing specifications of a cloud WAF instance billed yearly/monthly.

Function

This API is used to change specifications of a cloud WAF instance that is billed yearly/monthly. Notes:

- **1:** The cloud WAF instance must be billed yearly/monthly.
- **2:** The edition for the WAF instance cannot be scaled down. The number of any type of expansion packages cannot be decreased to 0.
- **3:** The number of each type of expansion packages can only be increased or decreased together.

Constraints

If the payment fails, the system automatically generates a pending payment order. You can select another payment method on the console.

URI

POST /v1/{project_id}/waf/subscription/batchalter/prepaid-cloud-waf

Table 4-826 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain the value, go to the Cloud management console first. Then, click your username, select My Credentials , and view the Project ID column in the Projects area.

Table 4-827 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-828 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-829 Request body parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Parameter	Mandatory	Type	Description
is_auto_pay	Yes	Boolean	Whether automatic payment is enabled. <ul style="list-style-type: none"> • false: Automatic payment is not enabled. You need to complete payment manually. • **: Automatic payment is enabled.
waf_product_info	No	AlterWafProductInfo object	Changing the WAF edition.
domain_expand_product_info	No	ExpackProductInfo object	Changing the quantity of domain name expansion packages
bandwidth_expand_product_info	No	ExpackProductInfo object	Changing the quantity of bandwidth name expansion packages
rule_expand_product_info	No	ExpackProductInfo object	Changing the quantity of rule name expansion packages

Table 4-830 AlterWafProductInfo

Parameter	Mandatory	Type	Description
resource_spec_code	No	String	WAF editions <ul style="list-style-type: none"> • detection: The Starter edition. • professional: The Standard edition. • enterprise: The Professional edition. • ultimate: The Platinum edition.

Table 4-831 ExpackProductInfo

Parameter	Mandatory	Type	Description
resource_size	No	Integer	Number of expansion packages

Response Parameters

Status code: 200

Table 4-832 Response body parameters

Parameter	Type	Description
orderId	String	Order ID.

Status code: 400

Table 4-833 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-834 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-835 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to change the yearly/monthly cloud WAF specifications. Project ID: 550500b49078408682d0d4f7d923f3e1. Auto-renewal: changed to enabled. Quantity of bandwidth expansion packages: changed to 2.

```
POST https://{Endpoint}/v1/{project_id}/waf/subscription/batchalter/prepaid-cloud-waf?
enterprise_project_id=0
```

```
{  
  "project_id" : "550500b49078408682d0d4f7d923f3e1",  
  "is_auto_pay" : true,  
  "domain_expack_product_info" : {  
    "resource_size" : 2  
  }  
}
```

Example Responses

Status code: 200

Request succeeded.

```
{  
  "orderId" : "38ff0cb9a10e4d5293c642bc0350fa6d"  
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.9.3 Enabling Pay-Per-Use Billing for Cloud WAF

Function

This API is used to enable the pay-per-use billing mode for cloud WAF.

URI

POST /v1/{project_id}/waf/postpaid

Table 4-836 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-837 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-838 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
region	Yes	String	Region ID.

Table 4-839 Request body parameters

Parameter	Mandatory	Type	Description
console_area	Yes	String	Website the account belongs to. The value is hec-hk for International website.

Response Parameters

Status code: 200

Table 4-840 Response body parameters

Parameter	Type	Description
type	Integer	The edition for the cloud WAF instance. <ul style="list-style-type: none"> • -2: Frozen. • 1: Not subscribed. • 2: The Standard edition. • 3: The Professional edition. • 4: The Platinum edition. • 7: The Starter edition. • 22: The pay-per-use edition.
resources	Array of ResourceResponse objects	The resource list.
isNewUser	Boolean	New user or not.

Table 4-841 ResourceResponse

Parameter	Type	Description
resourceId	String	Resource ID.
cloudServiceType	String	Cloud service type

Parameter	Type	Description
resourceType	String	Cloud service resource type. <ul style="list-style-type: none"> • hws.resource.type.waf: yearly/monthly cloud-mode WAF • hws.resource.type.waf.domain: domain name expansion packages in yearly/monthly cloud-mode WAF • hws.resource.type.waf.domain: bandwidth expansion packages in yearly/monthly cloud-mode WAF • hws.resource.type.waf.domain: rule expansion packages in yearly/monthly cloud-mode WAF • hws.resource.type.waf.payperuserequest: requests to pay-per-use WAF instances • hws.resource.type.waf.payperusedomain: domain names protected with pay-per-use WAF instances • hws.resource.type.waf.payperuserule: rules created in pay-per-use WAF instances
resourceSpecCode	String	Cloud resource specifications.
status	Integer	Resource status. The value can be: <ul style="list-style-type: none"> • 0: Unfrozen/Normal. • 1: Frozen. • 2: Deleted.
expireTime	String	Resource expiration time.
resourceSize	Integer	Resource quantity.

Status code: 400

Table 4-842 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-843 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-844 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to enable pay-per-use billing for cloud WAF in a specific project. The project ID is specified by `project_id`. The site is International website.

```
POST https://{Endpoint}/v1/{project_id}/waf/postpaid?enterprise_project_id=0
{
  "console_area" : "hec-hk"
}
```

Example Responses

Status code: 200

OK

```
{
  "type" : 22,
  "resources" : [ {
    "resourceId" : "71f5de5f03414225b79be43ee3dc6bae",
    "cloudServiceType" : "hws.service.type.waf",
    "resourceType" : "hws.resource.type.waf.payperusedomain",
    "resourceSpecCode" : "waf.payperuse.domain",
    "resourceSize" : null,
    "expireTime" : null,
    "status" : 0
  }, {
    "resourceId" : "eb0760007a0b43fd9e445f5ce810f4c4",
    "cloudServiceType" : "hws.service.type.waf",
    "resourceType" : "hws.resource.type.waf.payperuserequest",
    "resourceSpecCode" : "waf.payperuse.request",
    "resourceSize" : null,
    "expireTime" : null,
    "status" : 0
  }, {
    "resourceId" : "6cae8a4d8074499d8c3bda687d63c4f9",
    "cloudServiceType" : "hws.service.type.waf",
    "resourceType" : "hws.resource.type.waf.payperuserule",
```

```

"resourceSpecCode" : "waf.payperuse.rule",
"resourceSize" : null,
"expireTime" : null,
"status" : 0
}],
"isNewUser" : false
}

```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.9.4 Disabling Pay-Per-Use Pricing for Cloud WAF

Function

This API is used to disable the pay-per-use billing mode for cloud WAF.

URI

DELETE /v1/{project_id}/waf/postpaid

Table 4-845 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-846 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-847 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
region	No	String	Region ID

Response Parameters

Status code: 200

Table 4-848 Response body parameters

Parameter	Type	Description
type	Integer	The edition for the cloud WAF instance. <ul style="list-style-type: none"> • -2: Frozen. • 1: Not subscribed. • 2: The Standard edition. • 3: The Professional edition. • 4: The Platinum edition. • 7: The Starter edition. • 22: The pay-per-use edition.
resources	Array of ResourceResponse objects	The resource list.
isNewUser	Boolean	New user or not.

Table 4-849 ResourceResponse

Parameter	Type	Description
resourceId	String	Resource ID.
cloudServiceType	String	Cloud service type
resourceType	String	Cloud service resource type. <ul style="list-style-type: none"> hws.resource.type.waf: yearly/monthly cloud-mode WAF hws.resource.type.waf.domain: domain name expansion packages in yearly/monthly cloud-mode WAF hws.resource.type.waf.domain: bandwidth expansion packages in yearly/monthly cloud-mode WAF hws.resource.type.waf.domain: rule expansion packages in yearly/monthly cloud-mode WAF hws.resource.type.waf.payperuserequest: requests to pay-per-use WAF instances hws.resource.type.waf.payperusedomain: domain names protected with pay-per-use WAF instances hws.resource.type.waf.payperuserule: rules created in pay-per-use WAF instances
resourceSpecCode	String	Cloud resource specifications.
status	Integer	Resource status. The value can be: <ul style="list-style-type: none"> 0: Unfrozen/Normal. 1: Frozen. 2: Deleted.
expireTime	String	Resource expiration time.
resourceSize	Integer	Resource quantity.

Status code: 400

Table 4-850 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-851 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-852 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to disable the pay-per-use billing for cloud WAF in a specific project. The project ID is specified by `project_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/postpaid?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "type" : -1,
  "resources" : [ ],
  "isNewUser" : false
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.9.5 Querying Your Subscriptions

Function

This API is used to query your subscriptions to cloud and dedicated WAF instances billed on a yearly/monthly or pay-per-use basis.

URI

GET /v1/{project_id}/waf/subscription

Table 4-853 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain the value, go to the Cloud management console first. Then, click your username, select My Credentials , and view the Project ID column in the Projects area.

Request Parameters

Table 4-854 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-855 Response body parameters

Parameter	Type	Description
type	Integer	The edition for the cloud WAF instance. <ul style="list-style-type: none"> • -2: Frozen. • -1: Not subscribed. • 2: The Standard edition. • 3: The Professional edition. • 4: The Platinum edition. • 7: The Starter edition. • 22: The pay-per-use edition.
resources	Array of ResourceResponse objects	The resource list.
isNewUser	Boolean	New user or not.
premium	Premium object	Information about subscriptions to dedicated WAF instances

Table 4-856 ResourceResponse

Parameter	Type	Description
resourceId	String	Resource ID.
cloudServiceType	String	Cloud service type

Parameter	Type	Description
resourceType	String	Cloud service resource type. <ul style="list-style-type: none"> hws.resource.type.waf: yearly/monthly cloud-mode WAF hws.resource.type.waf.domain: domain name expansion packages in yearly/monthly cloud-mode WAF hws.resource.type.waf.domain: bandwidth expansion packages in yearly/monthly cloud-mode WAF hws.resource.type.waf.domain: rule expansion packages in yearly/monthly cloud-mode WAF hws.resource.type.waf.payperuserequest: requests to pay-per-use WAF instances hws.resource.type.waf.payperusedomain: domain names protected with pay-per-use WAF instances hws.resource.type.waf.payperuserule: rules created in pay-per-use WAF instances
resourceSpecCode	String	Cloud resource specifications.
status	Integer	Resource status. The value can be: <ul style="list-style-type: none"> 0: Unfrozen/Normal. 1: Frozen. 2: Deleted.
expireTime	String	Resource expiration time.
resourceSize	Integer	Resource quantity.

Table 4-857 Premium

Parameter	Type	Description
purchased	Boolean	Whether the dedicated mode is enabled.
total	Integer	The number of dedicated WAF instances, including load-balancing instances.
elb	Integer	The number of load-balancing WAF instances (ELB mode).
dedicated	Integer	The number of the dedicated WAF instances

Status code: 400

Table 4-858 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-859 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-860 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the subscriptions in a project. The project ID is specified by `project_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/subscription?
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "type" : 3,
  "resources" : [ {
    "resourceId" : "d2759a06ed844b9c9837bb76326ca656",
    "cloudServiceType" : "hws.service.type.waf",
    "resourceType" : "hws.resource.type.waf",
    "resourceSpecCode" : "waf.enterprise",
    "resourceSize" : null,
    "expireTime" : "2022-12-07T15:59:59Z",
    "status" : 0
  }, {
    "resourceId" : "6a5a4b06dbcd4cc5be6ff88bcd988046",
```

```

"cloudServiceType" : "hws.service.type.waf",
"resourceType" : "hws.resource.type.waf.rule",
"resourceSpecCode" : "waf.expack.rule.enterprise",
"resourceSize" : 5,
"expireTime" : "2022-12-07T15:59:59Z",
"status" : 0
}, {
"resourceId" : "a9202ca8704740b6a1e0481c80bd4255",
"cloudServiceType" : "hws.service.type.waf",
"resourceType" : "hws.resource.type.waf.domain",
"resourceSpecCode" : "waf.expack.domain.enterprise",
"resourceSize" : 10,
"expireTime" : "2022-12-07T15:59:59Z",
"status" : 0
}],
"isNewUser" : false,
"premium" : {
"purchased" : true,
"total" : 8,
"elb" : 0,
"dedicated" : 8
}
}

```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.10 Domain Name Management

4.10.1 Migrating Protected Domain Names by Enterprise Project

Function

This API is used to migrate a WAF instance along with domain names it protects from the current enterprise project to another. Only the professional and platinum editions support this function.

URI

POST /v1/{project_id}/composite-waf/hosts/migration

Table 4-861 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-862 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	Yes	String	ID of the source enterprise project
target_enterprise_project_id	Yes	String	ID of the destination enterprise project

Request Parameters

Table 4-863 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-864 Request body parameters

Parameter	Mandatory	Type	Description
host_ids	Yes	Array of strings	Host ID list.
policy_id	Yes	String	ID of the rule in the current enterprise project.

Parameter	Mandatory	Type	Description
certificate_id	No	String	Certificate ID (certificate ID in the current enterprise project)

Response Parameters

Status code: 200

Table 4-865 Response body parameters

Parameter	Type	Description
host_ids	Array of strings	Specifies the host ID list.
policy_id	String	ID of the rule in the current enterprise project.
certificate_id	String	Certificate ID (certificate ID in the current enterprise project)

Status code: 400

Table 4-866 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-867 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-868 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to migrate a domain name along with protection policy used for the domain name in a project from an enterprise project to another. Domain name ID: 6cc26af071de46479840b41c143bb79b. Protection policy ID: b97ce5d4e38d4eaf94d65be7372974a8. Project ID: project_id. Source enterprise project ID: 0. Destination enterprise project ID: c341b6bd-0935-462b-abb5-28a63bd68021

```
POST https://{Endpoint}/v1/{project_id}/composite-waf/hosts/migration?
enterprise_project_id=0&target_enterprise_project_id=c341b6bd-0935-462b-abb5-28a63bd68021

{
  "host_ids" : [ "6cc26af071de46479840b41c143bb79b" ],
  "policy_id" : "b97ce5d4e38d4eaf94d65be7372974a8"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "host_ids" : [ "6cc26af071de46479840b41c143bb79b" ],
  "policy_id" : "b97ce5d4e38d4eaf94d65be7372974a8"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.11 System Management

4.11.1 Querying the IP addresses of WAF

Function

This API is used to query WAF IP addresses.

URI

GET /v1/{project_id}/waf/config/source-ip

Table 4-869 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Request Parameters

Table 4-870 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-871 Response body parameters

Parameter	Type	Description
source_ip	Array of IpsItem objects	Origin server information list
last_modify	Long	Last time the WAF IP addresses are updated.

Table 4-872 IpsItem

Parameter	Type	Description
ips	Array of strings	WAF retrieval IP address
update_time	Long	Time the WAF IP addresses are updated.

Status code: 400

Table 4-873 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-874 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-875 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Example Requests

The following example shows how to query the WAF IP addresses in a project. The project ID is specified by `project_id`.

```
GET https://{endpoint}/v1/{project_id}/waf/config/source-ip
```

Example Responses

Status code: 200

IP addresses of WAF

```
{
  "source_ip": [ {
    "ips": [ "122.112.208.32/28", "49.4.56.64/27", "2407:c080:804::/48" ],
    "update_time": 1573779840000
  } ]
}
```

Status Codes

Status Code	Description
200	IP addresses of WAF
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.12 Alarm Management

4.12.1 This API is used to query configuration of alarm notifications.

Function

Querying Alarm Notification Configuration

URI

GET /v2/{project_id}/waf/alerts

Table 4-876 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-877 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-878 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-879 Response body parameters

Parameter	Type	Description
total	Integer	Total number of configured alarm notifications
items	Array of AlertNoticeConfigResponse objects	Configured alarm notifications

Table 4-880 AlertNoticeConfigResponse

Parameter	Type	Description
id	String	ID
name	String	Alarm notification name
enabled	Boolean	Whether to enable <ul style="list-style-type: none"> false: It is disabled for WAF. true: It is enabled.
topic_urn	String	Theme
sendfreq	Integer	Interval, in minute. When the notification type is event, an alarm notification is sent when the number of attacks within the given interval is greater than or equal to the threshold. The value can be 5, 15, 30, 60, 120, 360, 720, or 1440 . When the notification type is certificate expiration, an alarm notification is sent once within the give interval. The supported values are 1440 and 10080 (unit: minute).
locale	String	Language
times	Integer	This parameter is mandatory when notification type is set to Event . A notification alarm is sent when the number of attacks reaches the configured threshold. Default: 1
threat	Array of strings	Event type
prefer_html	Boolean	This parameter is reserved and can be ignored. Default: false
notice_class	String	Notification type
nearly_expire_d_time	String	Advance notification days

Parameter	Type	Description
is_all_enterprise_project	Boolean	Whether all enterprise projects are involved. Default: true
enterprise_project_id	String	Specifies the enterprise project ID.
update_time	Long	Update time.

Status code: 400

Table 4-881 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-882 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-883 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the alarm notifications in a project. The project ID is specified by project_id.

```
GET https://{Endpoint}/v2/{project_id}/waf/alerts?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total": 1,
  "items": [ {
    "enabled": true,
    "enterprise_project_id": "0",
    "id": "753231205d474fa78655760c8dbd9e6f",
    "is_all_enterprise_project": true,
    "locale": "zh-cn",
    "name": "test-demo33",
    "nearly_expired_time": 60,
    "notice_class": "cert_alert_notice",
    "prefer_html": false,
    "sendfreq": 10080,
    "threat": [ ],
    "times": 1,
    "topic_urn": "urn:smn:cn-north-7:550500b49078408682d0d4f7d923f3e1:ces_zyh_test",
    "update_time": 1664347553944
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.12.2 This API is used to update alarm notification configuration.

Function

Updating Alarm Notification Configuration

URI

PUT /v2/{project_id}/waf/alert/{alert_id}

Table 4-884 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
alert_id	Yes	String	Alarm ID.

Request Parameters

Table 4-885 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8
X-Language	Yes	String	zh-cn/en-us

Table 4-886 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Alarm notification name
enabled	No	Boolean	Whether to enable this function. <ul style="list-style-type: none"> false: It is disabled for WAF. true: It is enabled.
topic_urn	Yes	String	Topic URN. You can obtain it by calling an API of [Simple Message Notification].

Parameter	Mandatory	Type	Description
sendfreq	No	Integer	Interval, in minute. When the notification type is event, an alarm notification is sent when the number of attacks within the given interval is greater than or equal to the threshold. The value can be 5, 15, 30, 60, 120, 360, 720 , or 1440 . When the notification type is certificate expiration, an alarm notification is sent once within the give interval. The supported values are 1440 and 10080 (unit: minute). Default: 5
locale	No	String	Language. <ul style="list-style-type: none"> • zh-cn: Chinese. • en-us: English.
times	No	Integer	This parameter is mandatory when notification type is event-based. A notification alarm is sent when the number of attacks reaches the configured threshold. Default: 1
threat	No	Array of strings	Event type
notice_class	Yes	String	Notification type. <ul style="list-style-type: none"> • threat_alert_notice: Events. • cert_alert_notice: Certificate expiration
nearly_expired_time	No	String	How long before you certificate expires you want the system to notify you. This parameter is mandatory when the notification type is certificate expiration.
is_all_enterprise_project	No	Boolean	Whether all enterprise projects are involved.

Response Parameters

Status code: **200**

Table 4-887 Response body parameters

Parameter	Type	Description
id	String	ID
name	String	Alarm notification name
enabled	Boolean	Whether to enable this function <ul style="list-style-type: none"> ● false: It is disabled for WAF. ● true: Enable
topic_urn	String	Theme
sendfreq	Integer	Interval, in minute. When the notification type is event, an alarm notification is sent when the number of attacks within the given interval is greater than or equal to the threshold. The value can be 5, 15, 30, 60, 120, 360, 720, or 1440 . When the notification type is certificate expiration, an alarm notification is sent once within the give interval. The supported values are 1440 and 10080 (unit: minute).
locale	String	Languages
times	Integer	This parameter is mandatory when notification type is event-based. A notification alarm is sent when the number of attacks reaches the configured threshold. Default: 1
threat	Array of strings	Event type.
prefer_html	Boolean	This parameter is reserved and can be ignored. Default: false
notice_class	String	Alarm type.
nearly_expire_d_time	String	Advance notification days
is_all_enterprise_project	Boolean	Whether all enterprise projects are involved. Default: true
enterprise_project_id	String	Enterprise project ID.
update_time	Long	Update time.

Status code: 400

Table 4-888 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-889 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-890 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to update the alarm notification configuration for a project. Project ID: project_id. Notification type: Certificate expiration. Topic URN: urn:smn:cn-north-7:550500b49078408682d0d4f7d923f3e1:ces_zyh_test. Alarm notification name: test. Notifications are sent 60 days before a certificate expires at an interval of 10,080 minutes.

```
PUT https://{Endpoint}/v2/{project_id}/waf/alert/{alert_id}?enterprise_project_id=0
{
  "notice_class": "cert_alert_notice",
  "topic_urn": "urn:smn:cn-north-7:550500b49078408682d0d4f7d923f3e1:ces_zyh_test",
  "name": "test",
  "nearly_expired_time": 60,
  "sendfreq": 10080
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "enabled": true,
```

```
"enterprise_project_id" : "0",
"id" : "7a19ee86a7dc43f0b12093decb795096",
"is_all_enterprise_project" : true,
"locale" : "zh-cn",
"name" : "demo",
"nearly_expired_time" : 60,
"notice_class" : "cert_alert_notice",
"prefer_html" : false,
"sendfreq" : 10080,
"threat" : [ ],
"times" : 1,
"topic_urn" : "urn:smn:cn-north-7:550500b49078408682d0d4f7d923f3e1:ces_zyh_test"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.13 Protected Website Management in Cloud Mode

4.13.1 Querying the List of Domain Names Protected in Cloud Mode

Function

This API is used to query the list of domain names protected in cloud mode.

URI

GET /v1/{project_id}/waf/instance

Table 4-891 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-892 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned. Default: 1
pagesize	No	Integer	Number of results on each page in query pagination. The value range is 1 to 100. The default value is 10 , indicating that each page contains 10 results. To query all domain names at a time, set this parameter to -1 . Default: 10
hostname	No	String	The domain name whose information you want to query. This parameter is used to query information about a specified domain name. If this parameter is not specified, all domain names protected with cloud WAF are queried.
policyname	No	String	Protection policy name. This parameter is used to query domain names added to a specified protection policy. This parameter is optional.

Request Parameters

Table 4-893 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-894 Response body parameters

Parameter	Type	Description
total	Integer	Number of domain names protected with cloud WAF
items	Array of CloudWafHostItem objects	Array of details about the protected domain names protected with cloud WAF.

Table 4-895 CloudWafHostItem

Parameter	Type	Description
id	String	Domain name ID
hostid	String	Domain name ID
region	String	Region ID. This parameter is included when the domain name was added to WAF through the console. This parameter is left blank when the domain name was added to WAF by calling an API. You can query the region ID on the Regions and Endpoints page on the website.
description	String	(Optional) Descriptions of the domain names
type	Integer	WAF deployment mode. The default value is 1 . Currently, only the reverse proxy is supported. This parameter is redundant.

Parameter	Type	Description
proxy	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> ● false: No proxy is used. ● true: A proxy is used.
hostname	String	Domain name added to cloud WAF.
access_code	String	CNAME prefix, CNAME suffix: .vip1.huaweicloudwaf.com
policyid	String	Policy ID
timestamp	Long	Time the domain name was added to WAF.
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> ● -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. ● 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
exclusive_ip	Boolean	Whether to use a dedicated IP address. This parameter is reserved and can be ignored. <ul style="list-style-type: none"> ● true: Use a dedicated IP address. ● false: Do not use a dedicated IP address.
paid_type	String	Package billing mode. The value can be prePaid or postPaid. prePaid is for yearly/monthly billing. postPaid is for pay-per-use billing. Default value: prePaid.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
flag	Flag object	Special identifier, which is used on the console.

Table 4-896 Flag

Parameter	Type	Description
pci_3ds	String	<p>Whether the website passes the PCI 3DS certification check.</p> <ul style="list-style-type: none"> ● true: The website passed the PCI 3DS certification check. ● false: The website failed the PCI 3DS certification check. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
pci_dss	String	<p>Whether the website passed the PCI DSS certification check.</p> <ul style="list-style-type: none"> ● true: The website passed the PCI DSS certification check. ● false: The website failed the PCI DSS certification check. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
cname	String	<p>The CNAME record being used.</p> <ul style="list-style-type: none"> ● old: The old CNAME record is used. ● new: The new CNAME record is used. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	<p>Whether WAF support Multi-AZ DR</p> <ul style="list-style-type: none"> ● true: WAF supports multi-AZ DR. ● false: WAF does not support multi-AZ DR. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
ipv6	String	<p>Whether IPv6 protection is supported.</p> <ul style="list-style-type: none"> ● true: IPv6 protection is supported. ● false: IPv6 protection is not supported. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false

Status code: 400

Table 4-897 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-898 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-899 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to obtain all domain names protected with cloud WAF in a specific project. The project ID is specified by project_id.

```
GET https://{Endpoint}/v1/{project_id}/waf/instance?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "total": 1,
  "items": [ {
    "id": "d0a4bc2f74e3407388a50243af700305",
    "hostid": "d0a4bc2f74e3407388a50243af700305",
    "description": "e",
    "type": 1,
    "proxy": false,
    "flag": {
```



```
"pci_3ds" : "false",
"pci_dss" : "false",
"ipv6" : "false",
"cname" : "new",
"is_dual_az" : "true"
},
"region" : "cn-north-4",
"hostname" : "www.demo.com",
"access_code" : "7d06456ffaxxxxxxxxxxxx281bc13b",
"policyid" : "bb2124fabe6f42ff9fe4770eeccb2670",
"timestamp" : 1642648030687,
"protect_status" : 1,
"access_status" : 0,
"exclusive_ip" : false,
"web_tag" : "iii",
"paid_type" : "prePaid"
}]
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.13.2 Adding a Domain Name to the Cloud WAF

Function

This API is used to add a domain name to the cloud WAF.

URI

POST /v1/{project_id}/waf/instance

Table 4-900 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-901 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-902 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-903 Request body parameters

Parameter	Mandatory	Type	Description
hostname	Yes	String	The domain name can contain a maximum of 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed, for example, www.domain.com.

Parameter	Mandatory	Type	Description
policyid	No	String	ID of the policy initially used to the domain name. You can call the ListPolicy API to query the policy list and view the ID of the specific policy.
server	Yes	Array of CloudWafServer objects	Origin server configuration of the protected domain name
certificateid	No	String	Certificate ID. It can be obtained by calling the ListCertificates API. <ul style="list-style-type: none"> This parameter is not required when the client protocol is HTTP. This parameter is mandatory when the client protocol is HTTPS.
certificatename	No	String	Certificate name. <ul style="list-style-type: none"> This parameter is not required when the client protocol is HTTP. This parameter is mandatory when the client protocol is HTTPS.
web_tag	No	String	Website name
exclusive_ip	No	Boolean	Whether to use a dedicated IP address. This parameter is reserved and can be ignored. <ul style="list-style-type: none"> true: Use a dedicated IP address. false: Do not use a dedicated IP address.
paid_type	No	String	Package billing mode. The value can be prePaid or postPaid. prePaid is for yearly/monthly billing. postPaid is for pay-per-use billing. Default value: prePaid.
proxy	Yes	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> false: No proxy is used. true: A proxy is used.

Parameter	Mandatory	Type	Description
lb_algorithm	No	String	<p>Load balancing algorithms. This parameter is included only in the professional edition (formerly enterprise edition) and platinum edition (formerly premium edition).</p> <ul style="list-style-type: none"> • Source IP hash: Requests from a certain IP address are forwarded to the same server. • Weighted round robin: All requests are distributed to origin servers in turn based on the weight assigned to each server. • Session hash: Requests with a specific session ID are forwarded to the same origin server. Ensure that the traffic identifiers for known attack sources are configured after the domain name was added to WAF. Otherwise, the session hash configuration does not take effect. <p>Enumeration values:</p> <ul style="list-style-type: none"> • ip_hash • round_robin • session_hash
description	No	String	Domain name description

Parameter	Mandatory	Type	Description
forward_header_map	No	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: <ul style="list-style-type: none"> • \$time_local • \$request_id • \$connection_requests • \$tenant_id • \$project_id • \$remote_addr • \$remote_port • \$scheme • \$request_method • \$http_host • \$origin_uri • \$request_length • \$ssl_server_name • \$ssl_protocol • \$ssl_curves • \$ssl_session_reused

Table 4-904 CloudWafServer

Parameter	Mandatory	Type	Description
front_protocol	Yes	String	Protocol used by the client to request access to the origin server. Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
back_protocol	Yes	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS

Parameter	Mandatory	Type	Description
weight	No	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is 1 . This field is not included by cloud WAF.
address	Yes	String	IP address of your origin server requested by the client
port	Yes	Integer	Port used by WAF to forward client requests to the origin server
type	Yes	String	Origin server IP address format, IPv4 and IPv6 Enumeration values: <ul style="list-style-type: none"> • ipv4 • ipv6

Response Parameters

Status code: 200

Table 4-905 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name added to cloud WAF.
policyid	String	Policy ID
access_code	String	CNAME prefix, CNAME suffix: .vip1.huaweicloudwaf.com
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> • -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.

Parameter	Type	Description
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
lb_algorithm	String	Load balancing algorithms. This parameter is included only in the professional edition (formerly enterprise edition) and platinum edition (formerly premium edition). <ul style="list-style-type: none"> ● Source IP hash: Requests from a certain IP address are forwarded to the same server. ● Weighted round robin: All requests are distributed to origin servers in turn based on the weight assigned to each server. ● Session hash: Requests with a specific session ID are forwarded to the same origin server. Ensure that the traffic identifiers for known attack sources are configured after the domain name was added to WAF. Otherwise, the session hash configuration does not take effect. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● ip_hash ● round_robin ● session_hash
protocol	String	Returned client protocol type
certificateid	String	Returned certificate ID
certificatenam e	String	Certificate name
server	Array of CloudWafServer objects	Origin server configuration of the protected domain name
proxy	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> ● false: No proxy is used. ● true: A proxy is used.
timestamp	Long	Time the domain name was added to WAF.
exclusive_ip	Boolean	Whether to use a dedicated IP address. This parameter is reserved and can be ignored. <ul style="list-style-type: none"> ● true: Use a dedicated IP address. ● false: Do not use a dedicated IP address.
web_tag	String	Website name

Parameter	Type	Description
http2_enable	Boolean	Whether to support HTTP/2. <ul style="list-style-type: none"> ● true: HTTP/2 is supported. ● false: HTTP/2 is not supported.
block_page	BlockPage object	Alarm page configuration
flag	Flag object	Special identifier, which is used on the console.
extend	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.
forward_header_map	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: <ul style="list-style-type: none"> ● \$time_local ● \$request_id ● \$connection_requests ● \$tenant_id ● \$project_id ● \$remote_addr ● \$remote_port ● \$scheme ● \$request_method ● \$http_host ● \$origin_uri ● \$request_length ● \$ssl_server_name ● \$ssl_protocol ● \$ssl_curves ● \$ssl_session_reused

Table 4-906 CloudWafServer

Parameter	Type	Description
front_protocol	String	Protocol used by the client to request access to the origin server. Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
back_protocol	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
weight	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is 1. This field is not included by cloud WAF.
address	String	IP address of your origin server requested by the client
port	Integer	Port used by WAF to forward client requests to the origin server
type	String	Origin server IP address format, IPv4 and IPv6 Enumeration values: <ul style="list-style-type: none"> • ipv4 • ipv6

Table 4-907 BlockPage

Parameter	Type	Description
template	String	Template name
custom_page	CustomPage object	Custom alarm page
redirect_url	String	URL of the redirected page

Table 4-908 CustomPage

Parameter	Type	Description
status_code	String	Status Codes

Parameter	Type	Description
content_type	String	The content type of the custom alarm page. The value can be text/html , text/xml , or application/json .
content	String	The page content based on the selected page type. For details, see the <i>Web Application Firewall (WAF) User Guide</i> .

Table 4-909 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. <ul style="list-style-type: none"> ● true: The website passed the PCI 3DS certification check. ● false: The website failed the PCI 3DS certification check. Enumeration values: <ul style="list-style-type: none"> ● true ● false
pci_dss	String	Whether the website passed the PCI DSS certification check. <ul style="list-style-type: none"> ● true: The website passed the PCI DSS certification check. ● false: The website failed the PCI DSS certification check. Enumeration values: <ul style="list-style-type: none"> ● true ● false
cname	String	The CNAME record being used. <ul style="list-style-type: none"> ● old: The old CNAME record is used. ● new: The new CNAME record is used. Enumeration values: <ul style="list-style-type: none"> ● old ● new

Parameter	Type	Description
is_dual_az	String	Whether WAF support Multi-AZ DR <ul style="list-style-type: none"> • true: WAF supports multi-AZ DR. • false: WAF does not support multi-AZ DR. Enumeration values: <ul style="list-style-type: none"> • true • false
ipv6	String	Whether IPv6 protection is supported. <ul style="list-style-type: none"> • true: IPv6 protection is supported. • false: IPv6 protection is not supported. Enumeration values: <ul style="list-style-type: none"> • true • false

Status code: 400

Table 4-910 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-911 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-912 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to add a website domain name to cloud WAF in a specific project. The project ID is specified by `project_id`, and the domain name is `www.demo.com`. The client protocol is HTTPS, and server protocol is HTTP. The origin server address is `ipv4 x.x.x.x`. The service port used by WAF to forward client requests to the origin server is 7443. The domain name does not use a proxy or dedicated IP address. The WAF is billed yearly/monthly. The domain name description is `dome`. The website name is `dome`. The certificate name is `test6`, and the certificate ID is `3ac1402300374a63a05be68c641e92c8`.

```
POST https://{Endpoint}/v1/{project_id}/waf/instance?enterprise_project_id=0
{
  "hostname": "www.demo.com",
  "server": [ {
    "front_protocol": "HTTPS",
    "back_protocol": "HTTP",
    "type": "ipv4",
    "address": "x.x.x.x",
    "port": "7443"
  } ],
  "proxy": false,
  "paid_type": "prePaid",
  "description": "demo",
  "web_tag": "demo",
  "certificateid": "3ac1402300374a63a05be68c641e92c8",
  "certificatename": "test6",
  "exclusive_ip": false
}
```

Example Responses

Status code: 200

OK

```
{
  "id": "31af669f567246c289771694f2112289",
  "hostname": "www.demo.com",
  "protocol": "HTTP",
  "server": [ {
    "address": "x.x.x.x",
    "port": 80,
    "type": "ipv4",
    "weight": 1,
    "front_protocol": "HTTP",
    "back_protocol": "HTTP"
  } ],
  "proxy": false,
  "timestamp": 1650527546420,
  "flag": {
    "pci_3ds": "false",
    "pci_dss": "false",
    "ipv6": "false",
    "cname": "new",
    "is_dual_az": "true"
  },
  "policyid": "41cba8aee2e94bcdbf57460874205494",
  "protect_status": 1,
  "access_status": 0,
  "access_code": "1b18879b9d064f8bbcbf8abce7294cac",
  "block_page": {
    "template": "default"
  },
  "web_tag": ""
}
```

```
"exclusive_ip" : false,  
"http2_enable" : false  
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.13.3 Querying Details About a Domain Name by Domain Name ID in Cloud Mode

Function

This API is used to query details about a domain name protected in cloud mode by domain name ID.

URI

GET /v1/{project_id}/waf/instance/{instance_id}

Table 4-913 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
instance_id	Yes	String	Domain name ID. It can be obtained by calling the ListHost API.

Table 4-914 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-915 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-916 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name added to cloud WAF.
policyid	String	ID of the policy used for the domain name.
domainid	String	Account ID, which is the same as the account ID on the My Credentials page. To go to this page, log in to Cloud management console, hover the cursor over your username, and click My Credentials in the displayed window.
projectid	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Parameter	Type	Description
enterprise_project_id	String	Enterprise project ID. To obtain the ID, log in to the Cloud management console first. On the menu bar at the top of the page, choose Enterprise > Project Management . Then, click the project name and view the ID.
protocol	String	Backend protocol type. The value can be HTTPS, HTTP, or HTTP&HTTPS.
server	Array of CloudWafServer objects	Origin server configuration of the protected domain name
proxy	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> ● false: No proxy is used. ● true: A proxy is used.
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> ● -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. ● 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
access_code	String	CNAME prefix, CNAME suffix: .vip1.huaweicloudwaf.com
locked	Integer	This parameter is reserved, which will be used to freeze a domain name.
timestamp	Long	Timestamp (ms) when the protected domain name is created.
certificateid	String	HTTPS certificate ID.
certificatename	String	Certificate name

Parameter	Type	Description
tls	String	<p>Minimum TLS version. The value can be TLS v1.0, TLS v1.1, or TLS v1.2. TLS v1.0 is used by default.</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • TLS v1.0 • TLS v1.1 • TLS v1.2
cipher	String	<p>Cipher suite. The value can be cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default: cipher_1: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH</p> <ul style="list-style-type: none"> • cipher_2: ECDH+AESGCM:EDH+AESGCM • cipher_3: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH • cipher_4: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH • cipher_default: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. <p>Enumeration values:</p> <ul style="list-style-type: none"> • cipher_1 • cipher_2 • cipher_3 • cipher_4 • cipher_default
block_page	BlockPage object	Alarm page configuration
extend	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.
traffic_mark	TrafficMark object	Traffic identifier
circuit_breaker	CircuitBreaker object	Circuit breaker configuration

Parameter	Type	Description
lb_algorithm	String	<p>Load balancing algorithms. This parameter is included only in the professional edition (formerly enterprise edition) and platinum edition (formerly premium edition).</p> <ul style="list-style-type: none"> ● Source IP hash: Requests from a certain IP address are forwarded to the same server. ● Weighted round robin: All requests are distributed to origin servers in turn based on the weight assigned to each server. ● Session hash: Requests with a specific session ID are forwarded to the same origin server. Ensure that the traffic identifiers for known attack sources are configured after the domain name was added to WAF. Otherwise, the session hash configuration does not take effect. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● ip_hash ● round_robin ● session_hash
timeout_config	TimeoutConfig object	Timeout settings
web_tag	String	Website name
flag	Flag object	Special identifier, which is used on the console.
description	String	Website remarks
http2_enable	Boolean	<p>Whether to support HTTP/2.</p> <ul style="list-style-type: none"> ● true: HTTP/2 is supported. ● false: HTTP/2 is not supported.
exclusive_ip	Boolean	<p>Whether to use a dedicated IP address. This parameter is reserved and can be ignored.</p> <ul style="list-style-type: none"> ● true: Use a dedicated IP address. ● false: Do not use a dedicated IP address.
access_progress	Array of Access_progress objects	Access progress, which is used only for the new WAF console.

Parameter	Type	Description
forward_header_map	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: <ul style="list-style-type: none"> • \$time_local • \$request_id • \$connection_requests • \$tenant_id • \$project_id • \$remote_addr • \$remote_port • \$scheme • \$request_method • \$http_host • \$origin_uri • \$request_length • \$ssl_server_name • \$ssl_protocol • \$ssl_curves • \$ssl_session_reused

Table 4-917 CloudWafServer

Parameter	Type	Description
front_protocol	String	Protocol used by the client to request access to the origin server. Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
back_protocol	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
weight	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is 1 . This field is not included by cloud WAF.

Parameter	Type	Description
address	String	IP address of your origin server requested by the client
port	Integer	Port used by WAF to forward client requests to the origin server
type	String	Origin server IP address format, IPv4 and IPv6 Enumeration values: <ul style="list-style-type: none"> • ipv4 • ipv6

Table 4-918 BlockPage

Parameter	Type	Description
template	String	Template name
custom_page	CustomPage object	Custom alarm page
redirect_url	String	URL of the redirected page

Table 4-919 CustomPage

Parameter	Type	Description
status_code	String	Status Codes
content_type	String	The content type of the custom alarm page. The value can be text/html , text/xml , or application/json .
content	String	The page content based on the selected page type. For details, see the <i>Web Application Firewall (WAF) User Guide</i> .

Table 4-920 TrafficMark

Parameter	Type	Description
sip	Array of strings	IP tag. HTTP request header field of the original client IP address.

Parameter	Type	Description
cookie	String	Session tag. This tag is used by known attack source rules to block malicious attacks based on cookie attributes. This parameter must be configured in known attack source rules to block requests based on cookie attributes.
params	String	User tag. This tag is used by known attack source rules to block malicious attacks based on params attributes. This parameter must be configured to block requests based on the params attributes.

Table 4-921 CircuitBreaker

Parameter	Type	Description
switch	Boolean	Whether to enable connection protection. <ul style="list-style-type: none"> • true: Enable connection protection. • false: Disable the connection protection.
dead_num	Integer	502/504 error threshold. 502/504 errors allowed for every 30 seconds.
dead_ratio	Number	A breakdown protection is triggered when the 502/504 error threshold and percentage threshold have been reached.
block_time	Integer	Protection period upon the first breakdown. During this period, WAF stops forwarding client requests.
superposition_num	Integer	The maximum multiplier you can use for consecutive breakdowns. The number of breakdowns are counted from 0 every time the accumulated breakdown protection duration reaches 3,600s. For example, assume that Initial Downtime (s) is set to 180s and Multiplier for Consecutive Breakdowns is set to 3. If the breakdown is triggered for the second time, that is, less than 3, the protection duration is 360s (180s X 2). If the breakdown is triggered for the third or fourth time, that is, equal to or greater than 3, the protection duration is 540s (180s X 3). When the accumulated downtime duration exceeds 1 hour (3,600s), the number of breakdowns are counted from 0.

Parameter	Type	Description
suspend_num	Integer	Threshold of the number of pending URL requests. Connection protection is triggered when the threshold has been reached.
sus_block_time	Integer	Downtime duration after the connection protection is triggered. During this period, WAF stops forwarding website requests.

Table 4-922 TimeoutConfig

Parameter	Type	Description
connect_timeout	Integer	Timeout for WAF to connect to the origin server.
send_timeout	Integer	Timeout for WAF to send requests to the origin server.
read_timeout	Integer	Timeout for WAF to receive responses from the origin server.

Table 4-923 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. <ul style="list-style-type: none"> ● true: The website passed the PCI 3DS certification check. ● false: The website failed the PCI 3DS certification check. Enumeration values: <ul style="list-style-type: none"> ● true ● false
pci_dss	String	Whether the website passed the PCI DSS certification check. <ul style="list-style-type: none"> ● true: The website passed the PCI DSS certification check. ● false: The website failed the PCI DSS certification check. Enumeration values: <ul style="list-style-type: none"> ● true ● false

Parameter	Type	Description
cname	String	The CNAME record being used. <ul style="list-style-type: none"> ● old: The old CNAME record is used. ● new: The new CNAME record is used. Enumeration values: <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	Whether WAF support Multi-AZ DR <ul style="list-style-type: none"> ● true: WAF supports multi-AZ DR. ● false: WAF does not support multi-AZ DR. Enumeration values: <ul style="list-style-type: none"> ● true ● false
ipv6	String	Whether IPv6 protection is supported. <ul style="list-style-type: none"> ● true: IPv6 protection is supported. ● false: IPv6 protection is not supported. Enumeration values: <ul style="list-style-type: none"> ● true ● false

Table 4-924 Access_progress

Parameter	Type	Description
step	Integer	Procedure <ul style="list-style-type: none"> ● 1: Whitelisting the WAF IP addresses. ● 2: Testing connectivity. ● 3: Modifying DNS records.
status	Integer	Status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The step has not been finished. ● 1: The step has finished.

Status code: 400

Table 4-925 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Status code: 401

Table 4-926 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-927 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following shows how to obtain details about domain names protected with cloud WAF in a specific project. The project ID is specified by `project_id`, and the domain ID is specified by `instance_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/instance/{instance_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "id": "31af669f567246c289771694f2112289",
  "hostname": "www.demo.com",
  "protocol": "HTTP",
  "server": [ {
    "address": "x.x.x.x",
    "port": 80,
    "type": "ipv4",
    "weight": 1,
    "front_protocol": "HTTP",
    "back_protocol": "HTTP"
  } ],
  "proxy": false,
  "locked": 0,
  "timestamp": 1650527546420,
```

```

"flag" : {
  "pci_3ds" : "false",
  "pci_dss" : "false",
  "ipv6" : "false",
  "cname" : "new",
  "is_dual_az" : "true"
},
"description" : "",
"policyid" : "41cba8aee2e94bcd5f7460874205494",
"domainid" : "d4ecb00b031941ce9171b7bc3386883f",
"projectid" : "0456cf04d6f64725ab02ed5bd2efdfa4",
"enterprise_project_id" : "0",
"protect_status" : 0,
"access_status" : 0,
"access_code" : "1b18879b9d064f8bbcbf8abce7294cac",
"block_page" : {
  "template" : "default"
},
"web_tag" : "",
"exclusive_ip" : false,
"http2_enable" : false
}

```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.13.4 Updating Configurations of Domain Names Protected with Cloud WAF

Function

This API is used to update configurations of domain names protected with cloud WAF. The new origin server information will overwrite the old origin server information. If you want to keep the old information, provide them as new data. You can provide only the updated information in the request body.

URI

PATCH /v1/{project_id}/waf/instance/{instance_id}

Table 4-928 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
instance_id	Yes	String	Domain name ID. It can be obtained by calling the ListHost API.

Table 4-929 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-930 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-931 Request body parameters

Parameter	Mandatory	Type	Description
proxy	No	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> ● false: No proxy is used. ● true: A proxy is used.
certificateid	No	String	Certificate ID. It can be obtained by calling the ListCertificates API. <ul style="list-style-type: none"> ● This parameter is not required when the client protocol is HTTP. ● This parameter is mandatory when the client protocol is HTTPS.
certificatenam e	No	String	Certificate name. <ul style="list-style-type: none"> ● This parameter is not required when the client protocol is HTTP. ● This parameter is mandatory when the client protocol is HTTPS.
server	No	Array of CloudWafServer objects	Origin server configuration of the protected domain name
tls	No	String	Minimum TLS version. The value can be TLS v1.0 , TLS v1.1 , or TLS v1.2 . TLS v1.0 is used by default. Enumeration values: <ul style="list-style-type: none"> ● TLS v1.0 ● TLS v1.1 ● TLS v1.2

Parameter	Mandatory	Type	Description
cipher	No	String	<p>Cipher suite. The value can be cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default:</p> <ul style="list-style-type: none"> cipher_1: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH cipher_2: ECDH+AESGCM:EDH+AESGCM cipher_3: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH cipher_4: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH cipher_default: The cryptographic algorithms are ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:AESGCM. <p>Enumeration values:</p> <ul style="list-style-type: none"> cipher_1 cipher_2 cipher_3 cipher_4 cipher_default
http2_enable	No	Boolean	<p>Whether to support HTTP/2.</p> <ul style="list-style-type: none"> true: HTTP/2 is supported. false: HTTP/2 is not supported.

Parameter	Mandatory	Type	Description
ipv6_enable	No	Boolean	Whether to enable IPv6 protection. Only the professional edition (formerly enterprise edition) and platinum edition (formerly premium edition) support IPv6 protection. <ul style="list-style-type: none"> • true: IPv6 protection is enabled. • false: IPv6 protection is disabled.
web_tag	No	String	Website name
exclusive_ip	No	Boolean	Whether to use a dedicated IP address. This parameter is reserved and can be ignored. <ul style="list-style-type: none"> • true: Use a dedicated IP address. • false: Do not use a dedicated IP address.
paid_type	No	String	Package billing mode. The value can be prePaid or postPaid. prePaid is for yearly/monthly billing. postPaid is for pay-per-use billing. Default value: prePaid.
block_page	No	BlockPage object	Alarm page configuration
traffic_mark	No	TrafficMark object	Traffic identifier
flag	No	Flag object	Special identifier, which is used on the console.
extend	No	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.
circuit_breaker	No	CircuitBreaker object	Circuit breaker configuration
timeout_config	No	TimeoutConfig object	Timeout settings

Parameter	Mandatory	Type	Description
forward_header_map	No	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: <ul style="list-style-type: none"> • \$time_local • \$request_id • \$connection_requests • \$tenant_id • \$project_id • \$remote_addr • \$remote_port • \$scheme • \$request_method • \$http_host • \$origin_uri • \$request_length • \$ssl_server_name • \$ssl_protocol • \$ssl_curves • \$ssl_session_reused

Table 4-932 CloudWafServer

Parameter	Mandatory	Type	Description
front_protocol	Yes	String	Protocol used by the client to request access to the origin server. Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
back_protocol	Yes	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS

Parameter	Mandatory	Type	Description
weight	No	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is 1 . This field is not included by cloud WAF.
address	Yes	String	IP address of your origin server requested by the client
port	Yes	Integer	Port used by WAF to forward client requests to the origin server
type	Yes	String	Origin server IP address format, IPv4 and IPv6 Enumeration values: <ul style="list-style-type: none"> • ipv4 • ipv6

Table 4-933 BlockPage

Parameter	Mandatory	Type	Description
template	Yes	String	Template name
custom_page	No	CustomPage object	Custom alarm page
redirect_url	No	String	URL of the redirected page

Table 4-934 CustomPage

Parameter	Mandatory	Type	Description
status_code	Yes	String	Status Codes
content_type	Yes	String	The content type of the custom alarm page. The value can be text/html , text/xml , or application/json .
content	Yes	String	The page content based on the selected page type. For details, see the <i>Web Application Firewall (WAF) User Guide</i> .

Table 4-935 TrafficMark

Parameter	Mandatory	Type	Description
sip	No	Array of strings	IP tag. HTTP request header field of the original client IP address.
cookie	No	String	Session tag. This tag is used by known attack source rules to block malicious attacks based on cookie attributes. This parameter must be configured in known attack source rules to block requests based on cookie attributes.
params	No	String	User tag. This tag is used by known attack source rules to block malicious attacks based on params attributes. This parameter must be configured to block requests based on the params attributes.

Table 4-936 Flag

Parameter	Mandatory	Type	Description
pci_3ds	No	String	<p>Whether the website passes the PCI 3DS certification check.</p> <ul style="list-style-type: none"> ● true: The website passed the PCI 3DS certification check. ● false: The website failed the PCI 3DS certification check. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false

Parameter	Mandatory	Type	Description
pci_dss	No	String	<p>Whether the website passed the PCI DSS certification check.</p> <ul style="list-style-type: none"> • true: The website passed the PCI DSS certification check. • false: The website failed the PCI DSS certification check. <p>Enumeration values:</p> <ul style="list-style-type: none"> • true • false
cname	No	String	<p>The CNAME record being used.</p> <ul style="list-style-type: none"> • old: The old CNAME record is used. • new: The new CNAME record is used. <p>Enumeration values:</p> <ul style="list-style-type: none"> • old • new
is_dual_az	No	String	<p>Whether WAF support Multi-AZ DR</p> <ul style="list-style-type: none"> • true: WAF supports multi-AZ DR. • false: WAF does not support multi-AZ DR. <p>Enumeration values:</p> <ul style="list-style-type: none"> • true • false
ipv6	No	String	<p>Whether IPv6 protection is supported.</p> <ul style="list-style-type: none"> • true: IPv6 protection is supported. • false: IPv6 protection is not supported. <p>Enumeration values:</p> <ul style="list-style-type: none"> • true • false

Table 4-937 CircuitBreaker

Parameter	Mandatory	Type	Description
switch	No	Boolean	Whether to enable connection protection. <ul style="list-style-type: none"> • true: Enable connection protection. • false: Disable the connection protection.
dead_num	No	Integer	502/504 error threshold. 502/504 errors allowed for every 30 seconds.
dead_ratio	No	Number	A breakdown protection is triggered when the 502/504 error threshold and percentage threshold have been reached.
block_time	No	Integer	Protection period upon the first breakdown. During this period, WAF stops forwarding client requests.
superposition_num	No	Integer	The maximum multiplier you can use for consecutive breakdowns. The number of breakdowns are counted from 0 every time the accumulated breakdown protection duration reaches 3,600s. For example, assume that Initial Downtime (s) is set to 180s and Multiplier for Consecutive Breakdowns is set to 3. If the breakdown is triggered for the second time, that is, less than 3, the protection duration is 360s (180s X 2). If the breakdown is triggered for the third or fourth time, that is, equal to or greater than 3, the protection duration is 540s (180s X 3). When the accumulated downtime duration exceeds 1 hour (3,600s), the number of breakdowns are counted from 0.

Parameter	Mandatory	Type	Description
suspend_num	No	Integer	Threshold of the number of pending URL requests. Connection protection is triggered when the threshold has been reached.
sus_block_time	No	Integer	Downtime duration after the connection protection is triggered. During this period, WAF stops forwarding website requests.

Table 4-938 TimeoutConfig

Parameter	Mandatory	Type	Description
connect_timeout	No	Integer	Timeout for WAF to connect to the origin server.
send_timeout	No	Integer	Timeout for WAF to send requests to the origin server.
read_timeout	No	Integer	Timeout for WAF to receive responses from the origin server.

Response Parameters

Status code: 200

Table 4-939 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name connected to a cloud WAF instance
policyid	String	Policy ID
domainid	String	Account ID.
projectid	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Parameter	Type	Description
enterprise_project_id	String	Enterprise Project ID
protocol	String	Backend protocol type
server	Array of CloudWafServer objects	Origin server configuration of the protected domain name
proxy	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> ● false: No proxy is used. ● true: A proxy is used.
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> ● -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. ● 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
access_code	String	CNAME prefix
locked	Integer	This parameter is reserved, which will be used to freeze a domain name.
timestamp	Long	Time the domain name was added to WAF.
certificateid	String	HTTPS certificate ID.
certificatename	String	Certificate name
tls	String	SSL version Enumeration values: <ul style="list-style-type: none"> ● TLS v1.0 ● TLS v1.1 ● TLS v1.2

Parameter	Type	Description
cipher	String	<p>Cipher suite. The value can be cipher_1, cipher_2, cipher_3, cipher_4, or cipher_default: cipher_1: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH cipher_2: ECDH+AESGCM:EDH+AESGCM cipher_3: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH cipher_4: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH cipher_default: The cryptographic algorithms are ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> ● cipher_1 ● cipher_2 ● cipher_3 ● cipher_4 ● cipher_default
block_page	BlockPage object	Alarm page configuration
extend	Map<String,String>	Special identifier, which is used on the console.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
traffic_mark	TrafficMark object	Traffic identifier
circuit_breaker	CircuitBreaker object	Circuit breaker configuration
lb_algorithm	String	<p>Load balancing algorithm. Weighted round robin is used by default and cannot be changed.</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> ● ip_hash ● round_robin ● session_hash

Parameter	Type	Description
timeout_config	TimeoutConfig object	Timeout settings
flag	Flag object	Special identifier, which is used on the console.
description	String	Domain name description
http2_enable	Boolean	Whether to support HTTP/2. <ul style="list-style-type: none"> ● true: HTTP/2 is supported. ● false: HTTP/2 is not supported.
exclusive_ip	Boolean	Whether to use a dedicated IP address. This parameter is reserved and can be ignored. <ul style="list-style-type: none"> ● true: Use a dedicated IP address. ● false: Do not use a dedicated IP address.
access_progress	Array of Access_progress objects	Access progress, which is used only for the new console (frontend).
forward_header_map	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: <ul style="list-style-type: none"> ● \$time_local ● \$request_id ● \$connection_requests ● \$tenant_id ● \$project_id ● \$remote_addr ● \$remote_port ● \$scheme ● \$request_method ● \$http_host ● \$origin_uri ● \$request_length ● \$ssl_server_name ● \$ssl_protocol ● \$ssl_curves ● \$ssl_session_reused

Table 4-940 CloudWafServer

Parameter	Type	Description
front_protocol	String	Protocol used by the client to request access to the origin server. Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
back_protocol	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
weight	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is 1. This field is not included by cloud WAF.
address	String	IP address of your origin server requested by the client
port	Integer	Port used by WAF to forward client requests to the origin server
type	String	Origin server IP address format, IPv4 and IPv6 Enumeration values: <ul style="list-style-type: none"> • ipv4 • ipv6

Table 4-941 BlockPage

Parameter	Type	Description
template	String	Template name
custom_page	CustomPage object	Custom alarm page
redirect_url	String	URL of the redirected page

Table 4-942 CustomPage

Parameter	Type	Description
status_code	String	Status Codes

Parameter	Type	Description
content_type	String	The content type of the custom alarm page. The value can be text/html , text/xml , or application/json .
content	String	The page content based on the selected page type. For details, see the <i>Web Application Firewall (WAF) User Guide</i> .

Table 4-943 TrafficMark

Parameter	Type	Description
sip	Array of strings	IP tag. HTTP request header field of the original client IP address.
cookie	String	Session tag. This tag is used by known attack source rules to block malicious attacks based on cookie attributes. This parameter must be configured in known attack source rules to block requests based on cookie attributes.
params	String	User tag. This tag is used by known attack source rules to block malicious attacks based on params attributes. This parameter must be configured to block requests based on the params attributes.

Table 4-944 CircuitBreaker

Parameter	Type	Description
switch	Boolean	Whether to enable connection protection. <ul style="list-style-type: none"> • true: Enable connection protection. • false: Disable the connection protection.
dead_num	Integer	502/504 error threshold. 502/504 errors allowed for every 30 seconds.
dead_ratio	Number	A breakdown protection is triggered when the 502/504 error threshold and percentage threshold have been reached.
block_time	Integer	Protection period upon the first breakdown. During this period, WAF stops forwarding client requests.

Parameter	Type	Description
superposition_num	Integer	The maximum multiplier you can use for consecutive breakdowns. The number of breakdowns are counted from 0 every time the accumulated breakdown protection duration reaches 3,600s. For example, assume that Initial Downtime (s) is set to 180s and Multiplier for Consecutive Breakdowns is set to 3. If the breakdown is triggered for the second time, that is, less than 3, the protection duration is 360s (180s X 2). If the breakdown is triggered for the third or fourth time, that is, equal to or greater than 3, the protection duration is 540s (180s X 3). When the accumulated downtime duration exceeds 1 hour (3,600s), the number of breakdowns are counted from 0.
suspend_num	Integer	Threshold of the number of pending URL requests. Connection protection is triggered when the threshold has been reached.
sus_block_time	Integer	Downtime duration after the connection protection is triggered. During this period, WAF stops forwarding website requests.

Table 4-945 TimeoutConfig

Parameter	Type	Description
connect_timeout	Integer	Timeout for WAF to connect to the origin server.
send_timeout	Integer	Timeout for WAF to send requests to the origin server.
read_timeout	Integer	Timeout for WAF to receive responses from the origin server.

Table 4-946 Flag

Parameter	Type	Description
pci_3ds	String	<p>Whether the website passes the PCI 3DS certification check.</p> <ul style="list-style-type: none"> ● true: The website passed the PCI 3DS certification check. ● false: The website failed the PCI 3DS certification check. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
pci_dss	String	<p>Whether the website passed the PCI DSS certification check.</p> <ul style="list-style-type: none"> ● true: The website passed the PCI DSS certification check. ● false: The website failed the PCI DSS certification check. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
cname	String	<p>The CNAME record being used.</p> <ul style="list-style-type: none"> ● old: The old CNAME record is used. ● new: The new CNAME record is used. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	<p>Whether WAF support Multi-AZ DR</p> <ul style="list-style-type: none"> ● true: WAF supports multi-AZ DR. ● false: WAF does not support multi-AZ DR. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false
ipv6	String	<p>Whether IPv6 protection is supported.</p> <ul style="list-style-type: none"> ● true: IPv6 protection is supported. ● false: IPv6 protection is not supported. <p>Enumeration values:</p> <ul style="list-style-type: none"> ● true ● false

Table 4-947 Access_progress

Parameter	Type	Description
step	Integer	Procedure <ul style="list-style-type: none"> • 1: Whitelisting the WAF IP addresses. • 2: Testing connectivity. • 3: Modifying DNS records.
status	Integer	Status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The step has not been finished. • 1: The step has finished.

Status code: 400

Table 4-948 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-949 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-950 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following shows how to update two origin servers in a specific project. The project ID is specified by `project_id`, and domain ID is specified by `instance_id`. The

IP address of the first origin server is x.x.x.x, and the port is 80. The origin server address format is IPv4, and the origin server weight is 1. The client protocol and server protocol are HTTP. The IP address of the second origin server is x.x.x.x, the port is 80, and the origin server address format is IPv4. The client protocol and server protocol are HTTP. IPv6 protection is disabled for the domain name.

```
PATCH https://{Endpoint}/v1/{project_id}/waf/instance/{instance_id}?enterprise_project_id=0

{
  "server": [ {
    "address": "x.x.x.x",
    "port": "80",
    "type": "ipv4",
    "weight": 1,
    "front_protocol": "HTTP",
    "back_protocol": "HTTP"
  }, {
    "front_protocol": "HTTP",
    "back_protocol": "HTTP",
    "type": "ipv4",
    "address": "x.x.x.x",
    "port": "80"
  } ],
  "ipv6_enable": false
}
```

Example Responses

Status code: 200

OK

```
{
  "id": "e91ad96e379b4bea84f8fcd3d153370",
  "hostname": "www.demo.com",
  "protocol": "HTTP",
  "server": [ {
    "address": "x.x.x.x",
    "port": 80,
    "type": "ipv4",
    "weight": 1,
    "front_protocol": "HTTP",
    "back_protocol": "HTTP"
  }, {
    "address": "1.1.1.4",
    "port": 80,
    "type": "ipv4",
    "weight": 1,
    "front_protocol": "HTTP",
    "back_protocol": "HTTP"
  } ],
  "proxy": false,
  "locked": 0,
  "timestamp": 1650423573577,
  "flag": {
    "pci_3ds": "false",
    "pci_dss": "false",
    "ipv6": "false",
    "cname": "new",
    "is_dual_az": "true"
  },
  "description": "",
  "policyid": "f385eceedf7c4c34a4d1def19eafbe85",
  "domainid": "d4ecb00b031941ce9171b7bc3386883f",
  "projectid": "0456cf04d6f64725ab02ed5bd2efdfa4",
  "enterprise_project_id": "0",
  "protect_status": 1,
}
```

```
"access_status" : 0,  
"access_code" : "4f5372610cdc44f7970759fccca138c81",  
"block_page" : {  
  "template" : "default"  
},  
"web_tag" : "we",  
"exclusive_ip" : false,  
"http2_enable" : false  
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.13.5 Deleting a Domain Name from the Cloud WAF

Function

This API is used to delete a domain name from the cloud WAF.

URI

DELETE /v1/{project_id}/waf/instance/{instance_id}

Table 4-951 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
instance_id	Yes	String	Domain name ID. It can be obtained by calling the ListHost API.

Table 4-952 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-953 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-954 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostid	String	Domain name ID
description	String	Description.
type	Integer	WAF deployment mode. The default value is 1. Currently, only the reverse proxy is supported.
proxy	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> false: No proxy is used. true: A proxy is used.
flag	Flag object	Special identifier, which is used on the console.
hostname	String	Domain name added to cloud WAF.
access_code	String	CNAME suffix

Parameter	Type	Description
policyid	String	Policy ID
timestamp	Long	Time the domain name was added to WAF.
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> • -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Access status. <ul style="list-style-type: none"> • 0: The website traffic has not been routed to WAF. (Inaccessible) • 1: The website traffic has been routed to WAF. (Accessible)
exclusive_ip	Boolean	Whether to use a dedicated IP address. This parameter is reserved and can be ignored. <ul style="list-style-type: none"> • true: Use a dedicated IP address. • false: Do not use a dedicated IP address.
paid_type	String	Package billing mode. The value can be prePaid or postPaid. prePaid is for yearly/monthly billing. postPaid is for pay-per-use billing. Default value: prePaid.
web_tag	String	Website name

Table 4-955 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. <ul style="list-style-type: none"> • true: The website passed the PCI 3DS certification check. • false: The website failed the PCI 3DS certification check. Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
pci_dss	String	Whether the website passed the PCI DSS certification check. <ul style="list-style-type: none"> ● true: The website passed the PCI DSS certification check. ● false: The website failed the PCI DSS certification check. Enumeration values: <ul style="list-style-type: none"> ● true ● false
cname	String	The CNAME record being used. <ul style="list-style-type: none"> ● old: The old CNAME record is used. ● new: The new CNAME record is used. Enumeration values: <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	Whether WAF support Multi-AZ DR <ul style="list-style-type: none"> ● true: WAF supports multi-AZ DR. ● false: WAF does not support multi-AZ DR. Enumeration values: <ul style="list-style-type: none"> ● true ● false
ipv6	String	Whether IPv6 protection is supported. <ul style="list-style-type: none"> ● true: IPv6 protection is supported. ● false: IPv6 protection is not supported. Enumeration values: <ul style="list-style-type: none"> ● true ● false

Status code: 400

Table 4-956 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-957 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-958 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
DELETE https://{Endpoint}/v1/{project_id}/waf/instance/{instance_id}?enterprise_project_id=0
```

The following shows how to delete domain names protected with cloud WAF in a specific project. The project ID is specified by `project_id`, and the domain ID is specified by `instance_id`.

Example Responses

Status code: 200

OK

```
{
  "id" : "e91ad96e379b4bea84f8fcda3d153370",
  "hostid" : "e91ad96e379b4bea84f8fcda3d153370",
  "description" : "",
  "type" : 1,
  "proxy" : true,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false",
    "ipv6" : "true",
    "cname" : "new",
    "is_dual_az" : "true"
  },
  "region" : "cn-north-4",
  "hostname" : "www.demo.com",
  "access_code" : "4f5372610cdc44f7970759fcca138c81",
  "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",
  "timestamp" : 1650423573650,
  "protect_status" : 1,
  "access_status" : 0,
  "exclusive_ip" : false,
  "web_tag" : "we",
  "paid_type" : "prePaid"
}
```


Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.13.6 Changing the Protection Status of a Domain Name

Function

This API is used to change the protection status of a domain name.

URI

PUT /v1/{project_id}/waf/instance/{instance_id}/protect-status

Table 4-959 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
instance_id	Yes	String	Domain name ID. This parameter is used to specify the domain name whose protection status you want to modify. You can obtain the domain name ID by calling the API (ListHost) for querying the list of domain names protected with cloud WAF.

Table 4-960 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-961 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-962 Request body parameters

Parameter	Mandatory	Type	Description
protect_status	Yes	Integer	WAF status of the protected domain name. <ul style="list-style-type: none">• -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF.• 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks.• 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.

Response Parameters

Status code: 200

Table 4-963 Response body parameters

Parameter	Type	Description
protect_status	Integer	<p>WAF status of the protected domain name.</p> <ul style="list-style-type: none"> • -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.

Status code: 400

Table 4-964 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-965 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-966 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following shows how to change WAF protection to suspended for a domain name in a specific project. The project ID is specified by `project_id`, and the domain ID is specified by `instance_id`.

```
PUT https://{Endpoint}/v1/{project_id}/waf/instance/{instance_id}/protect-status?enterprise_project_id=0
{
  "protect_status" : 0
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "protect_status" : 0
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.13.7 Obtaining Domain Name Routing Information (in Cloud Mode)

Function

This API is used to obtain the domain name routes.

 **NOTE**

This API is restricted at some sites and will be brought offline later.

URI

GET `/v1/{project_id}/waf/instance/{instance_id}/route`

Table 4-967 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
instance_id	Yes	String	Domain name ID. It can be obtained by calling the ListHost API.

Table 4-968 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-969 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-970 Response body parameters

Parameter	Type	Description
total	Integer	Number of routes
items	Array of RouteBody objects	Route list

Table 4-971 RouteBody

Parameter	Type	Description
cname	String	CNAME suffix of the WAF cluster
name	String	Name of the WAF cluster
servers	Array of RouteServerBody objects	Origin server information list of the protected domain name

Table 4-972 RouteServerBody

Parameter	Type	Description
back_protocol	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: <ul style="list-style-type: none"> • HTTP • HTTPS
address	String	IP address of your origin server requested by the client
port	Integer	Port used by WAF to forward client requests to the origin server

Status code: 400

Table 4-973 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-974 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-975 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following shows how to obtain routes of domain names protected with cloud WAF in a specific project. The project ID is specified by `project_id`, and the domain ID is specified by `instance_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/instance/{instance_id}/route?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total": 1,
  "items": [ {
    "cname": "e9d30fda6xxxxxxxxxxxx5b3d3286",
    "name": "Beijing",
    "servers": [ {
      "back_protocol": "HTTP",
      "address": "x.x.x.x",
      "port": 80
    } ]
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.

Status Code	Description
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.14 Querying the Domain Name of a Tenant

4.14.1 Querying Domain Names Protected with All WAF Instances

Function

This API is used to query the list of protection domain names.

URI

GET /v1/{project_id}/composite-waf/host

Table 4-976 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-977 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS. If you use the default enterprise project, set this parameter to 0 . Default value: 0
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned. Default: 1
pagesize	No	Integer	Number of results on each page in query pagination. The value range is 1 to 100. The default value is 10 , indicating that each page contains 10 results. To query all domain names at a time, set this parameter to -1 . Default: 10
hostname	No	String	Domain name
policyname	No	String	Policy name
protect_status	No	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> • -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
waf_type	No	String	WAF mode of the domain name

Parameter	Mandatory	Type	Description
is_https	No	Boolean	Whether HTTPS is used for the domain name

Request Parameters

Table 4-978 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-979 Response body parameters

Parameter	Type	Description
total	Integer	Number of all protected domain names
cloud_total	Integer	Number of domain names protected with cloud WAF
premium_total	Integer	Number of domain names protected with dedicated WAF instances
items	Array of CompositeHostResponse objects	Details about the protected domain name

Table 4-980 CompositeHostResponse

Parameter	Type	Description
id	String	Domain name ID
hostid	String	Domain name ID

Parameter	Type	Description
hostname	String	Domain name added to cloud WAF.
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> • -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
proxy	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> • false: No proxy is used. • true: A proxy is used.
timestamp	Long	Time the domain name was added to WAF.
paid_type	String	Package billing mode. The value can be prePaid or postPaid. prePaid is for yearly/monthly billing. postPaid is for pay-per-use billing. Default value: prePaid.
flag	Flag object	Special identifier, which is used on the console.
waf_type	String	Mode of WAF that is used to protection the domain name. The value can be cloud or premium . cloud : The cloud WAF is used to protect the domain. premium : A dedicated WAF instance is used to protect the domain name.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
access_progress	Array of Access_progress objects	Access progress, which is used only for the new WAF console.

Parameter	Type	Description
premium_waf_instances	Array of Premium_waf_instances objects	List of dedicated WAF instances
description	String	Domain name description
exclusive_ip	Boolean	Whether to use a dedicated IP address. This parameter is reserved and can be ignored. <ul style="list-style-type: none"> ● true: Use a dedicated IP address. ● false: Do not use a dedicated IP address.
region	String	Region ID. This parameter is included when the domain name was added to WAF through the console. This parameter is left blank when the domain name was added to WAF by calling an API. You can query the region ID on the Regions and Endpoints page on the website.

Table 4-981 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. <ul style="list-style-type: none"> ● true: The website passed the PCI 3DS certification check. ● false: The website failed the PCI 3DS certification check. Enumeration values: <ul style="list-style-type: none"> ● true ● false
pci_dss	String	Whether the website passed the PCI DSS certification check. <ul style="list-style-type: none"> ● true: The website passed the PCI DSS certification check. ● false: The website failed the PCI DSS certification check. Enumeration values: <ul style="list-style-type: none"> ● true ● false

Parameter	Type	Description
cname	String	The CNAME record being used. <ul style="list-style-type: none"> ● old: The old CNAME record is used. ● new: The new CNAME record is used. Enumeration values: <ul style="list-style-type: none"> ● old ● new
is_dual_az	String	Whether WAF support Multi-AZ DR <ul style="list-style-type: none"> ● true: WAF supports multi-AZ DR. ● false: WAF does not support multi-AZ DR. Enumeration values: <ul style="list-style-type: none"> ● true ● false
ipv6	String	Whether IPv6 protection is supported. <ul style="list-style-type: none"> ● true: IPv6 protection is supported. ● false: IPv6 protection is not supported. Enumeration values: <ul style="list-style-type: none"> ● true ● false

Table 4-982 Access_progress

Parameter	Type	Description
step	Integer	Procedure <ul style="list-style-type: none"> ● 1: Whitelisting the WAF IP addresses. ● 2: Testing connectivity. ● 3: Modifying DNS records.
status	Integer	Status. The value can be 0 or 1 . <ul style="list-style-type: none"> ● 0: The step has not been finished. ● 1: The step has finished.

Table 4-983 Premium_waf_instances

Parameter	Type	Description
id	String	ID of the dedicated WAF instance
name	String	Name of the dedicated WAF instance

Parameter	Type	Description
accessed	Boolean	Whether the domain name is added to the dedicated WAF instance. The options are true and false . <ul style="list-style-type: none">• true: The domain name has been added to WAF.• false: The domain name has not been added to WAF.

Status code: 400**Table 4-984** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401**Table 4-985** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500**Table 4-986** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the protected domain name list in a project. The project ID is specified by `project_id`.

```
GET https://{Endpoint}/v1/{project_id}/composite-waf/host?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "items" : [ {
    "id" : "31af669f567246c289771694f2112289",
    "hostid" : "31af669f567246c289771694f2112289",
    "description" : "",
    "proxy" : false,
    "flag" : {
      "pci_3ds" : "false",
      "pci_dss" : "false",
      "ipv6" : "false",
      "cname" : "new",
      "is_dual_az" : "true"
    },
    "region" : "cn-north-4",
    "hostname" : "www.demo.com",
    "access_code" : "1b18879b9d064f8bbcbf8abce7294cac",
    "policyid" : "41cba8aee2e94bcd57460874205494",
    "timestamp" : 1650527546454,
    "protect_status" : 0,
    "access_status" : 0,
    "exclusive_ip" : false,
    "web_tag" : "",
    "paid_type" : "prePaid",
    "waf_type" : "cloud"
  } ],
  "total" : 1,
  "cloud_total" : 1,
  "premium_total" : 0
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.14.2 Querying a Domain Name by ID

Function

This API is used to query a protected domain name by ID.

URI

GET /v1/{project_id}/composite-waf/host/{host_id}

Table 4-987 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
host_id	Yes	String	Domain name ID. In the cloud mode, it can be obtained by calling the ListHost API. In the dedicated mode, it can be obtained by calling the ListPremiumHost API.

Table 4-988 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-989 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json; charset=utf8

Response Parameters

Status code: 200

Table 4-990 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostid	String	Domain name ID
hostname	String	Domain name added to cloud WAF.
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	WAF status of the protected domain name. <ul style="list-style-type: none"> • -1: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. • 0: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. • 1: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be 0 or 1 . 0 : The website traffic has not been routed to WAF. 1 : The website traffic has been routed to WAF.
proxy	Boolean	Whether a proxy is used for the protected domain name. <ul style="list-style-type: none"> • false: No proxy is used. • true: A proxy is used.
timestamp	Long	Time the domain name was added to WAF.
paid_type	String	Package billing mode. The value can be prePaid or postPaid. prePaid is for yearly/monthly billing. postPaid is for pay-per-use billing. Default value: prePaid.
flag	Flag object	Special identifier, which is used on the console.
waf_type	String	Mode of WAF that is used to protection the domain name. The value can be cloud or premium . cloud : The cloud WAF is used to protect the domain. premium : A dedicated WAF instance is used to protect the domain name.

Parameter	Type	Description
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
access_progress	Array of Access_progress objects	Access progress, which is used only for the new WAF console.
premium_waf_instances	Array of Premium_waf_instances objects	List of dedicated WAF instances
description	String	Domain name description
exclusive_ip	Boolean	Whether to use a dedicated IP address. This parameter is reserved and can be ignored. <ul style="list-style-type: none"> • true: Use a dedicated IP address. • false: Do not use a dedicated IP address.
region	String	Region ID. This parameter is included when the domain name was added to WAF through the console. This parameter is left blank when the domain name was added to WAF by calling an API. You can query the region ID on the Regions and Endpoints page on the website.

Table 4-991 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. <ul style="list-style-type: none"> • true: The website passed the PCI 3DS certification check. • false: The website failed the PCI 3DS certification check. Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
pci_dss	String	Whether the website passed the PCI DSS certification check. <ul style="list-style-type: none"> • true: The website passed the PCI DSS certification check. • false: The website failed the PCI DSS certification check. Enumeration values: <ul style="list-style-type: none"> • true • false
cname	String	The CNAME record being used. <ul style="list-style-type: none"> • old: The old CNAME record is used. • new: The new CNAME record is used. Enumeration values: <ul style="list-style-type: none"> • old • new
is_dual_az	String	Whether WAF support Multi-AZ DR <ul style="list-style-type: none"> • true: WAF supports multi-AZ DR. • false: WAF does not support multi-AZ DR. Enumeration values: <ul style="list-style-type: none"> • true • false
ipv6	String	Whether IPv6 protection is supported. <ul style="list-style-type: none"> • true: IPv6 protection is supported. • false: IPv6 protection is not supported. Enumeration values: <ul style="list-style-type: none"> • true • false

Table 4-992 Access_progress

Parameter	Type	Description
step	Integer	Procedure <ul style="list-style-type: none"> • 1: Whitelisting the WAF IP addresses. • 2: Testing connectivity. • 3: Modifying DNS records.

Parameter	Type	Description
status	Integer	Status. The value can be 0 or 1 . <ul style="list-style-type: none"> • 0: The step has not been finished. • 1: The step has finished.

Table 4-993 Premium_waf_instances

Parameter	Type	Description
id	String	ID of the dedicated WAF instance
name	String	Name of the dedicated WAF instance
accessed	Boolean	Whether the domain name is added to the dedicated WAF instance. The options are true and false . <ul style="list-style-type: none"> • true: The domain name has been added to WAF. • false: The domain name has not been added to WAF.

Status code: 400

Table 4-994 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-995 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-996 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following shows how to obtain details about a domain name. The project ID is specified by `project_id`, and the domain ID is specified by `host_id`.

```
GET https://{Endpoint}/v1/{project_id}/composite-waf/host/{host_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "id" : "31af669f567246c289771694f2112289",
  "hostid" : "31af669f567246c289771694f2112289",
  "description" : "",
  "proxy" : false,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false",
    "ipv6" : "false",
    "cname" : "new",
    "is_dual_az" : "true"
  },
  "region" : "cn-north-4",
  "hostname" : "www.demo.com",
  "access_code" : "1b18879b9d064f8bbcbf8abce7294cac",
  "policyid" : "41cba8aee2e94bcdcf57460874205494",
  "timestamp" : 1650527546454,
  "protect_status" : 0,
  "access_status" : 0,
  "exclusive_ip" : false,
  "web_tag" : "",
  "paid_type" : "prePaid",
  "waf_type" : "cloud"
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.15 Querying Features Available at a Site

4.15.1 Querying Features Available at a Site

Function

This API is used to query the features available at specific site.

URI

GET /v1/{project_id}/waf/config/console

Table 4-997 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Request Parameters

Table 4-998 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json; charset=utf8

Response Parameters

Status code: 200

Table 4-999 Response body parameters

Parameter	Type	Description
eps	Boolean	Whether EPS is supported. The options are false and true . <ul style="list-style-type: none"> • True: EPS is supported. • false: EPS is not supported.
tls	Boolean	Whether to support the TLS version. The value can be true or false . If you set it to true , you can configure TLS v1.0, TLS v1.1, or TLS v1.2. The default value is TLS v1.0 . <ul style="list-style-type: none"> • True: TLS version is supported. • false: TLS version is not supported.
ipv6	Boolean	Whether IPv6 protection is supported. The options are false and true . <ul style="list-style-type: none"> • True: IPv6 protection is supported. • false: IPv6 protection is not supported.
alert	Boolean	Whether alarm reporting is supported. The options are false and true . <ul style="list-style-type: none"> • True: Alarm reporting is supported. • false: Alarm reporting is not supported.
custom	Boolean	Whether precise protection is supported. The options are false and true . <ul style="list-style-type: none"> • True: Precise protection is supported. • false: Precise protection is not supported.
elb_mode	Boolean	Whether ELB mode is supported. The options are false and true . <ul style="list-style-type: none"> • True: The ELB mode is supported. • false: The ELB mode is not supported.
event_lts	Boolean	Whether LTS logging is supported. The options are false and true . <ul style="list-style-type: none"> • True: LTS logging is supported. • false: LTS logging is not supported.
multi_dns	Boolean	Whether multi-DNS resolution is supported. The options are false and true . <ul style="list-style-type: none"> • True: The multi-DNS resolution is supported. • false: The multi-DNS resolution is not supported.

Parameter	Type	Description
search_ip	Boolean	Whether IP address search is supported. The options are false and true . <ul style="list-style-type: none"> • True: IP address search is supported. • false: IP address search is not supported.
cc_enhance	Boolean	Whether CC attack protection is supported. The options are false and true . <ul style="list-style-type: none"> • True: CC attack protection is supported. • false: CC attack protection is not supported.
cname_switch	Boolean	Whether CNAME switchover is supported. The options are false and true . <ul style="list-style-type: none"> • True: CNAME switchover is supported. • false: CNAME switchover is not supported.
custom_block	Boolean	Whether custom block page is supported. The options are false and true . <ul style="list-style-type: none"> • True: The custom block page is supported. • false: The custom block page is not supported.
advanced_ignore	Boolean	Whether false alarm masking is supported. The options are false and true . <ul style="list-style-type: none"> • True: The false alarm masking is supported. • false: The false alarm masking is not supported.
js_crawler_enable	Boolean	Whether JavaScript-based anti-crawler is supported. The options are false and true . <ul style="list-style-type: none"> • True: The JavaScript-based anti-crawler is supported. • false: The JavaScript-based anti-crawler is not supported.
deep_decode_enable	Boolean	Whether deep inspection in basic web protection is supported. The options are false and true . <ul style="list-style-type: none"> • True: The deep inspection is supported. • false: The deep inspection is not supported.
overview_bandwidth	Boolean	Whether in-depth resolution is supported. The options are false and true . <ul style="list-style-type: none"> • True: The in-depth resolution is supported. • false: The in-depth resolution is not supported.

Parameter	Type	Description
proxy_use_old_cname	Boolean	Whether old CNAME resolution is supported. The options are false and true . <ul style="list-style-type: none"> • True: The old CNAME resolution is supported. • false: The old CNAME resolution is not supported.
check_all_headers_enable	Boolean	Whether header inspection is supported. The options are false and true . <ul style="list-style-type: none"> • True: The header inspection is supported. • false: The header inspection is not supported.
geoip_enable	Boolean	Whether to support geolocation access control. The options are false: not supported; true: supported.
load_balance_enable	Boolean	Whether to support domain name access load balancing. The options are false: not supported; true: supported.
ipv6_protection_enable	Boolean	Whether IPv6 defense is supported. The options are false: not supported; true: supported.
policy_sharing_enable	Boolean	Whether to support policy sharing. The options are false: not supported; true: supported.
ip_group	Boolean	Whether the IP address group is supported. The options are false: not supported; true: supported.
robot_action_enable	Boolean	Whether to support website anti-crawler. The options are false: not supported; true: supported.
http2_enable	Boolean	Whether to support HTTP2. The options are false: not supported; true: supported.
timeout_config_enable	Boolean	Whether to support the timeout configuration. The options are false: not supported; true: supported.

Status code: 400

Table 4-1000 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Status code: 401

Table 4-1001 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-1002 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query the features enabled at a site. The project ID is specified by project_id and the time is from 2022-04-21 00:00:00 to 2022-04-21 14:45:20.

```
GET https://{Endpoint}/v1/{project_id}/waf/config/console?
enterprise_project_id=0&from=1650470400089&to=1650523520089
```

Example Responses

Status code: 200

OK

```
{
  "eps" : true,
  "tls" : true,
  "ipv6" : true,
  "alert" : true,
  "custom" : true,
  "ip_group" : true,
  "event_lts" : true,
  "multi_dns" : true,
  "search_ip" : true,
  "cc_enhance" : true,
  "cname_switch" : true,
  "custom_block" : true,
  "geoip_enable" : true,
```

```
"http2_enable" : true,  
"advanced_ignore" : true,  
"js_crawler_enable" : true,  
"deep_decode_enable" : true,  
"overview_bandwidth" : true,  
"proxy_use_oldcname" : false,  
"load_balance_enable" : true,  
"robot_action_enable" : true,  
"policy_sharing_enable" : true,  
"timeout_config_enable" : true,  
"ipv6_protection_enable" : true,  
"check_all_headers_enable" : true,  
"elb_mode" : true  
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.16 Policy management

4.16.1 Querying the Protection Policy List

Function

This API is used to query the protection policy list.

URI

GET /v1/{project_id}/waf/policy

Table 4-1003 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-1004 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is 1 , indicating that the data on the first page is returned. Default: 1
pagesize	No	Integer	Number of results on each page during pagination query. Value range: 1 to 100 . The default value is 10 , indicating that each page contains 10 results. Default: 10
name	No	String	Policy name

Request Parameters

Table 4-1005 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-1006 Response body parameters

Parameter	Type	Description
total	Integer	Total number of policies
items	Array of PolicyResponse objects	Array of protection policy information

Table 4-1007 PolicyResponse

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies
level	Integer	<p>Protection level of basic web protection</p> <ul style="list-style-type: none"> • 1: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, Low is recommended. • 2: Medium. This protection level meets web protection requirements in most scenarios. • 3: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. <p>Default: 2</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • 1 • 2 • 3

Parameter	Type	Description
full_detection	Boolean	The detection mode in Precise Protection. <ul style="list-style-type: none"> ● false: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. ● true: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	Action object	Protective actions for each rule in anti-crawler protection.
action	PolicyAction object	Protective action
options	PolicyOption object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String, Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	Array of strings	Array of domain name IDs protected by the policy.
bind_host	Array of BindHost objects	Array of domain names protected with the protection policy. Compared with the hosts field, this field contains more details.
extend	Map<String, String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-1008 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: <ul style="list-style-type: none"> ● log: WAF only logs discovered attacks. ● block: WAF blocks discovered attacks.

Table 4-1009 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be log or block . log : WAF only logs discovered attacks. block : WAF blocks discovered attacks. Enumeration values: <ul style="list-style-type: none"> • block • log

Table 4-1010 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
common	Boolean	Whether general check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at true . You can ignore this parameter. Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
webshell	Boolean	Whether webshell detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: <ul style="list-style-type: none"> • true • false
custom	Boolean	Whether precise protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
privacy	Boolean	Whether data masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: <ul style="list-style-type: none"> • true • false

Table 4-1011 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-1012 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-1013 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-1014 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to obtain the policy list in a project. The project ID is specified by `project_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total": 1,
  "items": [ {
    "id": "41cba8aee2e94bcdbf57460874205494",
    "name": "policy_2FHwFOKz",
    "level": 2,
    "action": {
      "category": "log"
    },
  },
  "options": {
    "webattack": true,
    "common": true,
```

```

"crawler" : true,
"crawler_engine" : false,
"crawler_scanner" : true,
"crawler_script" : false,
"crawler_other" : false,
"webshell" : false,
"cc" : true,
"custom" : true,
"whiteblackip" : true,
"geoup" : true,
"ignore" : true,
"privacy" : true,
"antitamper" : true,
"antileakage" : false,
"bot_enable" : true,
"modulex_enabled" : false
},
"hosts" : [ ],
"extend" : { },
"timestamp" : 1650527546218,
"full_detection" : false,
"bind_host" : [ ]
}]
}

```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.16.2 Creating a Protection Policy

Function

This API is used to create a protection policy. The system configures some default configuration items when generating the policy. To modify the default configuration items, call the API for updating the protection policy.

URI

POST /v1/{project_id}/waf/policy

Table 4-1015 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Table 4-1016 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-1017 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-1018 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Array of details of policies

Response Parameters

Status code: 200

Table 4-1019 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies
level	Integer	<p>Protection level of basic web protection</p> <ul style="list-style-type: none"> • 1: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, Low is recommended. • 2: Medium. This protection level meets web protection requirements in most scenarios. • 3: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. <p>Default: 2</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • 1 • 2 • 3
full_detection	Boolean	<p>The detection mode in Precise Protection.</p> <ul style="list-style-type: none"> • false: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. • true: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	Action object	Protective actions for each rule in anti-crawler protection.
action	PolicyAction object	Protective action
options	PolicyOption object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String, Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.

Parameter	Type	Description
hosts	Array of strings	Array of domain name IDs protected by the policy.
bind_host	Array of BindHost objects	Array of domain names protected with the protection policy. Compared with the hosts field, this field contains more details.
extend	Map<String,String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-1020 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: <ul style="list-style-type: none"> ● log: WAF only logs discovered attacks. ● block: WAF blocks discovered attacks.

Table 4-1021 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be log or block . log : WAF only logs discovered attacks. block : WAF blocks discovered attacks. Enumeration values: <ul style="list-style-type: none"> ● block ● log

Table 4-1022 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: <ul style="list-style-type: none"> ● true ● false

Parameter	Type	Description
common	Boolean	Whether general check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at true . You can ignore this parameter. Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
webshell	Boolean	Whether webshell detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
custom	Boolean	Whether precise protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
privacy	Boolean	Whether data masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: <ul style="list-style-type: none">• true• false

Table 4-1023 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400**Table 4-1024** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401**Table 4-1025** Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 403

Table 4-1026 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-1027 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to create a protection policy named demo in a specific project. The project ID is specified by project_id.

```
POST https://{Endpoint}/v1/{project_id}/waf/policy?enterprise_project_id=0
{
  "name": "demo"
}
```

Example Responses

Status code: 200

OK

```
{
  "id": "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name": "demo",
  "level": 2,
  "action": {
    "category": "log"
  },
  "options": {
    "webattack": true,
    "common": true,
    "crawler": true,
    "crawler_engine": false,
    "crawler_scanner": true,
    "crawler_script": false,
    "crawler_other": false,
    "webshell": false,
    "cc": true,
    "custom": true,
    "whiteblackip": true,
    "geoip": true,
    "ignore": true,
    "privacy": true,
    "antitamper": true,
    "antileakage": false,
  }
}
```

```

"bot_enable" : true,
"modulex_enabled" : false
},
"hosts" : [ ],
"extend" : { },
"timestamp" : 1650529538732,
"full_detection" : false,
"bind_host" : [ ]
}

```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
403	The resource quota is insufficient.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.16.3 Querying a Policy by ID

Function

This API is used to query a policy by ID.

URI

GET /v1/{project_id}/waf/policy/{policy_id}

Table 4-1028 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-1029 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-1030 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-1031 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies

Parameter	Type	Description
level	Integer	<p>Protection level of basic web protection</p> <ul style="list-style-type: none"> • 1: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, Low is recommended. • 2: Medium. This protection level meets web protection requirements in most scenarios. • 3: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. <p>Default: 2</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • 1 • 2 • 3
full_detection	Boolean	<p>The detection mode in Precise Protection.</p> <ul style="list-style-type: none"> • false: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. • true: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	Action object	Protective actions for each rule in anti-crawler protection.
action	PolicyAction object	Protective action
options	PolicyOption object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String, Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	Array of strings	Array of domain name IDs protected by the policy.

Parameter	Type	Description
bind_host	Array of BindHost objects	Array of domain names protected with the protection policy. Compared with the hosts field, this field contains more details.
extend	Map<String,String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-1032 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: <ul style="list-style-type: none"> • log: WAF only logs discovered attacks. • block: WAF blocks discovered attacks.

Table 4-1033 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be log or block . log : WAF only logs discovered attacks. block : WAF blocks discovered attacks. Enumeration values: <ul style="list-style-type: none"> • block • log

Table 4-1034 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
common	Boolean	Whether general check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at true . You can ignore this parameter. Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
webshell	Boolean	Whether webshell detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: <ul style="list-style-type: none"> • true • false
custom	Boolean	Whether precise protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
privacy	Boolean	Whether data masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: <ul style="list-style-type: none"> • true • false

Table 4-1035 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-1036 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-1037 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-1038 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to query details about a protection policy in a specific project. The project is specified by `project_id`, and the policy is specified by `policy_id`.

```
GET https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "whiteblackip" : true,
    "geoup" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "antileakage" : false,
    "bot_enable" : true,
    "modulex_enabled" : false
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ ]
}
```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.16.4 Updating a Protection Policy

Function

This API is used to update a policy. The request body can contain only the part to be updated.

URI

PATCH /v1/{project_id}/waf/policy/{policy_id}

Table 4-1039 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-1040 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-1041 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Table 4-1042 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Array of details of policies
level	No	Integer	<p>Protection level of basic web protection</p> <ul style="list-style-type: none"> • 1: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, Low is recommended. • 2: Medium. This protection level meets web protection requirements in most scenarios. • 3: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. <p>Default: 2</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • 1 • 2 • 3

Parameter	Mandatory	Type	Description
full_detection	No	Boolean	<p>The detection mode in Precise Protection.</p> <ul style="list-style-type: none"> • false: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. • true: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	No	Action object	Protective actions for each rule in anti-crawler protection.
action	No	PolicyAction object	Protective action
options	No	PolicyOption object	Whether a protection type is enabled in protection policy.
modulex_options	No	Map<String, Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	No	Array of strings	Array of domain name IDs protected by the policy. This parameter cannot be edited and is reserved for extended functions. You can ignore it.
bind_host	No	Array of BindHost objects	Array of domain names protected with the protection policy. Compared with the hosts field, this field contains more details. This parameter cannot be edited and is reserved for extended functions. You can ignore it.

Parameter	Mandatory	Type	Description
extend	No	Map<String,String>	<p>Extended field, which is used to store the basic web protection settings.</p> <ul style="list-style-type: none"> • deep_decode: Deep inspection status. • check_all_headers: Header inspection status. • shiro_rememberMe_enable: Shiro decryption check status.

Table 4-1043 Action

Parameter	Mandatory	Type	Description
category	No	String	<p>Protective action for feature-based anti-crawler rules:</p> <ul style="list-style-type: none"> • log: WAF only logs discovered attacks. • block: WAF blocks discovered attacks.

Table 4-1044 PolicyAction

Parameter	Mandatory	Type	Description
category	No	String	<p>Basic web protection action. The value can be log or block. log: WAF only logs discovered attacks. block: WAF blocks discovered attacks.</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • block • log

Table 4-1045 PolicyOption

Parameter	Mandatory	Type	Description
webattack	No	Boolean	Whether basic web protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
common	No	Boolean	Whether general check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler	No	Boolean	This parameter is reserved. The value of this parameter is fixed at true . You can ignore this parameter. Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_engine	No	Boolean	Whether the search engine is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_scanner	No	Boolean	Whether the anti-crawler detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_script	No	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_other	No	Boolean	Whether other crawler check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Mandatory	Type	Description
webshell	No	Boolean	Whether webshell detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
cc	No	Boolean	Whether the CC attack protection rules are enabled Enumeration values: <ul style="list-style-type: none"> • true • false
custom	No	Boolean	Whether precise protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
whiteblackip	No	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
geoip	No	Boolean	Whether geolocation access control is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
ignore	No	Boolean	Whether false alarm masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
privacy	No	Boolean	Whether data masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Mandatory	Type	Description
antitamper	No	Boolean	Whether the web tamper protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antileakage	No	Boolean	Whether the information leakage prevention is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
bot_enable	No	Boolean	Whether the anti-crawler protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
modulex_enabled	No	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: <ul style="list-style-type: none"> • true • false

Table 4-1046 BindHost

Parameter	Mandatory	Type	Description
id	No	String	Domain name ID
hostname	No	String	Domain name
waf_type	No	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	No	String	This parameter is required only by the dedicated mode.

Response Parameters

Status code: 200

Table 4-1047 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies
level	Integer	<p>Protection level of basic web protection</p> <ul style="list-style-type: none"> • 1: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, Low is recommended. • 2: Medium. This protection level meets web protection requirements in most scenarios. • 3: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. <p>Default: 2</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • 1 • 2 • 3
full_detection	Boolean	<p>The detection mode in Precise Protection.</p> <ul style="list-style-type: none"> • false: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. • true: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	Action object	Protective actions for each rule in anti-crawler protection.
action	PolicyAction object	Protective action
options	PolicyOption object	Whether a protection type is enabled in protection policy.

Parameter	Type	Description
modulex_options	Map<String, Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	Array of strings	Array of domain name IDs protected by the policy.
bind_host	Array of BindHost objects	Array of domain names protected with the protection policy. Compared with the hosts field, this field contains more details.
extend	Map<String, String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-1048 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: <ul style="list-style-type: none"> • log: WAF only logs discovered attacks. • block: WAF blocks discovered attacks.

Table 4-1049 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be log or block . log : WAF only logs discovered attacks. block : WAF blocks discovered attacks. Enumeration values: <ul style="list-style-type: none"> • block • log

Table 4-1050 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
common	Boolean	Whether general check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at true . You can ignore this parameter. Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
webshell	Boolean	Whether webshell detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
custom	Boolean	Whether precise protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
privacy	Boolean	Whether data masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: <ul style="list-style-type: none"> • true • false

Table 4-1051 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-1052 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-1053 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-1054 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

- The following example shows how to modify basic web protection settings, including enabling deep inspection, header inspection, and Shiro decryption check, for a specific policy in a project. The project is specified by `project_id`, and the policy is specified by `policy_id`.

```
PATCH https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?enterprise_project_id=0
{
  "extend" : {
    "extend" : "{\"deep_decode\":true,\"check_all_headers\":true,\"shiro_rememberMe_enable\":true}"
  }
}
```

- The following example shows how to disable whitelist and blacklist protection for a specific policy in a project. The project is specified by `project_id`, and the policy is specified by `policy_id`.

```
PATCH https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?enterprise_project_id=0
{
  "options" : {
    "whiteblackip" : false
  }
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "whiteblackip" : false,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
  }
}
```

```

"antileakage" : false,
"bot_enable" : true
},
"hosts" : [ "c0268b883a854adc8a2cd352193b0e13" ],
"timestamp" : 1650529538732,
"full_detection" : false,
"bind_host" : [ {
  "id" : "c0268b883a854adc8a2cd352193b0e13",
  "hostname" : "www.demo.com",
  "waf_type" : "cloud"
} ]
}

```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.16.5 Deleting a Protection Policy

Function

This API is used to delete a protection policy. If the policy is in use, unbind the domain name from the policy before deleting the policy.

URI

DELETE /v1/{project_id}/waf/policy/{policy_id}

Table 4-1055 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-1056 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the ListEnterpriseProject API of EPS.

Request Parameters

Table 4-1057 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-1058 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies

Parameter	Type	Description
level	Integer	<p>Protection level of basic web protection</p> <ul style="list-style-type: none"> • 1: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, Low is recommended. • 2: Medium. This protection level meets web protection requirements in most scenarios. • 3: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. <p>Default: 2</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • 1 • 2 • 3
full_detection	Boolean	<p>The detection mode in Precise Protection.</p> <ul style="list-style-type: none"> • false: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. • true: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	Action object	Protective actions for each rule in anti-crawler protection.
action	PolicyAction object	Protective action
options	PolicyOption object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String, Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	Array of strings	Array of domain name IDs protected by the policy.

Parameter	Type	Description
bind_host	Array of BindHost objects	Array of domain names protected with the protection policy. Compared with the hosts field, this field contains more details.
extend	Map<String,String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-1059 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: <ul style="list-style-type: none"> • log: WAF only logs discovered attacks. • block: WAF blocks discovered attacks.

Table 4-1060 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be log or block . log : WAF only logs discovered attacks. block : WAF blocks discovered attacks. Enumeration values: <ul style="list-style-type: none"> • block • log

Table 4-1061 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
common	Boolean	Whether general check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at true . You can ignore this parameter. Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
webshell	Boolean	Whether webshell detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: <ul style="list-style-type: none"> • true • false
custom	Boolean	Whether precise protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
privacy	Boolean	Whether data masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: <ul style="list-style-type: none"> • true • false

Table 4-1062 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-1063 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-1064 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-1065 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to delete a protection policy in a specific project. The project is specified by `project_id`, and the policy is specified by `policy_id`.

```
DELETE https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "62169e2fc4e64148b775ec01b24a1947",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log",
    "modulex_category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true,
    "modulex_enabled" : false
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1649316510603,
  "full_detection" : false,
  "bind_host" : [ ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.16.6 Updating the Domain Name Protection Policy

Function

This API is used to update protection policy applied to a domain name.

URI

PUT /v1/{project_id}/waf/policy/{policy_id}

Table 4-1066 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose My Credentials . Then, in the Projects area, view Project ID of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the ListPolicy API.

Table 4-1067 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID.
hosts	Yes	String	Domain name ID. It can be obtained by calling the ListHost API.

Request Parameters

Table 4-1068 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).
Content-Type	Yes	String	Content type. Default: application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-1069 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies
level	Integer	<p>Protection level of basic web protection</p> <ul style="list-style-type: none"> • 1: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, Low is recommended. • 2: Medium. This protection level meets web protection requirements in most scenarios. • 3: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. <p>Default: 2</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • 1 • 2 • 3

Parameter	Type	Description
full_detection	Boolean	The detection mode in Precise Protection. <ul style="list-style-type: none"> • false: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. • true: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	Action object	Protective actions for each rule in anti-crawler protection.
action	PolicyAction object	Protective action
options	PolicyOption object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String, Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	Array of strings	Array of domain name IDs protected by the policy.
bind_host	Array of BindHost objects	Array of domain names protected with the protection policy. Compared with the hosts field, this field contains more details.
extend	Map<String, String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-1070 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: <ul style="list-style-type: none"> • log: WAF only logs discovered attacks. • block: WAF blocks discovered attacks.

Table 4-1071 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be log or block . log : WAF only logs discovered attacks. block : WAF blocks discovered attacks. Enumeration values: <ul style="list-style-type: none"> • block • log

Table 4-1072 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
common	Boolean	Whether general check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at true . You can ignore this parameter. Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
webshell	Boolean	Whether webshell detection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: <ul style="list-style-type: none"> • true • false
custom	Boolean	Whether precise protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
privacy	Boolean	Whether data masking is enabled Enumeration values: <ul style="list-style-type: none"> • true • false

Parameter	Type	Description
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: <ul style="list-style-type: none"> • true • false
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: <ul style="list-style-type: none"> • true • false

Table 4-1073 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be cloud for cloud WAF or premium for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-1074 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-1075 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-1076 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

The following example shows how to change a domain name added to a protection policy in a specific project. The project is specified by `project_id`, and the policy is specified by `policy_id`. The domain name ID is changed to `c0268b883a854adc8a2cd352193b0e13`.

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?
enterprise_project_id=0&hosts=c0268b883a854adc8a2cd352193b0e13
```

Example Responses

Status code: 200

OK

```
{
  "id": "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name": "demo",
  "level": 2,
  "action": {
    "category": "log"
  },
  "options": {
    "webattack": true,

```

```

"common" : true,
"crawler" : true,
"crawler_engine" : false,
"crawler_scanner" : true,
"crawler_script" : false,
"crawler_other" : false,
"webshell" : false,
"cc" : true,
"custom" : true,
"whiteblackip" : true,
"geoip" : true,
"ignore" : true,
"privacy" : true,
"antitamper" : true,
"antileakage" : false,
"bot_enable" : true,
"modulex_enabled" : false
},
"hosts" : [ "c0268b883a854adc8a2cd352193b0e13" ],
"extend" : { },
"timestamp" : 1650529538732,
"full_detection" : false,
"bind_host" : [ {
  "id" : "c0268b883a854adc8a2cd352193b0e13",
  "hostname" : "www.demo.com",
  "waf_type" : "cloud"
} ]
}

```

Status Codes

Status Code	Description
200	OK
400	Request failed.
401	The token does not have required permissions.
500	Internal server error.

Error Codes

See [Error Codes](#).

A Appendix

A.1 Status Code

- Normal

Returned Value	Description
200	The request is successfully processed.

- Abnormal

Status Code	Status	Description
400	Bad Request	The server fails to process the request.
401	Unauthorized	The requested page requires a username and a password.
403	Forbidden	Access to the requested page is denied.
404	Not Found	The server fails to find the requested page.
405	Method Not Allowed	Method specified in the request is not allowed.
406	Not Acceptable	Response generated by the server is not acceptable to the client.
407	Proxy Authentication Required	Proxy authentication is required before the request is processed.
408	Request Timeout	A timeout error occurs because the request is not processed within the specified waiting period of the server.

Status Code	Status	Description
409	Conflict	The request cannot be processed due to a conflict.
500	Internal Server Error	The request is not processed due to a server error.
501	Not Implemented	The request is not processed because the server does not support the requested function.
502	Bad Gateway	The request is not processed, and the server receives an invalid response from the upstream server.
503	Service Unavailable	The request is not processed due to a temporary system abnormality.
504	Gateway Timeout	A gateway timeout error occurs.

A.2 Error Codes

If an error code starting with APIGW is returned after you call an API, rectify the fault by referring to the instructions provided in [API Gateway Error Codes](#).

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00011001	bad.request	Bad request	Check param
400	WAF.00011002	url.param.illegal	The URL format is incorrect	Check URL format
400	WAF.00011003	request.body.illegal	Request body format error: missing parameter and illegal value in body	Check request body
400	WAF.00011004	id.illegal	Illegal ID	Check ID
400	WAF.00011005	name.illegal	Illegal name	Check name
400	WAF.00011006	host.illegal	Illegal domain name	Check domain name

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00011007	port.illegal	Illegal port	Check port
400	WAF.00011007	ip.illegal	Illegal IP	Check IP
400	WAF.00011008	protect.status.illegal	Illegal protection status	Check whether the protection state is in the range of enumeration value
400	WAF.00011009	access.status.illegal	Illegal access status	Check whether the access status is in the range of enumeration value
400	WAF.00011010	offsetOrLimit.illegal	Illegal offset or limit number	Check whether the starting line or limit number is within the range
400	WAF.00011011	pageOrPageSize.illegal	Illegal page number or number of entries per page	Check if page number or number of items per page are in range
400	WAF.00011012	standard.violated	Invalid parameter	Check the parameters
400	WAF.00011013	description.illegal	Illegal description format	Check description format
400	WAF.00011014	request.header.illegal	Request header format error: missing parameter and illegal value in header	Check header required parameters
400	WAF.00011014	website.not.register	The website has not been put on record	Filing website
400	WAF.00011016	name.duplicate	Duplicated name.	Change the name.

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00012001	invalid.token	Illegal token	Check whether the token is correct
400	WAF.00012002	invalid.project	Inconsistency between project_id and token	Check consistency of project_id and token
400	WAF.00012003	permission.denied	No permission	Assign WAF required permissions to account
400	WAF.00012004	account.frozen	Account freezing	Account unfreezing
400	WAF.00012005	not.subscribe	Unsubscribed	Subscribe to WAF service first
400	WAF.00012006	pdp.permission.denied	No permission	Check the PDP authority of the account
400	WAF.00012007	jwt.authentication.disabled	JWT certification off	Open JWT certification
400	WAF.00012008	jwt.authentication.invalid.token	Illegal JWT token	Check whether the account has JWT permission
400	WAF.00012009	jwt.authentication.failed	JWT authentication failed	Give the account authorization first
400	WAF.00012010	eps.all.not.support	eps.all.not.support	Open the write permission of enterprise project
400	WAF.00013001	insufficient.quota	Insufficient function quota	Purchase function quota upgrade package
400	WAF.00013002	feature.not.support	Function not supported	nothing
400	WAF.00013003	port.not.support	Port not supported	Port conversion via ELB
400	WAF.00013004	protocol.not.support	Protocol not supported	Through ELB conversion protocol

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00013005	wildcard.domain.not.support	Pan domain name not supported	Use specific domain names
400	WAF.00013006	ipv6.not.support	IPv6 is not supported	The current version does not support IPv6
400	WAF.00013007	insufficient.tenant.quota	insufficient.tenant.quota	Purchase quota upgrade package
400	WAF.00014001	resource.not.found	Resource not found	The resource has been deleted or does not exist
400	WAF.00014002	resource.already.exists	Resource already exists	Resource already exists
400	WAF.00014003	open.protection.failed	Failed to open protection	Check domain name protection status
400	WAF.00014004	access.failed	Failed to access WAF	Modify DNS resolution
400	WAF.00014005	bypass.failed	Bypasswaf failed	Check the protection status and try again
400	WAF.00014006	proxy.config.error	Agent configuration error	Reconfigure the agent correctly and try again
400	WAF.00014007	host.conflict	Domain name conflict	Check that the domain name already exists in the website configuration
400	WAF.00014008	cert.inconsistent	The same domain name, but the certificate is inconsistent	Use the same certificate
400	WAF.00014009	api.not.found	The interface does not exist	Check interface URL
400	WAF.00014010	port.protocol.mismatch	Port and protocol mismatch	Select the matching protocol and port

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00014011	host.blacklist	It is forbidden to add the protection website, and the domain name is blacklisted	
400	WAF.00014012	insufficient.tenant.quota	Insufficient tenant quota	Purchase quota upgrade package
400	WAF.00014013	exclusive.ip.config.error	Exclusive IP configuration error	Check exclusive IP configuration
400	WAF.00014014	exclusive.ip.config.error	exclusive.ip.config.error	Check exclusive IP configuration
400	WAF.00021002	url.param.illegal	The URL format is incorrect	It is recommended to modify the URL in the request body parameter to the standard URL and debug again
400	WAF.00021003	request.body.illegal	The request body parameter is incorrect	It is recommended that you verify the parameters according to the document before initiating debugging
400	WAF.00021004	id.illegal	The unique identifier ID format is incorrect	It is recommended to follow the correct instructions in the documentation to obtain the ID
400	WAF.00021005	name.illegal	The name parameter format is incorrect	Check the format of name, which can only be composed of letters, numbers, - _ And. Cannot exceed 64 characters in length

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00021006	host.illegal	The domain name format is incorrect	Domain name can only be composed of letters, numbers, -_ And. Cannot exceed 64 characters in length
400	WAF.00021007	protocol.illegal	The back-end protocol format is incorrect	The back-end protocol can only be configured as HTTP or HTTPS and must be capitalized
400	WAF.00021008	port.illegal	The source port format is incorrect	Check whether the configured port is empty and whether the target port is in the range of 0-65535
400	WAF.00021009	ip.illegal	Incorrect IP format	Check whether the IP format meets the standard format of IPv4 or IPv6
400	WAF.00021010	server.address.illegal	Server configuration exception	Check whether the server configuration is empty and whether the quantity is in the range of 1-80
400	WAF.00021012	path.illegal	The URL format in the rule configuration is incorrect	It is recommended to modify the URL in the request body parameter to the standard URL and debug again
400	WAF.00021013	cert.illegal	The HTTPS certificate has expired	It is recommended to upload the unexpired certificate again

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00021014	action.illegal	Illegal protective action	It is recommended to configure protection actions according to the enumerated values in the document
400	WAF.00021015	rule.status.illegal	Illegal rule status	It is recommended to modify the rule status according to the rule status enumeration value in the document
400	WAF.00021016	description.illegal	Description exception	It is recommended to use standard English grammar for description
400	WAF.00021017	incorrect.rule.config	Incorrect rule configuration	It is recommended to configure protection rules according to the documentation in the help center
400	WAF.00021018	incorrect.reference.table.config	Incorrect reference table configuration	It is recommended to configure the reference table according to the documentation in the help center
400	WAF.00021019	incorrect.route.config	Incorrect line configuration	It is recommended to configure the line according to the documentation in the help center

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00021020	offsetOrLimit.illegal	Paging parameter error	It is recommended to fill in pagination parameters according to the documents in the help center
400	WAF.00021021	param.exceed.limit	Parameter exceeds limit	It is recommended to view the parameter limits according to the documentation in the help center
400	WAF.00022002	resource.already.exists	Resource already exists	It is recommended to check whether the created resource already exists in the console
400	WAF.00022003	resource.is.being.used	The resource is in use	Remove the relationship between the resource and the user before deleting the resource
400	WAF.00022004	rule.conflict	Rule conflict	Check whether the target rule conflicts with the existing rule
403	WAF.00013014	insufficient.policy.quota	Insufficient policy quota	Purchase the domain name expansion package or upgrade the specification
403	WAF.00022005	insufficient.quota	Insufficient resources	It is recommended to purchase the upgrade package of corresponding resources

Status Code	Error Codes	Error Message	Description	Solution
404	WAF.00022001	resource.not.found	Resource does not exist	It is recommended to check the resource status on the console or ask for technical support
500	WAF.00010001	internal.error	Internal error	Contact technical support
500	WAF.00010002	system.busy	Internal error	Contact technical support
500	WAF.00010003	cname.failed	Failed to create or modify CNAME	Contact technical support
500	WAF.00010004	cname.failed	Failed to get OBS file download link	Contact technical support
500	WAF.00020001	internal.error	Service internal exception	It is recommended to try again in five minutes
500	WAF.00020002	system.busy	System busy	It is recommended to try again in five minutes

A.3 Obtaining a Project ID

Obtaining a Project ID by Calling an API

You can obtain the project ID by calling the API for [Querying Project Information Based on Specified Criteria](#).

The API used to obtain a project ID is GET `https://{Endpoint} /v3/projects`. {Endpoint} indicates the IAM endpoint, which can be obtained from the [Regions and Endpoints](#). For details about API authentication, see [Authentication](#).

In the following example, **id** indicates the project ID.

```
{
  "projects": [
    {
      "domain_id": "65382450e8f64ac0870cd180d14e684b",
      "is_domain": false,
```

```

    "parent_id": "65382450e8f64ac0870cd180d14e684b",
    "name": "xxxxxxx",
    "description": "",
    "links": {
      "next": null,
      "previous": null,
      "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
    },
    "id": "a4a5d4098fb4474fa22cd05f897d6b99",
    "enabled": true
  }
],
"links": {
  "next": null,
  "previous": null,
  "self": "https://www.example.com/v3/projects"
}
}

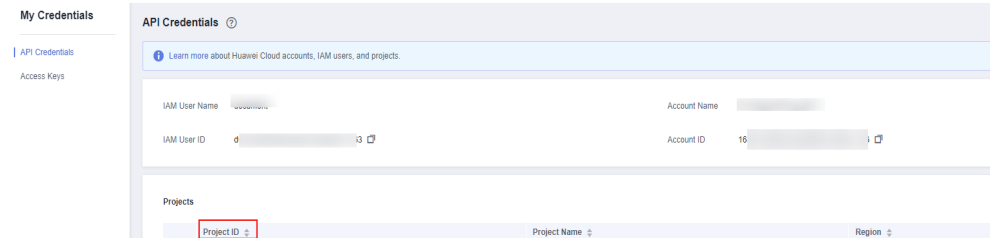
```

Obtaining a Project ID from the Console

A project ID is required for some URLs when an API is called. To obtain a project ID, perform the following operations:

1. Log in to the management console.
2. Click the username and choose **My Credentials** from the drop-down list.
3. On the **API Credentials** page, view the project ID in the project list.

Figure A-1 Viewing project IDs



A.4 Geographical Location Codes

Location	Code	Location	Code	Location	Code
China	CN	Chile	Chile	Lithuania	Lithuania
Anhui	AH	Christmas Island	Christmas Island	Luxembourg	Luxembourg
Beijing	BJ	Colombia	Colombia	North Macedonia (the former Yugoslav Republic of Macedonia)	Macedonia (FYROM)

Location	Code	Location	Code	Location	Code
Chongqing	CQ	Comoros	Comoros	Madagascar	Madagascar
Fujian	FJ	Congo	Congo	Malawi	Malawi
Guangdong	GD	Democratic Republic of the Congo	Congo, Democratic Republic	Malaysia	Malaysia
Gansu	GS	Cook Islands	Cook Islands	Maldives	Maldives
Guangxi	GX	Costa Rica	Costa Rica	Mali	Mali
Guizhou	GZ	Côte d'Ivoire	Cote D'Ivoire (Ivory Coast)	Malta	Malta
Henan	HA	Croatia	Croatia	Marshall Islands	Marshall Islands
Hubei	HB	Zimbabwe	Zimbabwe	Martinique	Martinique
Hebei	HE	Curacao	Curacao	Mauritania	Mauritania
Hainan	HI	Cyprus	Cyprus	Mauritius	Mauritius
Hong Kong (China)	HK	Czech Republic	Czech Republic	Mayotte	Mayotte
Heilongjiang	HL	Germany	DE	Mexico	Mexico
Hunan	HN	Denmark	Denmark	Micronesia	Micronesia
Jilin	JL	Djibouti	Djibouti	Moldova	Moldova
Jiangsu	JS	Dominica	Dominica	Monaco	Monaco
Jiangxi	JX	Dominican Republic	Dominican Republic	Mongolia	Mongolia
Liaoning	LN	East Timor	East Timor	Montenegro	Montenegro
Macao (China)	MO	Ecuador	Ecuador	Montserrat	Montserrat
Inner Mongolia	NM	Egypt	Egypt	Morocco	Morocco
Ningxia	NX	El Salvador	El Salvador	Mozambique	Mozambique
Qinghai	QH	Equatorial Guinea	Equatorial Guinea	Myanmar	Myanmar

Location	Code	Location	Code	Location	Code
Sichuan	SC	The State of Eritrea	Eritrea	Namibia	Namibia
Shandong	SD	Estonia	Estonia	Nauru	Nauru
Shanghai	SH	Ethiopian	Ethiopia	Nepal	Nepal
Shaanxi	SN	Falkland Islands	Falkland Islands	New Caledonia	New Caledonia
Shanxi	SX	Faroe Islands	Faroe Islands	New Zealand	New Zealand
Tianjin	TJ	Fiji	Fiji	Nicaragua	Nicaragua
Taiwan (China)	TW	Finland	Finland	Niger	Niger
Xinjiang	XJ	France	FR	Nigeria	Nigeria
Tibet	XZ	French Guiana	French Guiana	Niue	Niue
Yunnan	YN	French Polynesia	French Polynesia	Norfolk Island	Norfolk Island
Zhejiang	ZJ	Gabon	Gabon	United Arab Emirates	United Arab Emirates
Afghanistan	Afghanistan	Gambia	Gambia	Northern Mariana Islands	Northern Mariana Islands
Ahvenanmaa	Ahvenanmaa	Georgia	Georgia	Norway	Norway
Albania	Albania	Ghana	Ghana	Oman	Oman
Algeria	Algeria	Gibraltar	Gibraltar	Pakistan	Pakistan
American Samoa	American Samoa	Greece	Greece	Palau	Palau
Andorra	Andorra	Greenland	Greenland	Palestine	Palestine
Angola	Angola	Grenada	Grenada	Panama	Panama
Anguilla	Anguilla	Guadeloupe	Guadeloupe	Papua New Guinea	Papua New Guinea
Antigua and Barbuda	Antigua and Barbuda	Guam	Guam	Paraguay	Paraguay
Argentina	Argentina	Guatemala	Guatemala	Peru	Peru

Location	Code	Location	Code	Location	Code
Armenia	Armenia	Guernsey	Guernsey	Philippines	Philippines
Aruba	Aruba	Guinea	Guinea	Poland	Poland
Australia	AU	Guinea-Bissau	Guinea-Bissau	Portugal	Portugal
Austria	Austria	Guyana	Guyana	Puerto Rico	Puerto Rico
Azerbaijan	Azerbaijan	Haiti	Haiti	Qatar	Qatar
The Bahamas	Bahamas	Honduras	Honduras	Reunion	Reunion
Bahrain	Bahrain	Hungary	Hungary	Romania	Romania
Bangladesh	Bangladesh	Iceland	Iceland	Zambia	Zambia
Barbados	Barbados	India	IN	Rwanda	Rwanda
Belarus	Belarus	Indonesia	Indonesia	Saint Barthelemy	Saint Barthelemy
Belgium	Belgium	Wallis and Futuna	Wallis and Futuna	Saint Kitts and Nevis	Saint Kitts and Nevis
Belize	Belize	Iraq	Iraq	Sant Lucia	Saint Lucia
Benin	Benin	Ireland	Ireland	Saint Martin	Saint Martin
Bermuda	Bermuda	Isle of Man	Isle of Man, British Dependenc y	Saint Vincent and the Grenadines	Saint Vincent and the Grenadines
Bhutan	Bhutan	Yemen	Yemen	Saint Pierre and Miquelon	Saint-Pierre and Miquelon
Bolivia	Bolivia	Italy	Italy	Samoa	Samoa
Bosnia and Herzegovina	Bosnia and Herzegovina	Jamaica	Jamaica	San Marino	San Marino
Botswana	Botswana	Jersey	Jersey	São Tomé and Príncipe	Sao Tome and Principe
Bouvet Island	Bouvet Island	Jordan	Jordan	Saudi Arabia	Saudi Arabia
Brazil	BR	Japan	JP	Senegal	Senegal

Location	Code	Location	Code	Location	Code
British Indian Ocean Territory	British Indian Ocean Territory	Kazakhstan	Kazakhstan	Serbia	Serbia
Virgin Islands, British	British Virgin Islands	Kenya	Kenya	Seychelles	Seychelles
Brunei Darussalam	Brunei Darussalam	Kiribati	Kiribati	Sierra Leone	Sierra Leone
Bulgaria	Bulgaria	Kuwait	Kuwait	Singapore	Singapore
Burkina Faso	Burkina Faso	Kyrgyzstan	Kyrgyzstan	Sint Maarten	Sint Maarten
Burundi	Burundi	Laos	Laos	Slovakia	Slovakia
Canada	CA	Latvia	Latvia	Slovenia	Slovenia
Cambodia	Cambodia	Lebanon	Lebanon	Solomon Islands	Solomon Islands
Cameroon	Cameroon	Lesotho	Lesotho	Somalia	Somalia
Cape Verde	Cape Verde	Liberia	Liberia	South Africa	South Africa
Caribbean Netherlands	Caribbean Netherlands	Libya	Libya	South Georgia and South Sandwich Islands	South Georgia and The South Sandwich Islands
Cayman Islands	Cayman Islands	Liechtenstein	Liechtenstein	South Sudan	South Sudan
Central African Republic	Central African Republic	Suriname	Suriname	Spain	Spain
Chad	Chad	Thailand	Thailand	Sri Lanka	Sri Lanka
Swaziland	Swaziland	Netherlands	The Netherlands	Tonga	Tonga
Sweden	Sweden	South Korea	The Republic of Korea	Trinidad and Tobago	Trinidad and Tobago

Location	Code	Location	Code	Location	Code
Switzerland	Switzerland	Togo	Togo	Tunisia	Tunisia
Tajikistan	Tajikistan	Tokelau	Tokelau	Turkmenistan	Turkmenistan
Tanzania	Tanzania	United States Virgin Islands	United States Virgin Islands	Turks and Caicos Islands	Turks and Caicos Islands
Tuvalu	Tuvalu	Uruguay	Uruguay	Vatican City State	Vatican City
Uganda	Uganda	United States	US	Venezuela	Venezuela
United Kingdom	UK	Uzbekistan	Uzbekistan	Vietnam	Viet Nam

B Change History

Released On	Description
2024-03-22	This issue is the twenty-eighth official release. Modified Adding a Domain Name to a Dedicated WAF Instance : Optimized some parameters.
2024-01-26	This issue is the twenty-seventh official release. Modified the following content: <ul style="list-style-type: none">• Querying Top Statistics by Category on the Dashboard: The language can be set.• Error Codes: Added the error code for insufficient policy quota.
2023-12-30	This issue is the twenty-sixth official release. Added section "Permissions and Supported Actions"
2023-11-30	This is the twenty-fifth official release. Modified section "Obtaining Domain Name Route Information in Cloud Mode."
2023-09-18	This issue is the twenty-fourth official release. Updating a Protection Policy : Added examples.
2023-09-01	This issue is the twenty-third official release. Added the description of the default value for the enterprise project parameter.
2023-08-01	This issue is the twenty-second official release. Added "Geographical Location Codes".
2023-07-14	This issue is the twenty-first official release. Modified the following content: <ul style="list-style-type: none">• Enabling the Pay-per-Use Billing for Cloud WAF

Released On	Description
2023-06-19	<p>This is the twentieth official release.</p> <p>The forward_header_map field is added to the following APIs:</p> <ul style="list-style-type: none">• Adding a Domain Name to Cloud WAF• Querying Domain Names Protected by Cloud WAF• Updating Configurations of Domain Names Protected with Cloud WAF• Adding a Domain Name to a Dedicated WAF Instance• Querying Domain Names Protected by Dedicated WAF Engines• Querying Domain Name Settings in Dedicated Mode• Modifying a Domain Name Protected by a Dedicated WAF Instance
2023-06-16	<p>This issue is the nineteenth official release.</p> <p>Added descriptions to example API calls.</p>
2023-04-20	<p>This issue is the eighteenth official release.</p> <p>Optimized descriptions of some parameters.</p>
2023-03-31	<p>This issue is the seventeenth official release.</p> <p>Added APIs for querying a blacklist or whitelist protection rule, querying a data masking rule, querying a web tampering protection rule, and querying a reference table.</p>
2023-03-24	<p>This issue is the sixteenth official release.</p> <p>Added APIs for CC protection, precise protection, anti-crawler protection, known attack source, and information leakage prevention and the APIs for enabling and disabling the pay-per-use billing for cloud WAF.</p>
2023-02-09	<p>This issue is the fifteenth official release.</p> <p>Modified "Adding a Domain Name to Cloud WAF."</p>
2023-01-06	<p>This issue is the fourteenth official release.</p> <p>Modified "Querying Bandwidth Usage Statistics."</p>
2022-11-23	<p>This issue is the thirteenth official release.</p> <p>Added the following APIs:</p> <ul style="list-style-type: none">• Buying a Yearly/Monthly-billed Cloud WAF Instance• Changing Specifications of a Yearly/Monthly-Billed Cloud WAF Instance• Querying Your Subscriptions

Released On	Description
2022-11-15	This issue is the twelfth official release. Added the following APIs: <ul style="list-style-type: none"> • APIs for managing alarms • APIs for managing the system • APIs for managing protected domain names
2022-11-04	This issue is the eleventh official release. Added the following APIs: <ul style="list-style-type: none"> • APIs for managing address groups • APIs for managing dedicated WAF instances • APIs for managing log configurations
2022-10-25	This issue is the tenth official release. Modified the descriptions of some parameters in "Adding a Domain Name to Cloud WAF."
2022-10-09	This issue is the ninth official release. Modified the following content: <ul style="list-style-type: none"> • Querying the List of Geolocation Access Control Rules: Modified the description of the geqip parameter. • Creating a Geolocation Access Control Rule: Modified the description of the geqip parameter. • Updating a Geolocation Access Control Rule: Modified the description of the geqip parameter. • Deleting a Geolocation Access Control Rule: Modified the description of the geqip parameter.
2022-09-27	This issue is the eighth official release. Changed the type of parameter rule in the response body to String in "Deleting a Global Protection Whitelist (Formerly False Alarm Masking) Rule."
2022-09-08	This is the seventh official release. Modified the following content: <ul style="list-style-type: none"> • Deleting a Global Protection Whitelist (Formerly False Alarm Masking) Rule • Querying Global Protection Whitelist (Formerly False Alarm Masking) Rules" • Creating a Global Protection Whitelist (Formerly False Alarm Masking) Rule

Released On	Description
2022-09-02	This issue is the sixth official release. Modified the types of request parameters hosts and instances in "Querying Statistics of Requests and Attacks" to "Querying Top Security Statistics by Category."
2022-08-26	This issue is the fifth official release. Added the API for querying the requests to a protected website for a time range.
2022-08-15	This issue is the fourth official release. Optimized the parameter description in section "API."
2022-07-04	This issue is the third official release. Added the API for querying top security statistics by category.
2022-04-22	This issue is the second official issue. Added example requests and responses for each API.
2021-11-24	This is the first official release.