## Web Application Firewall

# API Reference

| | |
|---|---|
| **Issue** | 02 |
| **Date** | 2022-12-28 |

**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 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 modifying protected domain names. For details about all supported operations, see **API Overview**.

Before calling WAF APIs, ensure that you are familiar with WAF concepts. For details, see "Service Overview" in the *Web Application Firewall User Guide*.

## 1.2 API Calling

WAF supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS. For details about API calling, 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 Notes and Constraints

For details about constraints, see the description of a specific API.

# 1.5 Basic Concepts

- 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 Global region and specific regions. The Global region provides common cloud services for all tenants, and a specific region provides only services of the same type for specific tenants.

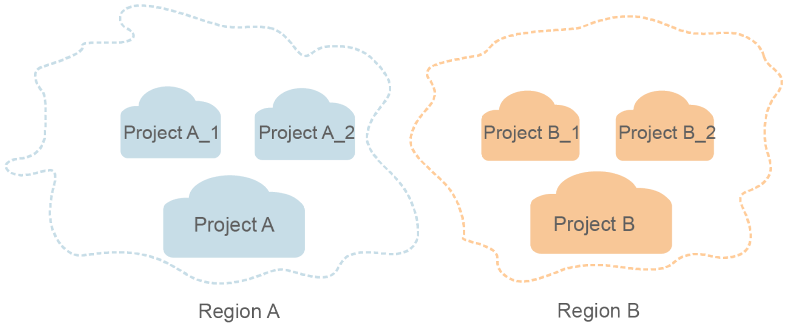
- Availability Zone (AZ)

  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 allow you to build highly available systems across AZs.

- Project

  Projects group and isolate resources (including 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 |
|---|---|
| Resource quotas | APIs used to obtain package information and the number of added resources |
| Protected domain names | APIs used to manage protected domain names, including querying and creating protected domain names |
| Certificate management | APIs used to manage certificates, including uploading and querying certificates |
| Protection status and domain name connection | APIs used to change the WAF protection status and add domain names to WAF |
| Policies | APIs used to manage protection policies, including querying and creating protection policies |
| Blacklist and whitelist | APIs used to manage whitelist and blacklist rules, including querying and creating IP address whitelists or blacklists |
| CC attack protection rules | APIs used to manage CC attack protection rules, including querying and creating CC attack protection rules |
| Precise protection rules | APIs used to manage precision protection rules, including querying and creating precise protection rules |
| Data masking rules | APIs used to manage data masking rules, including querying and creating data masking rules |
| Web tamper protection rules | APIs used to manage web tamper protection rules, including querying and creating web tamper protection rules |
| False alarm masking rules | APIs used to manage false alarm masking rules, including querying and creating false alarm masking rules |

| Type | Description |
|---|---|
| Event log query | APIs used to query event logs, including querying attack event logs and event type distribution. |
| Alarm notification | APIs used to query and update configurations of alarm notification |
| Obtaining option details | APIs used to query the event type in an alarm notification and obtain the HTTP request header of the source IP address |
| Interconnection with Cloud Eye | API used to query the name and status of a WAF instance interconnecting with Cloud Eye |

# 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 REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**.

- **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.

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://{{endpoint}}/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-based 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://{{endpoint}}/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 *xxxxxxxxxxxxxxxxxx* to the project name, such as **eu-west-0**. 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://{{endpoint}}/v3/auth/tokens
Content-Type: application/json

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

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://{{endpoint}}/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**.

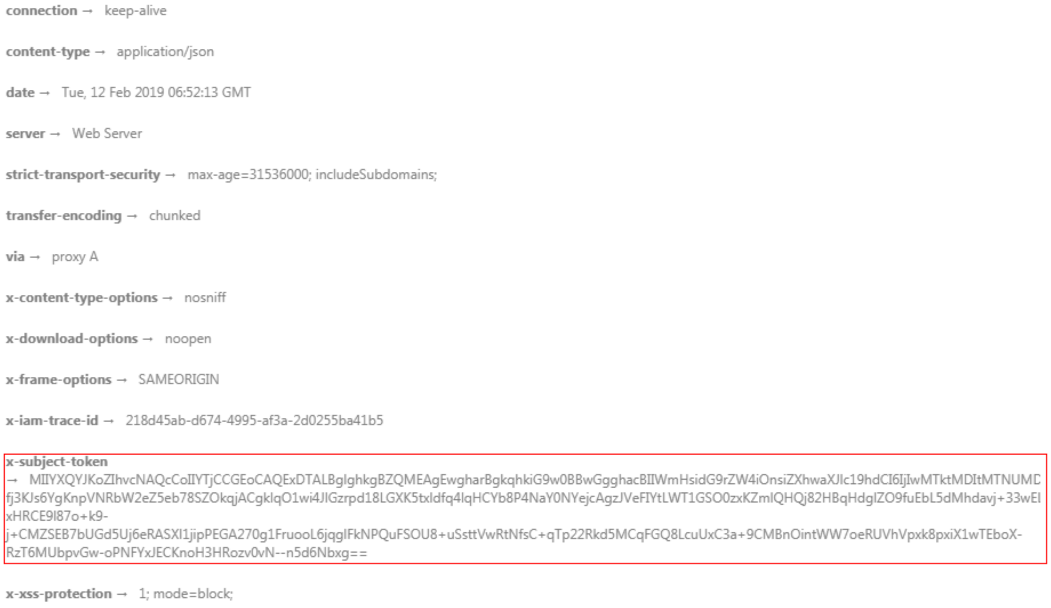
For example, if status code **201** is returned for calling the API used to obtain a user token, the request is successful.

## Response Header

A response header corresponds to a request header, for example, **Content-Type**.

**Figure 3-1** shows the response header for the API of obtaining a user token, in which **x-subject-token** is the desired user token. Then, you can use the token to authenticate the calling of other APIs.

**Figure 3-1** Header 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
→ MIIYXQYJKoZIhvcNAQcCoIIYTjCCGEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOnsiZXhwaXJlc19hdCI6IjIwMTktMDItMTNUMD
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkqjACgklqO1wi4JIGzrpd18LGXK5txldfq4lqHCYb8P4NaY0NYejcAgzJVeFIYtLWT1GSO0zxKZmIQHQj82HBqHdgIZO9fuEbL5dMhdavj+33wEl
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jqglFkNPQuFSOU8+uSsttVwRtNfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUVhVpxk8pxiX1wTEboX-
RzT6MUbpvGw-oPNFYxJECKnoH3HRozv0vN--n5d6Nbxg==

x-xss-protection → 1; mode=block;
```

## (Optional) Response Body

A response body is generally returned in a structured format, corresponding to the **Content-Type** in the response header, and is used to transfer content other than 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": "xxxxxxxx",
......
```

If an error occurs during API calling, the system returns an error code and a message to you. The following shows the format of an error response body:

```
{
    "error": {
        "message": "The request you have made requires authentication.",
        "title": "Unauthorized"
    }
}
```

In the preceding information, **error_code** is an error code, and **error_msg** describes the error.

# 4 APIs

## 4.1 Cloud Mode

## 4.1.1 Resource Quotas

### 4.1.1.1 Obtaining Package Information

### Function Description

This API is used to obtain package information of a user.

### URI

- URI format
  GET /v1/{project_id}/waf/bundle
- Parameter description

**Table 4-1** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |

### Request

Request parameters

None

### Response

Response parameters

**Table 4-2** Parameter description

| Parameter | Type | Description |
|---|---|---|
| type | Integer | Specifies version information. |
| name | String | Specifies the package name. |
| options | **Table 3** | Specifies the protection switches. |
| rule | **Table 4** | Specifies the maximum number of rules in a policy. |
| host | **Table 5** | Specifies the maximum number of domain names in a policy. |
| other | **Table 6** | Specifies other restrictions in the package. |

**Table 4-3 options**

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Specifies whether Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| common | Boolean | Specifies whether General Check in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler | Boolean | Specifies whether the master crawler detection switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled.<br>**NOTE**<br>If **crawler** is **false**, all the subswitches, **crawler_engine**, **crawler_scanner**, **crawler_script**, and **crawler_other** are invalid. |
| crawler_engine | Boolean | Specifies whether the Search Engine switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Type | Description |
|---|---|---|
| crawler_scanner | Boolean | Specifies whether the Scanner switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_script | Boolean | Specifies whether the Script Tool switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_other | Boolean | Specifies whether detection of other crawlers in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| webshell | Boolean | Specifies whether webshell detection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| cc | Boolean | Specifies whether CC Attack Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| custom | Boolean | Specifies whether Precise Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| whiteblackip | Boolean | Specifies whether Blacklist and Whitelist is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| privacy | Boolean | Specifies whether Data Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| Ignore | Boolean | Specifies whether False Alarm Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Type | Description |
|---|---|---|
| antitamper | Boolean | Specifies whether Web Tamper Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| full_detection | Boolean | Specifies whether the full detection mode in Precise Protection is enabled.<br>● **true**: full detection. Full detection finishes all threat detections before blocking requests that meet Precise Protection specified conditions.<br>● **false**: instant detection. Instant detection immediately ends threat detection after blocking a request that meets Precise Protection specified conditions. |
| log_download | Boolean | Specifies whether log download is available.<br>● **true**: available.<br>● **false**: unavailable. |

**Table 4-4** rule

| Parameter | Type | Description |
|---|---|---|
| antitamper | Integer | Specifies the total number of web tamper protection rules. The maximum value is **100**. |
| cc | Integer | Specifies the total number of CC attack protection rules. The maximum value is **100**. |
| custom | Integer | Specifies the total number of precise protection rules. The maximum value is **100**. |
| ignore | Integer | Specifies the total number of false alarm masking rules. The maximum value is **1000**. |

| Parameter | Type | Description |
|---|---|---|
| privacy | Integer | Specifies the total number of data masking rules. The maximum value is **1000**. |
| whiteblackip | Integer | Specifies the total number of blacklist and whitelist rules. The maximum value is **100**. |

NOTE

Contact the administrator to increase the maximum values in **Table 4-4**.

**Table 4-5 host**

| Parameter | Type | Description |
|---|---|---|
| wildcard | Boolean | Specifies whether a wildcard domain is supported.<br>● **true**: supported.<br>● **false**: unsupported. |
| ports | **Table 7** | Specifies the range of ports supported. |
| protocol | **Table 8** | Specifies the client protocol. |
| server | Integer | Specifies the number of backend servers supported. The maximum value is **30**. |
| host | Integer | Specifies the number of subdomain names supported. The maximum value is **100**. |
| domain | Integer | Specifies the number of domain names supported. The maximum value is **100**. |
| cert_num | Integer | Specifies the number of certificates supported. The maximum value is **100**. |

| Parameter | Type | Description |
|---|---|---|
| policy_apply_to | Boolean | Specifies whether a policy can be applied to multiple domain names.<br>● **true**: A policy can be applied to multiple domain names.<br>● **false**: A policy cannot be applied to multiple domain names. |
| policy_num | Integer | Specifies the number of policies supported. The maximum value is **5000**. |

**Table 4-6 other**

| Parameter | Type | Description |
|---|---|---|
| default_cc | Integer | Specifies the maximum number of requests from a web visitor in a default CC attack protection policy. |

**Table 4-7 ports**

| Parameter | Type | Description |
|---|---|---|
| http | Array | Specifies the list of HTTP ports supported. |
| https | Array | Specifies the list of HTTPS ports supported. |
| max_num | Integer | Specifies the number of ports supported. |
| none_standard | Boolean | Specifies whether non-standard ports are supported.<br>● **true**: Non-standard ports are supported.<br>● **false**: Non-standard ports are not supported. |

**Table 4-8 protocol**

| Parameter | Type | Description |
|---|---|---|
| http | Boolean | Specifies whether the HTTP protocol is supported.<br>● **true**: The HTTP protocol is supported.<br>● **false**: The HTTP protocol is not supported. |
| https | Boolean | Specifies whether the HTTPS protocol is supported.<br>● **true**: The HTTPS protocol is supported.<br>● **false**: The HTTPS protocol is not supported. |
| http_https | Boolean | Specifies whether the HTTP and HTTPS protocols are supported.<br>● **true**: Both HTTP and HTTPS are supported.<br>● **false**: Neither HTTP nor HTTPS is supported. |

## Example

Response example

```
{
  "type": 1,
  "name": "Basic",
  "options": {
    "webattack": true,
    "common": true,
    "crawler": true,
    "webshell": false,
    "cc": false,
    "custom": false,
    "whiteblackip": true,

    "privacy": true,
    "ignore": true,
    "antitamper": false,
"log_download": true,
  },
  "rule": {
    "cc": 0,
    "custom": 0,
    "whiteblackip": 10,

    "privacy": 10,
    "ignore": 1000,
"antitamper": 0,
  },
  "host": {
    "wildcard": false,
    "protocol": {
     "http": true,
     "https": false,
     "http_https": false
    },
    "ports": {
     "none_standard": false,
     "http": [],
     "https": [],
     "max_num": 0
    },
    "domain": 1,
    "host": 10,
    "server": 10,
    "route": false
  },
  "other": {
     "default_cc": 25000
    }
}
```

## Status Code

**Table 4-9** describes the normal status code returned by the API.

**Table 4-9** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.1.2 Querying the Number of Existing Resources

### Function Description

This API is used to query the number of existing resources of a user.

### URI

- URI format

  GET /v1/{project_id}/waf/bundle/usage/{resource_type}

- Parameter description

**Table 4-10** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| resource_type | Yes | String | Specifies the resource type. The options are **instance**, **policy**, and **certificate**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-11** Parameter description

| Parameter | Type | Description |
|---|---|---|
| count | Integer | Specifies the number of existing resources. |

## Example

The following shows the response if the number of uploaded certificates is queried.

Response example

```
{
  "count": 2
}
```

## Status Code

**Table 4-12** describes the normal status code returned by the API.

**Table 4-12** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.2 Domain Names

## 4.1.2.1 Querying the List of Domain Names

### Function Description

This API is used to query the list of domain names.

### URI

- URI format

GET /v1/{project_id}/waf/instance?offset={offset}&limit={limit}&hostname={hostname}&policyname={policyname}

- Parameter description

**Table 4-13** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |
| limit | No | Long | Specifies the maximum number of records displayed on each page. Its value ranges from **0** to **50**. The default value is **10**. If **limit** is **-1**, one page with 65535 records is displayed. |
| hostname | No | String | Specifies the domain name. |
| policyname | No | String | Specifies the policy name. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-14** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of domain names. |
| items | Table 3 | Specifies the domain objects. |

**Table 4-15 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the domain ID. |
| hostname | String | Specifies the returned domain name. |
| cname | String | Specifies the CNAME value.<br>For example, **efec1196267b41c399f2980ea4048517.waf.cloud.com**. |
| txt_code | String | Specifies the TXT record. This parameter is returned only when **proxy** is set to **true**. |
| sub_domain | String | Specifies the subdomain name. This parameter is returned only when **proxy** is set to **true**. |
| policy_id | String | Specifies the policy ID. |
| protect_status | Integer | Specifies the WAF mode.<br>● **-1**: bypassed.<br>● **0**: disabled.<br>● **1**: enabled. |
| access_status | Integer | Specifies whether a domain name is connected to WAF.<br>● **0**: The domain name is not connected to WAF.<br>● **1**: The domain name is connected to WAF. |
| proxy | Boolean | Specifies whether a proxy is configured.<br>● **true**: A proxy is configured.<br>● **false**: No proxy is configured. |
| timestamp | Long | Specifies the time when a domain name is created. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
    "total": 2,
    "items": [
        {
          "id": "388a7789d55b41d1918b3088a8f1e7f3",
          "hostname": "www.a.com",
          "cname": "3249d21e5eb34d21be12fdc817fcb67d.waf.cloud.com",
          "txt_code": "3249d21e5eb34d21be12fdc817fcb67d",
          "sub_domain": "3249d21e5eb34d21be12fdc817fcb67d.www.a.com",
          "policy_id": "xxxxxxxxxxxxxx",
          "protect_status": 0,
          "access_status": 0,
          "proxy": true,
          "timestamp": 1499817600
        },
        {
          "id": "296a7710d55b41d1918b3036a8f1e7e5",
          "hostname": "www.b.com",
          "cname": "efec1196267b41c399f2980ea4048517.waf.cloud.com",
          "policy_id": "xxxxxxxxxxxxxx",
          "protect_status": 1,
          "access_status": 1,
          "proxy": false,
          "timestamp": 1499817612
        }
      ]
}
```

## Status Code

**Table 4-16** describes the normal status code returned by the API.

**Table 4-16** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.2.2 Creating a Domain Name

## Function Description

This API is used to create a domain name.

## URI

- URI format

  POST /v1/{project_id}/waf/instance

- Parameter description

  **Table 4-17** Path parameters

  | Parameter | Mandatory | Type | Description |
  |---|---|---|---|
  | project_id | Yes | String | Specifies the project ID. |

## Request

Request parameters

**Table 4-18** Request parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| hostname | Yes | String | Specifies the domain name.<br>For example, **www.example.com** or ***.example.com**. |
| certificate_id | No | String | Specifies the certificate ID. This parameter is mandatory when **client_protocol** is set to **HTTPS**. |
| server | Yes | Array | Specifies the origin server information, including the **client_protocol**, **server_protocol**, **address**, and **port** fields.<br>• **client_protocol**: protocol type of the client. The options are **HTTP** and **HTTPS**.<br>• **server_protocol**: protocol used by WAF to forward client requests to the server. The options are **HTTP** and **HTTPS**.<br>• **address**: public IP address or domain name of the web server that the client accesses<br>• **port**: port number used by the web server. The value ranges from **0** to **65535**, for example, **8080**. |
| proxy | Yes | Boolean | Specifies whether a proxy is configured.<br>• **true**: A proxy is configured.<br>• **false**: No proxy is configured. |
| sip_header_name | No | String | Specifies the type of the source IP header. This parameter is required only when **proxy** is set to **true**.<br>The options are as follows: **default**, **cloudflare**, **akamai**, and **custom**. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| sip_header_list | No | Array | Specifies the HTTP request header for identifying the real source IP address. This parameter is required only when **proxy** is set to **true**.<br>● If **sip_header_name** is **default**, **sip_header_list** is **["X-Forwarded-For"]**.<br>● If **sip_header_name** is **cloudflare**, **sip_header_list** is **["CF-Connecting-IP", "X-Forwarded-For"]**.<br>● If **sip_header_name** is **akamai**, **sip_header_list** is **["True-Client-IP"]**.<br>● If **sip_header_name** is **custom**, you can customize a value. |

## Response

Response parameters

**Table 4-19** Response parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the instance ID. |
| hostname | String | Specifies the domain name. |
| cname | String | Specifies the CNAME value. For example, **efec1196267b41c399f2980ea4048517.waf.cloud.com**. |
| txt_code | String | Specifies the TXT record. This parameter is returned only when **proxy** is set to **true**. |
| sub_domain | String | Specifies the subdomain name. This parameter is returned only when **proxy** is set to **true**. |
| policy_id | String | Specifies the policy ID. |

| Parameter | Type | Description |
|---|---|---|
| protect_status | Integer | Specifies the WAF mode.<br>● **-1**: bypassed.<br>● **0**: disabled.<br>● **1**: enabled. |
| access_status | Integer | Specifies whether a domain name is connected to WAF.<br>● **0**: The domain name is not connected to WAF.<br>● **1**: The domain name is connected to WAF. |
| proxy | Boolean | Specifies whether a proxy is configured.<br>● **true**: A proxy is configured.<br>● **false**: No proxy is configured. |
| protocol | String | Specifies the protocol type of the client. The options are **HTTP**, **HTTPS**, and **HTTP,HTTPS**. |
| certificate_id | String | Specifies the certificate ID. This parameter is mandatory when **client_protocol** is set to **HTTPS**. |
| server | Array | Specifies the origin server information, including the **client_protocol**, **server_protocol**, **address**, and **port** fields. |
| sip_header_name | String | Specifies the type of the source IP header. This parameter is returned only when **proxy** is set to **true**.<br>The options are as follows: **default**, **cloudflare**, **akamai**, and **custom**. |
| sip_header_list | Array | Specifies the HTTP request header for identifying the real source IP address. This parameter is returned only when **proxy** is set to **true**.<br>● If **sip_header_name** is **default**, **sip_header_list** is **["X-Forwarded-For"]**.<br>● If **sip_header_name** is **cloudflare**, **sip_header_list** is **["CF-Connecting-IP", "X-Forwarded-For"]**.<br>● If **sip_header_name** is **akamai**, **sip_header_list** is **["True-Client-IP"]**.<br>● If **sip_header_name** is **custom**, you can customize a value. |
| timestamp | Long | Specifies the time when a domain name is created. |

## Examples

**www.b.com** is used as an example.

- Request example

```
{
  "hostname": "www.b.com",
  "certificate_id": "07fb6809a89241fca86ac6f69e34963d",
  "server": [
      {"client_protocol": "HTTPS", "server_protocol": "HTTP", "address": "X.X.X.X", "port": "8080"},
      {"client_protocol": "HTTP", "server_protocol": "HTTP", "address": "X.X.X.X", "port": "80"}
   ],
  "proxy": true,
  "sip_header_name": "default",
  "sip_header_list": ["X-Forwarded-For"]
}
```

- Response example

```
{
        "id": "388a7789d55b41d1918b3088a8f1e7f3",
        "hostname": "www.b.com",
        "cname": "3249d21e5eb34d21be12fdc817fcb67d.waf.cloud.com",
        "txt_code": "3249d21e5eb34d21be12fdc817fcb67d",
        "sub_domain": "3249d21e5eb34d21be12fdc817fcb67d.www.b.com",
        "policy_id": "xxxxxxxxxxxxxx",
        "certificate_id": "xxxxxxxxxxxxxxxxxxx",
        "protect_status": 0,
        "access_status": 0,
        "protocol": "HTTP,HTTPS",
        "server": [
           {"client_protocol": "HTTPS", "server_protocol":"HTTP", "address":"X.X.X.X", "port":443},
           {"client_protocol": "HTTP", "server_protocol":"HTTP", "address":"X.X.X.X", "port":80}
        ],
       "proxy": true,
       "sip_header_name": "default",
       "sip_header_list": ["X-Forwarded-For"],
       "timestamp": 1499817600


}
```

## Status Code

**Table 4-20** describes the normal status code returned by the API.

**Table 4-20** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.2.3 Querying a Domain Name

## Function Description

This API is used to query details about a domain name.

## URI

- URI format

  GET /v1/{project_id}/waf/instance/{instance_id}
- Parameter description

  **Table 4-21** Path parameters

  | Parameter | Mandatory | Type | Description |
  |---|---|---|---|
  | project_id | Yes | String | Specifies the project ID. |
  | instance_id | Yes | String | Specifies the instance ID. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-22** Response parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the instance ID. |
| hostname | String | Specifies the domain name. |
| cname | String | Specifies the CNAME value. For example, **efec1196267b41c399f2980ea4048517.waf.cloud.com**. |
| txt_code | String | Specifies the TXT record. This parameter is returned only when **proxy** is set to **true**. |
| sub_domain | String | Specifies the subdomain name. This parameter is returned only when **proxy** is set to **true**. |
| policy_id | String | Specifies the policy ID. |
| protect_status | Integer | Specifies the WAF mode.<br>● **0**: disabled.<br>● **1**: enabled.<br>● **-1**: bypassed. |

| Parameter | Type | Description |
|---|---|---|
| access_status | Integer | Specifies whether a domain name is connected to WAF.<br>● **0**: The domain name is not connected to WAF.<br>● **1**: The domain name is connected to WAF. |
| protocol | String | Specifies the protocol type. The options are **HTTP**, **HTTPS**, and **HTTP,HTTPS**. |
| certificate_id | String | Specifies the certificate ID. This parameter is returned only when **client_protocol** is set to **HTTPS**. |
| server | Array | Specifies the origin server information, including the **client_protocol**, **server_protocol**, **address**, and **port** fields.<br>● **client_protocol**: protocol type of the client. The options are **HTTP** and **HTTPS**.<br>● **server_protocol**: protocol used by WAF to forward client requests to the server. The options are **HTTP** and **HTTPS**.<br>● **address**: public IP address or domain name of the web server that the client accesses<br>● **port**: port number used by the web server. The value ranges from **0** to **65535**, for example, **8080**. |
| proxy | Boolean | Specifies whether a proxy is configured.<br>● **true**: A proxy is configured.<br>● **false**: No proxy is configured. |
| sip_header_name | String | Specifies the type of the source IP header. This parameter is returned only when **proxy** is set to **true**.<br>The options are as follows: **default**, **cloudflare**, **akamai**, and **custom**. |

| Parameter | Type | Description |
|---|---|---|
| sip_header_list | Array | Specifies the HTTP request header for identifying the real source IP address. This parameter is returned only when **proxy** is set to **true**.<br>● If **sip_header_name** is **default**, **sip_header_list** is **["X-Forwarded-For"]**.<br>● If **sip_header_name** is **cloudflare**, **sip_header_list** is **["CF-Connecting-IP", "X-Forwarded-For"]**.<br>● If **sip_header_name** is **akamai**, **sip_header_list** is **["True-Client-IP"]**.<br>● If **sip_header_name** is **custom**, you can customize a value. |
| timestamp | Long | Specifies the time when a domain name is created. |
| block_page | **BlockPage** object | Alarm page configuration |

**Table 4-23** BlockPage

| Parameter | Type | Description |
|---|---|---|
| template | String | Template name |
| custom_page | **CustomPage** object | Custom alarm page |
| redirect_url | String | URL |

**Table 4-24** CustomPage

| Parameter | Type | Description |
|---|---|---|
| status_code | String | Status code |
| content_type | String | The content type of the custom alarm page. The value can be **text/html**, **text/xml**, or **application/json**. |
| content | String | Configure the page content based on the value for **content_type**. |

## Example

**www.a.com** is used as an example.

Response example

```
{
        "id": "388a7789d55b41d1918b3088a8f1e7f3",
        "hostname": "www.a.com",

        "cname": "3249d21e5eb34d21be12fdc817fcb67d.waf.cloud.com",
        "txt_code": "3249d21e5eb34d21be12fdc817fcb67d",
        "sub_domain": "3249d21e5eb34d21be12fdc817fcb67d.www.a.com",
        "policy_id": "xxxxxxxxxxxxxx",
        "certificate_id": "xxxxxxxxxxxxxxxxxxx",
        "protect_status": 0,
        "access_status": 0,
        "protocol": "HTTP,HTTPS",

        "server": [
          {"client_protocol": "HTTPS", "server_protocol":"HTTP", "address":"X.X.X.X.", "port":443},
          {"client_protocol": "HTTP", "server_protocol":"HTTP", "address":"X.X.X.X", "port":80}
        ],
       "proxy": true,
       "sip_header_name": "default",
       "sip_header_list": ["X-Forwarded-For"],
       "timestamp": 1499817600
       "block_page" : {
       "template" : "default"
        },


}
```

## Status Code

**Table 4-25** describes the normal status code returned by the API.

**Table 4-25** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.2.4 Modifying the Configurations of a Domain Name

## Function Description

This API is used to modify basic configurations of a domain name.

## URI

- URI format

  PUT /v1/{project_id}/waf/instance/{instance_id}

- Parameter description

**Table 4-26** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| instance_id | Yes | String | Specifies the instance ID. |

## Request

Request parameters

**Table 4-27** Request parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate_id | No | String | Specifies the certificate ID. This parameter is not required when **client_protocol** is set to **HTTP**. |
| server | No | Array | Specifies the origin server information, including the **client_protocol**, **server_protocol**, **address**, and **port** fields.<br>● **client_protocol**: protocol type of the client. The options are **HTTP** and **HTTPS**.<br>● **server_protocol**: protocol used by WAF to forward client requests to the server. The options are **HTTP** and **HTTPS**.<br>● **address**: public IP address or domain name of the web server that the client accesses<br>● **port**: port number used by the web server. The value ranges from **0** to **65535**, for example, **8080**. |
| proxy | No | Boolean | Specifies whether a proxy is configured.<br>● **true**: A proxy is configured.<br>● **false**: No proxy is configured. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| sip_header_name | No | String | Specifies the type of the source IP header. This parameter is required only when **proxy** is set to **true**.<br>The options are as follows: **default**, **cloudflare**, **akamai**, and **custom**. |
| sip_header_list | No | Array | Specifies the HTTP request header for identifying the real source IP address. This parameter is required only when **proxy** is set to **true**.<br>● If **sip_header_name** is **default**, **sip_header_list** is **["X-Forwarded-For"]**.<br>● If **sip_header_name** is **cloudflare**, **sip_header_list** is **["CF-Connecting-IP", "X-Forwarded-For"]**.<br>● If **sip_header_name** is **akamai**, **sip_header_list** is **["True-Client-IP"]**.<br>● If **sip_header_name** is **custom**, you can customize a value. |

## Response

Response parameters

**Table 4-28** Request parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the domain ID. |
| hostname | String | Specifies the domain name. |
| cname | String | Specifies the CNAME value. For example, **efec1196267b41c399f2980ea4048517.waf.cloud.com**. |
| txt_code | String | Specifies the TXT record. This parameter is returned only when **proxy** is set to **true**. |
| sub_domain | String | Specifies the subdomain name. This parameter is returned only when **proxy** is set to **true**. |

| Parameter | Type | Description |
|---|---|---|
| policy_id | String | Specifies the policy ID. |
| protect_status | Integer | Specifies the WAF mode.<br>● **0**: disabled.<br>● **1**: enabled.<br>● **-1**: bypassed. |
| access_status | Integer | Specifies whether a domain name is connected to WAF.<br>● **0**: The domain name is not connected to WAF.<br>● **1**: The domain name is connected to WAF. |
| protocol | Integer | Specifies the protocol type. The options are **HTTP**, **HTTPS**, and **HTTP,HTTPS**. |
| certificate_id | String | Specifies the certificate ID. This parameter is returned only when **protocol** is set to **HTTPS**. |
| server | Array | Specifies the origin server information, including the **client_protocol**, **server_protocol**, **address**, and **port** fields. |
| proxy | Boolean | Specifies whether a proxy is configured.<br>● **true**: A proxy is configured.<br>● **false**: No proxy is configured. |
| sip_header_name | String | Specifies the type of the source IP header. This parameter is returned only when **proxy** is set to **true**.<br>The options are as follows: **default**, **cloudflare**, **akamai**, and **custom**. |
| sip_header_list | Array | Specifies the HTTP request header for identifying the real source IP address. This parameter is returned only when **proxy** is set to **true**.<br>● If **sip_header_name** is **default**, **sip_header_list** is **["X-Forwarded-For"]**.<br>● If **sip_header_name** is **cloudflare**, **sip_header_list** is **["CF-Connecting-IP", "X-Forwarded-For"]**.<br>● If **sip_header_name** is **akamai**, **sip_header_list** is **["True-Client-IP"]**.<br>● If **sip_header_name** is **custom**, you can customize a value. |
| timestamp | Long | Specifies the time when a domain name is created. |

## Examples

**www.a.com** is used as an example.

- Request example

```
{
  "certificate_id": "07fb6809a89241fca86ac6f69e34963d",
  "server": [
     {"client_protocol": "HTTPS","server_protocol": "HTTP", "address": "X.X.X.X","port": "8080"},
     {"client_protocol": "HTTP", "server_protocol": "HTTP", "address": "X.X.X.X", "port": "80"}
   ],
  "proxy": true,
   "sip_header_name": "default",
   "sip_header_list": ["X-Forwarded-For"]


}
```

- Response example

```
{
        "id": "388a7789d55b41d1918b3088a8f1e7f3",
        "hostname": "www.a.com",

        "cname": "3249d21e5eb34d21be12fdc817fcb67d.wafcloud.com",
        "txt_code": "3249d21e5eb34d21be12fdc817fcb67d",
        "sub_domain": "3249d21e5eb34d21be12fdc817fcb67d.www.a.com",
        "policy_id": "xxxxxxxxxxxxxx",
        "certificate_id": "xxxxxxxxxxxxxxxxxxx",
        "protect_status": 0,
        "access_status": 0,
        "protocol": "HTTP,HTTPS",

        "server": [
           {"client_protocol": "HTTPS", "server_protocol":"HTTP", "address":"X.X.X.X", "port":443},
           {"client_protocol": "HTTP", "server_protocol":"HTTP", "address":"X.X.X.X", "port":80}
        ],
       "proxy": true,
       "sip_header_name": "default",
        "sip_header_list": ["X-Forwarded-For"],
       "timestamp": 1499817600


}
```

## Status Code

**Table 4-29** describes the normal status code returned by the API.

**Table 4-29** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.2.5 Deleting a Domain Name

## Function Description

This API is used to delete a domain name.

**NOTICE**

Deleting a domain name relies on some components, such as DNS. These components may cause deletion failed.

## URI

- URI format

  DELETE /v1/{project_id}/waf/instance/{instance_id}?keepPolicy={keepPolicy}
- Parameter description

**Table 4-30** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| instance_id | Yes | String | Specifies the instance ID or domain ID. |
| keepPolicy | No | Boolean | Specifies whether to retain the policy when deleting a domain name.<br>● **true**: The policy is retained.<br>● **false**: The policy is deleted. |

## Request

Request parameters

None

## Response

Response parameters

None

## Status Code

**Table 4-31** describes the normal status code returned by the API.

**Table 4-31** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 204 | No Content | The server successfully processed the request and is not returning any content. |

For details about error status codes, see **Status Codes**.

# 4.1.3 Certificate Management

## 4.1.3.1 Obtaining the Certificate List

### Function Description

This API is used to obtain the certificate list of a user.

### URI

- URI format
  GET /v1/{project_id}/waf/certificate?offset={offset}&limit={limit}
- Parameter description

**Table 4-32** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |
| limit | No | Long | Specifies the maximum number of records displayed on each page. Its value ranges from **0** to **50**. The default value is **10**. If **limit** is **-1**, one page with 65535 records is displayed. |

### Request

Request parameters

None

## Response

Response parameters

**Table 4-33** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of certificates. |
| items | **Table 3** | Specifies the certificate objects. |

**Table 4-34 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the certificate ID. |
| name | String | Specifies the certificate name. |
| expireTime | Long | Specifies the time when the certificate expires. |
| timestamp | Long | Specifies the time when the certificate is uploaded. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
   "total": 2,
    "items": [
        {
          "id": "388a7789d55b41d1918b3088a8f1e7f3",
          "name": "cert_a",
          "timestamp": 1544756441859,
          "expireTime": 1545978662373
        }, {
          "id": "388a7789d55b41d1918b3088a8f1e7f4",
          "name": "cert_b",
          "timestamp": 1544756441859,
          "expireTime": 1545978662356
        }]
}
```

## Status Code

**Table 4-35** describes the normal status code returned by the API.

**Table 4-35** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.3.2 Uploading a Certificate

### Function Description

This API is used to upload a certificate.

### URI

- URI format
  POST /v1/{project_id}/waf/certificate
- Parameter description

**Table 4-36** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |

### Request

Request parameters

**Table 4-37** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | Yes | String | Specifies the certificate name. The maximum length is 256 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| content | Yes | String | Specifies the certificate content.<br>**NOTE**<br>- The following is an example of the obtained certificate content:<br>-----BEGIN CERTIFICATE-----<br>MIIDezCCAmOgAwIBAgIJAMJcdOLsrN3iMA0GCSqGSIb3DQEBCwUAMFQxCzAJBgNV<br>...<br>8qh1Vpk2FXoadOVze2fQFLBkkB7LPExj8Nrf76CJEA==<br>-----END CERTIFICATE-----<br>- Line endings are replaced with **\n** by default before uploading the certificate content. For example:<br>-----BEGIN CERTIFICATE-----**\n**MIIDezCCAmOgAwIBAgIJAMJcdOLsrN3iMA0GCSqGSIb3DQEBCwUAMFQxCzAJBgNV**\n**...**\n**8qh1Vpk2FXoadOVze2fQFLBkkB7LPExj8Nrf76CJEA==**\n**-----END CERTIFICATE----- |
| key | Yes | String | Specifies the private key.<br>**NOTE**<br>- The following is an example of the obtained private key:<br>-----BEGIN RSA PRIVATE KEY-----<br>MIIEowIBAAKCAQEAsj2QPAwXYcPDH0mvf6Jbej6RGgYlb4EFMS85BjKrKNPOTqZf<br>...<br>4j0RY9DeUgSLdy625BBmew2it9l/NynIScG4Ow6w8Bu4iBANGv94<br>-----END RSA PRIVATE KEY-----<br>- Line endings are replaced with **\n** by default before uploading the private key. For example:<br>----BEGIN RSA PRIVATE KEY----**\n**MIIEowIBAAKCAQEAsj2QPAwXYcPDH0mvf6Jbej6RGgYlb4EFMS85BjKrKNPOTqZf**\n**...**\n**4j0RY9DeUgSLdy625BBmew2it9l/NynIScG4Ow6w8Bu4iBANGv94**\n**-----END RSA PRIVATE KEY----- |

## Response

Response parameters

**Table 4-38** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the certificate ID. |
| name | String | Specifies the certificate name. |
| expireTime | Long | Specifies the time when the certificate expires. |
| timestamp | Long | Specifies the time when the certificate is uploaded. |

## Examples

A certificate named **cert_a** is used as an example.

- Request example

```
{
 "name": "cert_a",
 "content": "-----BEGIN CERTIFICATE-----
\nMIIDezCCAmOgAwIBAgIJAMJcdOLsrN3iMA0GCSqGSIb3DQEBCwUAMFQxCzAJBgNV\n...
\n8qh1Vpk2FXoadOVze2fQFLBkkB7LPExj8Nrf76CJEA==\n-----END CERTIFICATE-----",
 "key": "----BEGIN RSA PRIVATE KEY----
\nMIIEowIBAAKCAQEAsj2QPAwXYcPDH0mvf6Jbej6RGgYlb4EFMS85BjKrKNPOTqZf\n...
\n4j0RY9DeUgSLdy625BBmew2it9l/NynIScG4Ow6w8Bu4iBANGv94\n-----END RSA PRIVATE KEY-----"
}
```

- Response example

```
{
    "id": "388a7789d55b41d1918b3088a8f1e7f3",
    "name": "cert_b",
    "expireTime": 1565467166765,
    "timestamp": 1545467166765
}
```

## Status Code

Table 4-39 describes the normal status code returned by the API.

**Table 4-39** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.3.3 Querying a Certificate

## Function Description

This API is used to query information about a certificate.

## URI

- URI format
  GET /v1/{project_id}/waf/certificate/{certificate_id}
- Parameter description

**Table 4-40** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| certificate_id | Yes | String | Specifies the certificate ID. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-41** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the certificate ID. |
| name | String | Specifies the certificate name. |
| expireTime | Long | Specifies the time when the certificate expires. |
| timestamp | Long | Specifies the time when the certificate is uploaded. |

## Example

A certificate named **cert_b** is used as an example.

Response example

```
{
    "id": "388a7789d55b41d1918b3088a8f1e7f3",
    "name": "cert_b",
    "timestamp": 1545467166765,
    "expireTime": 1555467166765
}
```

## Status Code

Table 4-42 describes the normal status code returned by the API.

**Table 4-42** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.3.4 Changing the Name of a Certificate

## Function Description

This API is used to change the name of a certificate.

## URI

- URI format
  PUT /v1/{project_id}/waf/certificate/{certificate_id}
- Parameter description

**Table 4-43** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| certificate_id | Yes | String | Specifies the certificate ID. |

## Request

Request parameters

**Table 4-44** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | Yes | String | Specifies the certificate name. The maximum length is 256 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed. |

## Response

Response parameters

**Table 4-45** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the certificate ID. |
| name | String | Specifies the certificate name. |
| expireTime | Long | Specifies the time when the certificate expires. |
| timestamp | Long | Specifies the time when the certificate is uploaded. |

## Examples

A certificate named **cert_a** is used as an example.

- Request example
```
{
 "name": "cert_b"
}
```
- Response example
```
{
    "id": "388a7789d55b41d1918b3088a8f1e7f3",
    "name": "cert_b",
    "expireTime": 1565467166765,
    "timestamp": 1545467166765
}
```

## Status Code

**Table 4-46** describes the normal status code returned by the API.

**Table 4-46** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.3.5 Deleting a Certificate

## Function Description

This API is used to delete a certificate not associated with any domain name.

## URI

- URI format

  DELETE /v1/{project_id}/waf/certificate/{certificate_id}

- Parameter description

**Table 4-47** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| certificate_id | Yes | String | Specifies the certificate ID. |

## Request

Request parameters

None

## Response

Response parameters

None

## Status Code

**Table 4-48** describes the normal status code returned by the API.

**Table 4-48** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 204 | No Content | The server successfully processed the request and is not returning any content. |

For details about error status codes, see **Status Codes**.

# 4.1.3.6 Querying the Domain Name that A Certificate Secures

## Function Description

This API is used to query the domain name that a certificate secures.

## URI

- URI format

  GET /v1/{project_id}/waf/certificate/{certificate_id}/host
- Parameter description

**Table 4-49** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| certificate_id | Yes | String | Specifies the certificate ID. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-50** Parameter description

| Parameter | Type | Description |
|---|---|---|
| hostname | Array | Specifies the domain names. |

## Example

Response example

```
{
   "hostname": ["www.a.com","www.b.com"]
}
```

## Status Code

**Table 4-51** describes the normal status code returned by the API.

**Table 4-51** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.4 Protection Status and Domain Setup

### 4.1.4.1 Switching the WAF Mode

## Function Description

This API is used to switch the WAF mode.

## URI

- URI format
  PUT /v1/{project_id}/waf/instance/{instance_id}/protect_status
- Parameter description

**Table 4-52** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| instance_id | Yes | String | Specifies the instance ID. |

## Request

Request parameters

**Table 4-53** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| protect_status | Yes | Integer | Specifies the WAF mode of a domain name.<br>● **1**: enabled.<br>● **0**: disabled.<br>● **-1**: bypassed. That is, a client sends a request to the server without passing through WAF. |

## Response

Response parameters

**Table 4-54** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| protect_status | Yes | Integer | Specifies the WAF mode of a domain name.<br>- **1**: enabled.<br>- **0**: disabled.<br>- **-1**: bypassed. That is, a client sends a request to the server without passing through WAF. |

## Examples

**protect_status** with a value of **1** is used as an example.

- Request example
```
{
   "protect_status": 1
}
```
- Response example
```
{
   "protect_status": 1
}
```

## Status Code

**Table 4-55** describes the normal status code returned by the API.

**Table 4-55** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.4.2 Connecting a Domain Name to WAF

## Function Description

This API is used to connect a domain name to WAF.

## URI

- URI format
  PUT /v1/{project_id}/waf/instance/{instance_id}/access_status
- Parameter description

**Table 4-56** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| projecte_id | Yes | String | Specifies the project ID. |
| instance_id | Yes | String | Specifies the instance ID. |

## Request

Request parameters

**Table 4-57** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| access_status | Yes | Integer | Specifies whether a domain name is connected to WAF.<br>**1**: The domain name is connected to WAF. |

## Response

Response parameters

**Table 4-58** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| access_status | Yes | Integer | Specifies whether a domain name is connected to WAF.<br>● **1**: The domain name is connected to WAF.<br>● **0**: The domain name is not connected to WAF. |
| protect_status | Yes | Integer | Specifies the WAF mode of a domain name.<br>● **1**: enabled.<br>● **0**: disabled.<br>● **-1**: bypassed. That is, a client sends a request to the server without passing through WAF. |

## Examples

**access_status** with a value of **1** is used as an example.

- Request example

```
{
 "access_status": 1
}
```

- Response examples

  The following shows the response if the domain name is connected to WAF:

```
{
  "access_status": 1,
  "protect_status": 1
}
```

  The following shows the response if connection fails:

```
{
 "access_status": 0,
 "protect_status": 0
}
```

## Status Code

**Table 4-59** describes the normal status code returned by the API.

**Table 4-59** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.5 Policies

## 4.1.5.1 Querying All Policies

## Function Description

This API is used to query the list of policies.

## URI

- URI format

  GET /v1/{project_id}/waf/policy?policyname={policyname}&offset={offset}&limit={limit}

- Parameter description

**Table 4-60** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policyname | No | String | Specifies the policy name. GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip?offset={offset}&limit={limit} |
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |
| limit | No | Long | Specifies the maximum number of records displayed on each page. Value range: (**0**, **10**]. The default value is **10**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-61** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of policies. |
| items | **Table 3** | Specifies the policy objects. |

**Table 4-62 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the instance ID. |
| name | String | Specifies the policy name. |
| options | **Table 4** | Specifies whether a protection rule is enabled. |

| Parameter | Type | Description |
|---|---|---|
| action | Table 5 | Specifies the mode of Basic Web Protection.<br>● **block**: WAF blocks and logs detected attacks.<br>● **log**: WAF logs detected attacks only. |
| level | Integer | Specifies the protection level.<br>● **1**: low WAF detects wget, cURL, and more but does not detect XSS and command injection attacks in the header, so you may miss more vulnerabilities that in fact exist. If you find out that configured protection rules are affecting your services, adjust the protection level to **1**.<br>● **2**: medium By default, **2** is selected. In this level, WAF detects remote file inclusion, third-party software vulnerabilities, webshell, and cp and ftp commands.<br>● **3**: high WAF detects Netcat, Nmap, kill commands, and more. If you need stricter protection, select **3** to avoid unreported vulnerabilities but you may see more vulnerabilities that in fact unlikely exist. |
| full_detection | Boolean | Specifies the detection mode in Precise Protection.<br>● **true**: full detection. Full detection finishes all threat detections before blocking requests that meet Precise Protection specified conditions.<br>● **false**: instant detection. Instant detection immediately ends threat detection after blocking a request that meets Precise Protection specified conditions. |
| hosts | Array | Specifies the domain IDs. |

| Parameter | Type | Description |
|---|---|---|
| timestamp | Long | Specifies the time when a policy is created. |

**Table 4-63** options

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Specifies whether Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| common | Boolean | Specifies whether General Check in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler | Boolean | Specifies whether the master crawler detection switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_engine | Boolean | Specifies whether the Search Engine switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_scanner | Boolean | Specifies whether the Scanner switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_script | Boolean | Specifies whether the Script Tool switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Type | Description |
|---|---|---|
| crawler_other | Boolean | Specifies whether detection of other crawlers in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| webshell | Boolean | Specifies whether webshell detection in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| cc | Boolean | Specifies whether CC Attack Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| custom | Boolean | Specifies whether Precise Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| whiteblackip | Boolean | Specifies whether Blacklist and Whitelist is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| privacy | Boolean | Specifies whether Data Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| Ignore | Boolean | Specifies whether False Alarm Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| antitamper | Boolean | Specifies whether Web Tamper Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

**Table 4-64** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the mode of Basic Web Protection.<br>● **block**: WAF blocks and logs detected attacks.<br>● **log**: WAF logs detected attacks only. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
    "total": 2,
    "items": [
        {
          "id": "xxxxxxxxxxxxxxxxxxxxxxxx",
          "name": "policy_1",
          "action": {
              "category ": "block"
           },
           "options": {
               "webattack": true,
               "common": true,
               "crawler": true,
               "crawler_engine": true,
               "crawler_scanner": true,
               "crawler_script": true,
               "crawler_other": true,
               "webshell": true,
               "cc": true,
               "custom": true,
               "whiteblackip": true,
               "ignore": true,
               "privacy": true,
               "antitamper": true
            },
           "level": 1,
           "full_detection": false,
           "hosts": ["111111111111111111", "2222222222222222222"],
           "timestamp": 1499817612
        }, {
          "id": "xxxxxxxxxxxxxxxxxxxxxxxx",
          "name": "policy_2",
          "action": {
              "category": "block"
           },
           "options": {
               "webattack": true,
               "common": true,
               "crawler": true,
               "crawler_engine": true,
               "crawler_scanner": true,
               "crawler_script": true,
               "crawler_other": true,
               "webshell": true,
               "cc": true,
               "custom": true,
               "whiteblackip": true,
                "ignore": true,
                "privacy": true,
                "antitamper": true
             },
            "level": 1,
            "full_detection": false,
            "hosts": ["1111111111111111", "2222222222222222222"],
            "timestamp": 1499817612
        }
    ]
}
```

## Status Code

Table 4-65 describes the normal status code returned by the API.

**Table 4-65** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.5.2 Creating a Policy

## Function Description

This API is used to create a policy.

## URI

- URI format
  POST /v1/{project_id}/waf/policy
- Parameter description

**Table 4-66** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |

## Request

Request parameters

**Table 4-67** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | Yes | String | Specifies the policy name. The maximum length is 256 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed. |

## Response

Response parameters

**Table 4-68** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the instance ID. |
| name | String | Specifies the policy name. |
| options | **Table 4** | Specifies whether a protection rule is enabled. |
| action | **Table 5** | Specifies the mode of Basic Web Protection. The default value is **log**.<br>● **block**: WAF blocks and logs detected attacks.<br>● **log**: WAF logs detected attacks only. |
| level | Integer | Specifies the protection level.<br>● **1**: low<br>● **2**: medium<br>● **3**: high |
| full_detection | Boolean | Specifies the detection mode in Precise Protection. |
| hosts | Array | Specifies the domain IDs. |
| timestamp | Long | Specifies the time when a policy is created. |

**Table 4-69** options

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Specifies whether Basic Web Protection is enabled. By default, this function is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| common | Boolean | Specifies whether General Check in Basic Web Protection is enabled. By default, this function is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler | Boolean | Specifies whether the master crawler detection switch in Basic Web Protection is enabled. By default, this function is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_engine | Boolean | Specifies whether the Search Engine switch in Basic Web Protection is enabled. By default, this function is disabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_scanner | Boolean | Specifies whether the Scanner switch in Basic Web Protection is enabled. By default, this function is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_script | Boolean | Specifies whether the Script Tool switch in Basic Web Protection is enabled. By default, this function is disabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Type | Description |
|---|---|---|
| crawler_other | Boolean | Specifies whether detection of other crawlers in Basic Web Protection is enabled. By default, this function is disabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| webshell | Boolean | Specifies whether webshell detection in Basic Web Protection is enabled. By default, this function is disabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| cc | Boolean | Specifies whether CC Attack Protection is enabled. By default, this function is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| custom | Boolean | Specifies whether Precise Protection is enabled. By default, this function is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| whiteblackip | Boolean | Specifies whether Blacklist and Whitelist is enabled. By default, this function is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| privacy | Boolean | Specifies whether Data Masking is enabled. By default, this function is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Type | Description |
|---|---|---|
| Ignore | Boolean | Specifies whether False Alarm Masking is enabled. By default, this function is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| antitamper | Boolean | Specifies whether Web Tamper Protection is enabled. By default, this function is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

**Table 4-70** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the mode of Basic Web Protection. The default value is **log**.<br>● **block**: WAF blocks and logs detected attacks.<br>● **log**: WAF logs detected attacks only. |

## Examples

A policy named **policy_1** is used as an example.

- Request example

```
{
  "name": "policy_1"
}
```

- Response example

```
{
          "id": "xxxxxxxxxxxxxxxxxxxxxxxxxx",
          "name": "policy_1",
          "action": {
              "category": "block"
           },
           "options": {
               "webattack": true,
               "common": true,
               "crawler": true,
               "crawler_engine": true,
               "crawler_scanner": true,
               "crawler_script": true,
               "crawler_other": true,
               "webshell": true,
               "cc": true,
            "custom": true,
            "whiteblackip": true,
            "ignore": true,
            "privacy": true,
            "antitamper": true
          },
         "level": 1,
         "full_detection": false,
         "hosts": [],
         "timestamp": 1499817612
}
```

## Status Code

Table 4-71 describes the normal status code returned by the API.

**Table 4-71** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.5.3 Querying a Policy

## Function Description

This API is used to query details about a policy.

## URI

- URI format
  GET /v1/{project_id}/waf/policy/{policy_id}
- Parameter description

**Table 4-72** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-73** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the instance ID. |
| name | String | Specifies the policy name. |
| action | **Table 3** | Specifies the protective action after a rule is matched.<br>● **block**: block and log detected attacks.<br>● **log**: only log detected attacks. |
| options | **Table 4** | Specifies the protection switches. |
| level | Integer | Specifies the protection level.<br>● **1**: low<br>● **2**: medium<br>● **3**: high |
| full_detection | Boolean | Specifies the detection mode in Precise Protection.<br>● **true**: full detection. Full detection finishes all threat detections before blocking requests that meet Precise Protection specified conditions.<br>● **false**: instant detection. Instant detection immediately ends threat detection after blocking a request that meets Precise Protection specified conditions. |
| hosts | Array | Specifies the domain IDs. |
| timestamp | Long | Specifies the time when a policy is created. |

Table 4-74 action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the protective action.<br>● **block**: WAF blocks and logs detected attacks.<br>● **log**: WAF logs detected attacks only. |

Table 4-75 options

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Specifies whether Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| common | Boolean | Specifies whether General Check in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler | Boolean | Specifies whether the master crawler detection switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_engine | Boolean | Specifies whether the Search Engine switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_scanner | Boolean | Specifies whether the Scanner switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_script | Boolean | Specifies whether the Script Tool switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Type | Description |
|---|---|---|
| crawler_other | Boolean | Specifies whether detection of other crawlers in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| webshell | Boolean | Specifies whether webshell detection in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| cc | Boolean | Specifies whether CC Attack Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| custom | Boolean | Specifies whether Precise Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| whiteblackip | Boolean | Specifies whether Blacklist and Whitelist is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| privacy | Boolean | Specifies whether Data Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| Ignore | Boolean | Specifies whether False Alarm Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| antitamper | Boolean | Specifies whether Web Tamper Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

## Example

A policy named **policy_2** is used as an example.

Response example

```
{
        "id": "xxxxxxxxxxxxxxxxxxxxxxxxx",
        "name": "policy_2",
        "action": {
            "category": "block"
         },
         "options": {
             "webattack": true,
             "common": true,
             "crawler": true,
             "crawler_engine": true,
             "crawler_scanner": true,
             "crawler_script": true,
             "crawler_other": true,
             "webshell": true,
             "cc": true,
             "custom": true,
             "whiteblackip": true,
             "ignore": true,
             "privacy": true,
             "antitamper": true
          },
         "level": 1,
         "full_detection": false,
         "hosts": ["1111111111111111", "2222222222222222222"],
         "timestamp": 1499817612
}
```

## Status Code

**Table 4-76** describes the normal status code returned by the API.

**Table 4-76** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.5.4 Applying a Policy to Domain Names

### Function Description

This API is used to apply a policy to domain names.

### URI

- URI format

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

- Parameter description

**Table 4-77** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |

## Request

Request parameters

**Table 4-78** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| hosts | Yes | List | Specifies the domain IDs. |

## Response

Response parameters

**Table 4-79** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the policy ID. |
| name | String | Specifies the policy name. |
| action | **Table 4** | Specifies the protective action after a rule is matched.<br>● **block**: WAF blocks and logs detected attacks.<br>● **log**: WAF logs detected attacks only. |
| options | **Table 5** | Specifies the protection switches. |
| level | Integer | Specifies the protection level.<br>● **1**: low<br>● **2**: medium<br>● **3**: high |

| Parameter | Type | Description |
|---|---|---|
| full_detection | Boolean | Specifies the detection mode in Precise Protection.<br>● **true**: full detection. Full detection finishes all threat detections before blocking requests that meet Precise Protection specified conditions.<br>● **false**: instant detection. Instant detection immediately ends threat detection after blocking a request that meets Precise Protection specified conditions. |
| hosts | Array | Specifies the domain IDs. |
| timestamp | Long | Specifies the time when a policy is created. |

**Table 4-80 action**

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the protective action.<br>● **block**: block and log detected attacks.<br>● **log**: only log detected attacks. |

**Table 4-81 options**

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Specifies whether Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| common | Boolean | Specifies whether General Check in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Type | Description |
|---|---|---|
| crawler | Boolean | Specifies whether the master crawler detection switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_engine | Boolean | Specifies whether the Search Engine switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_scanner | Boolean | Specifies whether the Scanner switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_script | Boolean | Specifies whether the Script Tool switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_other | Boolean | Specifies whether detection of other crawlers in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| webshell | Boolean | Specifies whether webshell detection in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| cc | Boolean | Specifies whether CC Attack Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| custom | Boolean | Specifies whether Precise Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Type | Description |
|---|---|---|
| whiteblackip | Boolean | Specifies whether Blacklist and Whitelist is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| privacy | Boolean | Specifies whether Data Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| Ignore | Boolean | Specifies whether False Alarm Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| antitamper | Boolean | Specifies whether Web Tamper Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

## Examples

**policy_2** applying to domain IDs **de06e61829494691b51979b9a03d5dcb** and **563972cc974b43848c73ed1a86268136** is used as an example.

- Request example

```
{
  "hosts": [
     "de06e61829494691b51979b9a03d5dcb",
     "563972cc974b43848c73ed1a86268136"
   ]
}
```

- Response example

```
{
        "id": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
        "name": "policy_2",
        "action": {
            "category": "block"
         },
         "options": {
            "webattack": true,
            "common": true,
            "crawler": true,
            "crawler_engine": true,
            "crawler_scanner": true,
            "crawler_script": true,
            "crawler_other": true,
            "webshell": true,
            "cc": true,
            "custom": true,
            "whiteblackip": true,
            "ignore": true,
            "privacy": true,
            "antitamper": true
         },
         "level": 1,
         "full_detection": false,
         "hosts": ["de06e61829494691b51979b9a03d5dcb", "563972cc974b43848c73ed1a86268136"],
         "timestamp": 1499817612
}
```

## Status Code

Table 4-82 describes the normal status code returned by the API.

**Table 4-82** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.5.5 Updating a Policy

## Function Description

This API is used to update a policy.

## URI

- URI format

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

- Parameter description

**Table 4-83** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |

## Request

Request parameters

**Table 4-84** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | No | String | Specifies the policy name. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| action | No | **Table 3** | Specifies the protective action after a rule is matched.<br>- **block**: WAF blocks and logs detected attacks.<br>- **log**: WAF logs detected attacks only. |
| options | No | **Table 4** | Specifies the protection switches. |
| level | No | Integer | Specifies the protection level.<br>- **1**: low<br>- **2**: medium<br>- **3**: high |
| full_detection | No | Boolean | Specifies the detection mode in Precise Protection.<br>- **true**: full detection. Full detection finishes all threat detections before blocking requests that meet Precise Protection specified conditions.<br>- **false**: instant detection. Instant detection immediately ends threat detection after blocking a request that meets Precise Protection specified conditions. |

**Table 4-85** action

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | Yes | String | Specifies the protective action.<br>- **block**: WAF blocks and logs detected attacks.<br>- **log**: WAF logs detected attacks only. |

**Table 4-86** options

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| webattack | No | Boolean | Specifies whether Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| common | No | Boolean | Specifies whether General Check in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler | No | Boolean | Specifies whether the master crawler detection switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_engine | No | Boolean | Specifies whether the Search Engine switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_scanner | No | Boolean | Specifies whether the Scanner switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_script | No | Boolean | Specifies whether the Script Tool switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_other | No | Boolean | Specifies whether detection of other crawlers in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| webshell | No | Boolean | Specifies whether webshell detection in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| cc | No | Boolean | Specifies whether CC Attack Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| custom | No | Boolean | Specifies whether Precise Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| whiteblackip | No | Boolean | Specifies whether Blacklist and Whitelist is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| privacy | No | Boolean | Specifies whether Data Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| Ignore | No | Boolean | Specifies whether False Alarm Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| antitamper | No | Boolean | Specifies whether Web Tamper Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

## Response

Response parameters

**Table 4-87** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the instance ID. |

| Parameter | Type | Description |
|---|---|---|
| name | String | Specifies the policy name. |
| options | **Table 9** | Specifies the protection switches. |
| action | **Table 6** | Specifies the mode of Basic Web Protection.<br>● **block**: WAF blocks and logs detected attacks.<br>● **log**: WAF logs detected attacks only. |
| level | Integer | Specifies the protection level.<br>● **1**: low<br>● **2**: medium<br>● **3**: high |
| full_detection | Boolean | Specifies the detection mode in Precise Protection.<br>● **true**: full detection. Full detection finishes all threat detections before blocking requests that meet Precise Protection specified conditions.<br>● **false**: instant detection. Instant detection immediately ends threat detection after blocking a request that meets Precise Protection specified conditions. |
| hosts | Array | Specifies the domain IDs. |
| timestamp | Long | Specifies the time when a policy is created. |

**Table 4-88** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the protective action.<br>● **block**: WAF blocks and logs detected attacks.<br>● **log**: WAF logs detected attacks only. |

**Table 4-89** options

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Specifies whether Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Type | Description |
|---|---|---|
| common | Boolean | Specifies whether General Check in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler | Boolean | Specifies whether the master crawler detection switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_engine | Boolean | Specifies whether the Search Engine switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_scanner | Boolean | Specifies whether the Scanner switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_script | Boolean | Specifies whether the Script Tool switch in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| crawler_other | Boolean | Specifies whether detection of other crawlers in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| webshell | Boolean | Specifies whether webshell detection in Basic Web Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| cc | Boolean | Specifies whether CC Attack Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

| Parameter | Type | Description |
|---|---|---|
| custom | Boolean | Specifies whether Precise Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| whiteblackip | Boolean | Specifies whether Blacklist and Whitelist is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| privacy | Boolean | Specifies whether Data Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| Ignore | Boolean | Specifies whether False Alarm Masking is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |
| antitamper | Boolean | Specifies whether Web Tamper Protection is enabled.<br>● **true**: enabled.<br>● **false**: disabled. |

## Examples

A policy named **policy_1** is used as an example.

- Request example

```
{
         "name": "policy_1",
         "action": {
             "category": "block"
          },
          "options": {
              "webattack": true,
              "common": true,
              "crawler": true,
              "crawler_engine": true,
              "crawler_scanner": true,
              "crawler_script": true,
              "crawler_other": true,
              "webshell": true,
              "cc": true,
              "custom": true,
              "whiteblackip": true,
              "ignore": true,
              "privacy": true,
              "antitamper": true
           },
          "level": 1,
          "full_detection": false
}
```

- Response example

```
{
        "id": "xxxxxxxxxxxxxxxxxxxxxxxxxx",
        "name": "policy_1",
        "action": {
           "category": "block"
         },
         "options": {
            "webattack": true,
            "common": true,
            "crawler": true,
            "crawler_engine": true,
            "crawler_scanner": true,
            "crawler_script": true,
            "crawler_other": true,
            "webshell": true,
            "cc": true,
            "custom": true,
            "whiteblackip": true,
            "ignore": true,
            "privacy": true,
            "antitamper": true
          },
         "level": 1,
         "full_detection": false,
         "hosts": [],
         "timestamp": 1499817612
}
```

## Status Code

**Table 4-90** describes the normal status code returned by the API.

**Table 4-90** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.5.6 Deleting a Policy

## Function Description

This API is used to delete a policy.

## URI

- URI format
  DELETE /v1/{project_id}/waf/policy/{policy_id}
- Parameter description

**Table 4-91** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |

## Request

Request parameters

None

## Response

Response parameters

None

## Status Code

**Table 4-92** describes the normal status code returned by the API.

**Table 4-92** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 204 | No Content | The server successfully processed the request and is not returning any content. |

For details about error status codes, see **Status Codes**.

# 4.1.6 Blacklist and Whitelist Rules

## 4.1.6.1 Querying Blacklist and Whitelist Rules

## Function Description

This API is used to query all blacklist and whitelist rules.

## URI

- URI format

  GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip?offset={offset}&limit={limit}
- Parameter description

**Table 4-93** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |
| limit | No | Long | Specifies the maximum number of records displayed on each page. Its value ranges from **0** to **50**. The default value is **10**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-94** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of rules. |
| items | **Table 3** | Specifies the blacklist or whitelist rule objects. |

**Table 4-95 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a blacklist or whitelist rule. |
| policy_id | String | Specifies the ID of the policy to which the rule belongs. |

| Parameter | Type | Description |
|---|---|---|
| addr | String | Specifies the public IP address or range (IP address and subnet mask). For example, *X.X.***0.125** or *X.X.***6.0/24**. |
| white | Integer | Specifies the IP address type.<br>● **1**: **Whitelist**<br>● **0**: **Blacklist** |
| timestamp | Long | Specifies the time when a blacklist or whitelist rule is added. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
  "total": 2,
  "items": [{
      "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
      "policy_id": "ertr45c0f96784ec8abd8ba61a98064ef",
      "addr": "X.X.0.125",
      "white": 1,
      "timestamp": 1499817600
    }, {
      "id": "44d887434169475794b2717438f7fa78",
      "policy_id": "ertr45c0f96784ec8abd8ba61a98064ef",
      "addr": "X.X.0.125",
      "white": 0,
      "timestamp": 1499817601
    }
  ]
}
```

## Status Code

**Table 4-96** describes the normal status code returned by the API.

**Table 4-96** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.6.2 Adding a Blacklist or Whitelist Rule

## Function Description

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

## URI

- URI format

  POST /v1/{project_id}/waf/policy/{policy_id}/whiteblackip
- Parameter description

**Table 4-97** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |

## Request

Request parameters

**Table 4-98** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| addr | Yes | String | Specifies the public IP address or range (IP address and subnet mask). For example, *X.X.***0.125** or *X.X.***6.0/24**. |
| white | No | Integer | Specifies the IP address type.<br>● **1**: **Whitelist**<br>● **0**: **Blacklist**<br>If you do not configure the **white** parameter, the value is **Blacklist** by default. |

## Response

Response parameters

**Table 4-99** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a blacklist or whitelist rule. |
| policy_id | String | Specifies the policy ID. |
| addr | String | Specifies the public IP address or range (IP address and subnet mask). For example, *X.X*.**0.125** or *X.X*.**6.0/24**. |
| white | Integer | Specifies the IP address type.<br>● **1**: **Whitelist**<br>● **0**: **Blacklist**<br>If you do not configure the **white** parameter, the value is **Blacklist** by default. |
| timestamp | Long | Specifies the time when a blacklist or whitelist rule is added. |

## Examples

*X.X*.**0.125** is used as an example.

- Request example

```
{
    "addr": "X.X.0.125",
    "white": 1
}
```

- Response example

```
{
  "id": "44d887434169475794b2717438f7fa78",
  "policy_id": "ertr45c0f96784ec8abd8ba61a98064ef",
  "addr": "X.X.0.125",
  "white": 1,
  "timestamp": 1499817600
}
```

## Status Code

**Table 4-100** describes the normal status code returned by the API.

**Table 4-100** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.6.3 Deleting a Blacklist or Whitelist Rule

## Function Description

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

## URI

- URI format

  DELETE /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{whiteblackip_rule_id}
- Parameter description

**Table 4-101** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| whiteblackip_rule_id | Yes | String | Specifies the ID of a blacklist or whitelist rule. |

## Request

Request

None

## Response

Response parameters

None

## Status Code

**Table 4-102** describes the normal status code returned by the API.

**Table 4-102** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 204 | No Content | The server successfully processed the request and is not returning any content. |

For details about error status codes, see **Status Codes**.

### 4.1.6.4 Querying a Blacklist or Whitelist Rule

## Function Description

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

## URI

- URI format

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

- Parameter description

**Table 4-103** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| whiteblackip_rule_id | Yes | String | Specifies the ID of a blacklist or whitelist rule. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-104** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a blacklist or whitelist rule. |
| policy_id | String | Specifies the policy ID. |
| addr | String | Specifies the public IP address or range (IP address and subnet mask). For example, *X.X.***0.125** or *X.X.***6.0/24**. |
| white | Integer | Specifies the IP address type.<br>● **1**: **Whitelist**<br>● **0**: **Blacklist** |

| Parameter | Type | Description |
|---|---|---|
| timestamp | Long | Specifies the time when a blacklist or whitelist rule is added. |

## Example

*X.X.***0.125** is used as an example.

Response example

```
{
  "id": "44d887434169475794b2717438f7fa78",
  "policy_id": "ertr45c0f96784ec8abd8ba61a98064ef",
  "addr": "X.X.0.125",
  "white": 0,
  "timestamp": 1499817600
}
```

## Status Code

**Table 4-105** describes the normal status code returned by the API.

**Table 4-105** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.6.5 Updating a Blacklist or Whitelist Rule

## Function Description

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

## URI

- URI format

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

- Parameter description

**Table 4-106** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| policy_id | Yes | String | Specifies the policy ID. |
| whiteblackip_rule_id | Yes | String | Specifies the ID of a blacklist or whitelist rule. |

## Request

Request parameters

**Table 4-107** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| addr | Yes | String | Specifies the public IP address or range (IP address and subnet mask). For example, *X.X.***0.125** or *X.X.***6.0/24**. |
| white | No | Integer | Specifies the IP address type.<br>- **1**: **Whitelist**<br>- **0**: **Blacklist** |

## Response

Response parameters

**Table 4-108** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a blacklist or whitelist rule. |
| policy_id | String | Specifies the policy ID. |
| addr | String | Specifies the public IP address or range (IP address and subnet mask). For example, *X.X.***0.125** or *X.X.***6.0/24**. |
| white | Integer | Specifies the IP address type.<br>- **1**: **Whitelist**<br>- **0**: **Blacklist**<br>If you do not configure the **white** parameter, the value is **Blacklist** by default. |

| Parameter | Type | Description |
|---|---|---|
| timestamp | Long | Specifies the time when a blacklist or whitelist rule is added. |

## Examples

*X.X.***0.125** is used as an example.

- Request example

```
{
 "addr": "X.X.0.125",
 "white": 1
}
```

- Response example

```
{
  "id": "44d887434169475794b2717438f7fa78",
  "policy_id": "ertr45c0f96784ec8abd8ba61a98064ef",
  "addr": "X.X.0.125",
  "white": 1,
  "timestamp": 1499817600
}
```

## Status Code

**Table 4-109** describes the normal status code returned by the API.

**Table 4-109** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.7 CC Attack Protection Rules

## 4.1.7.1 Querying CC Attack Protection Rules

## Function Description

This API is used to query all CC attack protection rules in a policy.

## URI

- URI format

  GET /v1/{project_id}/waf/policy/{policy_id}/cc?offset={offset}&limit={limit}

- Parameter description

**Table 4-110** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |
| limit | No | Long | Specifies the maximum number of records displayed on each page. Its value ranges from **0** to **50**. The default value is **10**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-111** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of CC attack protection rules in a policy. |
| items | **Table 3** | Specifies the CC attack protection rule objects. |

**Table 4-112 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a CC attack protection rule. |
| policy_id | String | Specifies the ID of the policy to which the rule belongs. |

| Parameter | Type | Description |
|---|---|---|
| path | String | Specifies the URL to which the rule applies, excluding a domain name.<br>● Prefix match: The path ending with * indicates that the path is used as a prefix. For example, if the path to be protected is **/admin/test.php** or **/adminabc**, set **Path** to **/admin***.<br>● Exact match: The path to be entered must match the path to be protected. If the path to be protected is **/admin**, set **url** to **/admin**. |
| limit_num | Integer | Specifies the number of requests allowed from a web visitor in a rate limiting period. |
| limit_period | Integer | Specifies the rate limiting period. |
| lock_time | Integer | Specifies the lock duration. The value ranges from **0** seconds to $\mathbf{2^{32}}$ seconds. |
| tag_type | String | Specifies the rate limit mode.<br>● **ip**: A web visitor is identified by the IP address.<br>● **cookie**: A web visitor is identified by the cookie key value.<br>● **other**: A web visitor is identified by the Referer field (user-defined request source). |
| tag_index | String | If **tag_type** is set to **cookie**, this parameter indicates cookie name. |
| tag_condition | Table 4 | Specifies the **Referer** (customized request source) field. This field is returned when **tag_type** is set to **other**. |

| Parameter | Type | Description |
|---|---|---|
| action | Table 5 | Specifies the action taken when the number of requests reaches the upper limit. |
| timestamp | Long | Specifies the time when a CC attack protection rule is added. |
| default | Boolean | Specifies whether the rule is the default CC attack protection rule.<br>● **true**: The rule is the default CC attack protection rule created by the system when creating a domain name.<br>● **false**: The rule is created by users. |

**Table 4-113 tag_condition**

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the category. The value is **Referer**. |
| contents | List | Specifies the category content. For example, **http://www.*xxx*.com**. |

**Table 4-114 action**

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the action. The default value is **block**.<br>● **block**: block the requests.<br>● **captcha**: Verification code. The user needs to enter the correct verification code after blocking to restore the correct access page.<br>The default value is **block**. |

| Parameter | Type | Description |
|---|---|---|
| detail | **Table 6** | Specifies the action details. If **detail** is **null**, the default block page is displayed by default. |

**Table 4-115** detail

| Parameter | Type | Description |
|---|---|---|
| response | **Table 7** | Specifies the returned page. |

**Table 4-116** response

| Parameter | Type | Description |
|---|---|---|
| content_type | String | Specifies the type of the returned page.<br>The options are **application/json**, **text/html**, and **text/xml**. |
| content | String | Specifies the content of the returned page. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
  "total": 2,
  "items": [{
      "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
      "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
      "path": "/abc1",
      "limit_num": 10,
      "limit_period": 60,
      "lock_time": 10,
      "tag_type": "cookie",
      "tag_index": "sesssionid",
      "action": {
        "category": "block",
        "detail": {
          "response": {
              "content_type": "application/json",
              "content": "{\"error\":\"forbidden\"}"
          }
        }
      },
      "timestamp": 1499817600,
      "default": true
    }, {
      "id": "3d7bea768b10480984f98c6b69d43d0f",
      "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
      "path": "/efgh",
      "limit_num": 10,
      "limit_period": 60,
      "lock_time": 5,
      "tag_type": "other",
      "tag_condition":{
          "category": "referer",
         "contents": ["http://www.example.com"]
       }
      "action": {
        "category": "block",
      },
      "timestamp": 1499817600,
      "default": true
    }
  ]
}
```

## Status Code

**Table 4-117** describes the normal status code returned by the API.

**Table 4-117** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.7.2 Adding a CC Attack Protection Rule

## Function Description

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

## URI

- URI format
  POST /v1/{project_id}/waf/policy/{policy_id}/cc
- Parameter description

**Table 4-118** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |

## Request

Request parameters

**Table 4-119** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| path | Yes | String | Specifies the URL to which the rule applies, excluding a domain name.<br>● Prefix match: The path ending with * indicates that the path is used as a prefix. For example, if the path to be protected is **/admin/test.php** or **/adminabc**, set **Path** to **/admin***.<br>● Exact match: The path to be entered must match the path to be protected. If the path to be protected is **/admin**, set **url** to **/admin**. |
| limit_num | No | Integer | Specifies the number of requests allowed from a web visitor in a rate limiting period. Value range: (0, $2^{32}$). The default value is 1. |
| limit_period | No | Integer | Specifies the rate limiting period. Value range: (0, $2^{32}$), in seconds. The default value is 1. |
| lock_time | No | Integer | Specifies the lock duration. The value ranges from **0** seconds to **$2^{32}$** seconds. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| tag_type | Yes | String | Specifies the rate limit mode.<br>● **ip**: A web visitor is identified by the IP address.<br>● **cookie**: A web visitor is identified by the cookie key value.<br>● **other**: A web visitor is identified by the Referer field (user-defined request source). |
| tag_index | No | String | If **tag_type** is set to **cookie**, this parameter indicates cookie name. |
| tag_condition | No | Table 3 | Specifies the **Referer** (customized request source) field. This field is mandatory when **tag_type** is set to **other**. |
| action | Yes | Table 4 | Specifies the action taken when the number of requests reaches the upper limit. |

**Table 4-120** tag_condition

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | Yes | String | Specifies the category. The value is **Referer**.<br>This parameter is mandatory when the **tag_condition** field is transferred. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| contents | Yes | List | Specifies the category content.<br>The format is as follows: **http://www.example.com/path**.<br>This parameter is mandatory when the **tag_condition** field is transferred. Currently, only one value is accepted. |

**Table 4-121** action

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | Yes | String | Specifies the action. The default value is **block**.<br>● **block**: block the requests.<br>● **captcha**: Verification code. The user needs to enter the correct verification code after blocking to restore the correct access page.<br>The default value is **block**.<br>If **tag_type** is set to **other**, this parameter value can only be **block**. |
| detail | No | **Table 5** | Specifies the action details. If **detail** is **null**, the default block page is displayed by default.<br>This parameter is not required if **category** is set to **captcha**.<br>This parameter is required if **category** is set to **block**. |

**Table 4-122** detail

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| response | Yes | Table 6 | Specifies the returned page. |

**Table 4-123** response

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| content_type | Yes | String | Specifies the type of the returned page.<br>The options are **application/json**, **text/html**, and **text/xml**.<br>The default value is **application/json**. |
| content | Yes | String | Specifies the content of the returned page. |

## Response

Response parameters

**Table 4-124** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a CC attack protection rule. |
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies the URL to which the rule applies. |
| limit_num | Integer | Specifies the number of requests allowed from a web visitor in a rate limiting period. |
| limit_period | Integer | Specifies the rate limiting period. |
| lock_time | Integer | Specifies the lock duration. The value ranges from **0** seconds to $\mathbf{2^{32}}$ seconds. |

| Parameter | Type | Description |
|---|---|---|
| tag_type | String | Specifies the rate limit mode.<br>- **ip**: A web visitor is identified by the IP address.<br>- **cookie**: A web visitor is identified by the cookie key value.<br>- **other**: A web visitor is identified by the Referer field (user-defined request source). |
| tag_index | String | If **tag_type** is set to **cookie**, this parameter indicates cookie name. |
| tag_condition | **Table 8** | Specifies the **Referer** (customized request source) field. This field is returned when **tag_type** is set to **other**. |
| action | **Table 9** | Specifies the action taken when the number of requests reaches the upper limit. |
| timestamp | Long | Specifies the time when a CC attack protection rule is added. |
| default | Boolean | Specifies whether the rule is the default CC attack protection rule.<br>- **true**: The rule is the default CC attack protection rule created by the system when creating a domain name.<br>- **false**: The rule is created by users. |

**Table 4-125 tag_condition**

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the category. The value is **Referer**. |
| contents | List | Specifies the category content. |

**Table 4-126** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the action. The default value is **block**.<br>● **block**: block the requests.<br>● **captcha**: Verification code. The user needs to enter the correct verification code after blocking to restore the correct access page.<br>The default value is **block**.<br>If **tag_type** is set to **other**, this parameter value can only be **block**. |
| detail | Table 10 | Specifies the action details. If **detail** is **null**, the default block page is displayed by default. |

**Table 4-127** detail

| Parameter | Type | Description |
|---|---|---|
| response | Table 11 | Specifies the returned page. |

**Table 4-128** response

| Parameter | Type | Description |
|---|---|---|
| content_type | String | Specifies the type of the returned page.<br>The options are **application/json**, **text/html**, and **text/xml**. |
| content | String | Specifies the content of the returned page. |

## Examples

- Request example

```
{
    "path": "/abc1",
    "limit_num": 10,
    "limit_period": 60,
    "lock_time": 10,
    "tag_type": "cookie",
    "tag_index": "sesssionid",
    "action": {
      "category": "block",
      "detail": {
        "response": {
            "content_type": "application/json",
            "content": "{\"error\":\"forbidden\"}"
        }
      }
    }
}
```

- Response example

```
{
    "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
    "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
    "path": "/abc1",
    "limit_num": 10,
    "limit_period": 60,
    "lock_time": 10,
    "tag_type": "cookie",
    "tag_index": "sesssionid",
    "action": {
      "category": "block",
      "detail": {
        "response": {
            "content_type": "application/json",
            "content": "{\"error\":\"forbidden\"}"
        }
      }
      },
    "timestamp": 1499817600,
    "default": false
}
```

## Status Code

**Table 4-129** describes the normal status code returned by the API.

**Table 4-129** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.7.3 Deleting a CC Attack Protection Rule

## Function Description

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

## URI

- URI format

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

- Parameter description

**Table 4-130** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| ccrule_id | Yes | String | Specifies the ID of a CC attack protection rule. |

## Request

Request parameters

None

## Response

Response parameters

None

## Status Code

**Table 4-131** describes the normal status code returned by the API.

**Table 4-131** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 204 | No Content | The server successfully processed the request and is not returning any content. |

For details about error status codes, see **Status Codes**.

# 4.1.7.4 Querying a CC Attack Protection Rule

## Function Description

This API is used to query details about a CC attack protection rule.

## URI

- URI format
  GET /v1/{project_id}/waf/policy/{policy_id}/cc/{ccrule_id}
- Parameter description

**Table 4-132** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| ccrule_id | Yes | String | Specifies the ID of a CC attack protection rule. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-133** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a CC attack protection rule. |
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies the URL to which the rule applies, excluding a domain name. |
| limit_num | Integer | Specifies the number of requests allowed from a web visitor in a rate limiting period. |
| limit_period | Integer | Specifies the rate limiting period. |
| lock_time | Integer | Specifies the lock duration. The value ranges from **0** seconds to **$2^{32}$** seconds. |

| Parameter | Type | Description |
|---|---|---|
| tag_type | String | Specifies the rate limit mode.<br>- **ip**: A web visitor is identified by the IP address.<br>- **cookie**: A web visitor is identified by the cookie key value.<br>- **other**: A web visitor is identified by the Referer field (user-defined request source). |
| tag_index | String | If **tag_type** is set to **cookie**, this parameter indicates cookie name. |
| tag_condition | **Table 3** | Specifies the **Referer** (customized request source) field. This field is returned when **tag_type** is set to **other**. |
| action | **Table 4** | Specifies the action taken when the number of requests reaches the upper limit. |
| timestamp | Long | Specifies the time when a CC attack protection rule is added. |
| default | Boolean | Specifies whether the rule is the default CC attack protection rule.<br>- **true**: The rule is the default CC attack protection rule created by the system when creating a domain name.<br>- **false**: The rule is created by users. |

**Table 4-134 tag_condition**

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the category. The value is **Referer**. |
| contents | List | Specifies the category content. |

**Table 4-135** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the action. The default value is **block**.<br>● **block**: block the requests.<br>● **captcha**: Verification code. The user needs to enter the correct verification code after blocking to restore the correct access page.<br>The default value is **block**.<br>If **tag_type** is set to **other**, this parameter value can only be **block**. |
| detail | **Table 5** | Specifies the action details. If **detail** is **null**, the default block page is displayed by default. |

**Table 4-136** detail

| Parameter | Type | Description |
|---|---|---|
| response | **Table 6** | Specifies the returned page. |

**Table 4-137** response

| Parameter | Type | Description |
|---|---|---|
| content_type | String | Specifies the type of the returned page.<br>The options are **application/json**, **text/html**, and **text/xml**. |
| content | String | Specifies the content of the returned page. |

## Example

- Response example

```
{
  "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
  "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
  "path": "/abc1",
  "limit_num": 10,
  "limit_period": 60,
  "lock_time": "",
  "tag_type": "cookie",
  "tag_index": "sesssionid",
  "action": {
    "category": "block",
    "detail": {
      "response": {
        "content_type": "application/json",
        "content": "{\"error\":\"forbidden\"}"
      }
    }
  },
  "timestamp": 1499817600,
   "default": false
}
```

## Status Code

Table 4-138 describes the normal status code returned by the API.

**Table 4-138** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.7.5 Updating a CC Attack Protection Rule

## Function Description

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

## URI

- URI format

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

- Parameter description

**Table 4-139** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| ccrule_id | Yes | String | Specifies the ID of a CC attack protection rule. |

## Request

Request parameters

**Table 4-140** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| path | Yes | String | Specifies the URL to which the rule applies, excluding a domain name. |
| limit_num | Yes | Integer | Specifies the number of requests allowed from a web visitor in a rate limiting period. The value ranges from **0** to **$2^{32}$**. |
| limit_period | Yes | Integer | Specifies the rate limiting period. The value ranges from **0** seconds to **$2^{32}$** seconds. |
| lock_time | No | Integer | Specifies the lock duration. The value ranges from **0** seconds to **$2^{32}$** seconds. |
| tag_type | Yes | String | Specifies the rate limit mode.<br>● **ip**: A web visitor is identified by the IP address.<br>● **cookie**: A web visitor is identified by the cookie key value.<br>● **other**: A web visitor is identified by the Referer field (user-defined request source). |
| tag_index | No | String | If **tag_type** is set to **cookie**, this parameter indicates cookie name. |
| tag_condition | No | Table 3 | Specifies the **Referer** (customized request source) field. This field is mandatory when **tag_type** is set to **other**. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| action | Yes | **Table 4** | Specifies the action taken when the number of requests reaches the upper limit. |

**Table 4-141** tag_condition

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | Yes | String | Specifies the category. The value is **Referer**.<br>This parameter is mandatory when the **tag_condition** field is transferred. |
| contents | Yes | List | Specifies the category content.<br>The format is as follows: **http://www.example.com/path**.<br>This parameter is mandatory when the **tag_condition** field is transferred. Currently, only one value is accepted. |

**Table 4-142** action

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | Yes | String | Specifies the action. The default value is **block**.<br>● **block**: block the requests.<br>● **captcha**: Verification code. The user needs to enter the correct verification code after blocking to restore the correct access page.<br>The default value is **block**.<br>If **tag_type** is set to **other**, this parameter value can only be **block**. |
| detail | No | Table 5 | Specifies the action details. If **detail** is **null**, the default block page is displayed by default.<br>This parameter is not required if **category** is set to **captcha**.<br>This parameter is required if **category** is set to **block**. |

**Table 4-143** detail

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| response | Yes | Table 6 | Specifies the returned page. |

**Table 4-144** response

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| content_type | Yes | String | Specifies the type of the returned page.<br>The options are **application/json**, **text/html**, and **text/xml**.<br>The default value is **application/json**. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| content | Yes | String | Specifies the content of the returned page. |

GET /v1/{project_id}/waf/policy/{policy_id}/custom?offset={offset}&limit={limit}

## Response

Response parameters

**Table 4-145** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a CC attack protection rule. |
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies the URL to which the rule applies, excluding a domain name. |
| limit_num | Integer | Specifies the number of requests allowed from a web visitor in a rate limiting period. |
| limit_period | Integer | Specifies the rate limiting period. |
| lock_time | Integer | Specifies the lock duration. The value ranges from **0** seconds to **2**$^{32}$ seconds. |
| tag_type | String | Specifies the tag object type. The value can be **cookie**, **ip**, or **other**. |
| tag_index | String | If **tag_type** is set to **cookie**, **index** indicates cookie name. |
| tag_condition | **Table 8** | This field is valid only when **tag_type** is set to **other**. |
| action | **Table 9** | Specifies the action taken when the number of requests reaches the upper limit. |
| timestamp | Long | Specifies the time when a CC attack protection rule is added. |

| Parameter | Type | Description |
|---|---|---|
| default | Boolean | Specifies whether the rule is the default CC attack protection rule.<br>● **true**: The rule is the default CC attack protection rule created by the system when creating a domain name.<br>● **false**: The rule is created by users. |

**Table 4-146** tag_condition

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the category. The value is **Referer**. |
| contents | List | Specifies the category content. |

**Table 4-147** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the action. The default value is **block**.<br>● **block**: block the requests.<br>● **captcha**: Verification code. The user needs to enter the correct verification code after blocking to restore the correct access page.<br>The default value is **block**.<br>If **tag_type** is set to **other**, this parameter value can only be **block**. |
| detail | **Table 10** | Specifies the action details. If **detail** is **null**, the default block page is displayed by default. |

**Table 4-148** detail

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| response | Yes | Table 11 | Specifies the returned page. |

**Table 4-149** response

| Parameter | Type | Description |
|---|---|---|
| content_type | String | Specifies the type of the returned page.<br>The options are **application/json**, **text/html**, and **text/xml**. |
| content | String | Specifies the content of the returned page. |

## Examples

- Request example

```
{
  "path": "/abc1",
  "limit_num": 10,
  "limit_period": 60,
  "lock_time": "",
  "tag_type": "cookie",
  "tag_index": "sesssionid",
  "action": {
    "category": "block",
    "detail": {
      "response": {
        "content_type": "application/json",
        "content": "{\'error\':\'forbidden\}"
      }
    }
  }
}
```

- Response example

```
{
  "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
  "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
  "path": "/abc1",
  "limit_num": 10,
  "limit_period": 60,
  "lock_time": "",
  "tag_type": "cookie",
  "tag_index": "sesssionid",
  "action": {
    "category": "block",
    "detail": {
      "response": {
        "content_type": "application/json",
        "content": "{\"error\":\"forbidden\"}"
      }
```

```
   }
 },
 "timestamp": 1499817600,
  "default": false
}
```

## Status Code

Table 4-150 describes the normal status code returned by the API.

**Table 4-150** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.8 Precise Protection Rules

## 4.1.8.1 Querying Precise Protection Rules

## Function Description

This API is used to query all precise protection rules in a policy.

## URI

- URI format
  GET /v1/{project_id}/waf/policy/{policy_id}/custom?offset={offset}&limit={limit}
- Parameter description

**Table 4-151** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| limit | No | Long | Specifies the maximum number of records displayed on each page. Its value ranges from **0** to **50**. The default value is **10**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-152** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of precise protection rules in a policy. |
| items | **Table 3** | Specifies the precise protection rule objects. |

**Table 4-153 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a precise protection rule. |
| policy_id | String | Specifies the policy ID. |
| name | String | Specifies the rule name. |
| conditions | **Table 4** | Specifies the condition parameters. If there are multiple conditions, the conditions must be met at the same time. |
| action | **Table 5** | Specifies the protective action after the precise protection rule is matched. |

| Parameter | Type | Description |
|---|---|---|
| time | Boolean | Specifies the effect time of the precise protection rule.<br>● **false**: The rule takes effect immediately.<br>● **true**: The rule takes effect at the scheduled time. |
| start | Long | Specifies the time when the precise protection rule takes effect. This parameter is returned only when **time** is **true**. |
| end | Long | Specifies the time when the precise protection rule expires. This parameter is returned only when **time** is **true**. |
| priority | Integer | Specifies the priority of a rule being executed. Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority. The value ranges from **0** to **65535**. |
| timestamp | Long | Specifies the time when a precise protection rule is added. |

**Table 4-154** conditions

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the condition type. The value can be **path**, **user-agent**, **ip**, **params**, **cookie**, **referer**, or **header**. |
| index | String | ● If **category** is set to **cookie**, **index** indicates cookie name.<br>● If **category** is set to **params**, **index** indicates param name.<br>● If **category** is set to **header**, **index** indicates an option in the header. |

| Parameter | Type | Description |
|---|---|---|
| logic | String | **contain**, **not_contain**, **equal**, **not_equal**, **prefix**, **not_prefix**, **suffix**, and **not_suffix** indicate **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, and **Suffix is not** respectively.<br>If **category** is set to **ip**, **logic** can only be **equal** or **not_equal**. |
| contents | List | Specifies content matching the condition. |

**Table 4-155** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the protective action.<br>● **block**: block.<br>● **pass**: allow. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
  "total": 2,
  "items": [{
      "id": "7374ad99c6c448e9a9ca35cb46660a39",
      "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
      "name": "rule1",
      "time": true,
      "start": 1499817600,
      "end": 1567817600,
      "conditions": [{
          "category": "path",
          "contents": ["/login"],
          "logic": "containi"
        },{
          "category": "ip",
           "logic": "equal",
           "contents": ["X.X.1.1"]
        }
      ],
      "action": {
        "category": "block"
      },

     "priority": 1,
     "timestamp": 1499817600
    }, {
      "id": "7374ad99c6c448e9a9ca35cb46660a39",
      "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
      "name": "rule2",
      "time": false,
      "conditions": [{
          "category": "path",
          "contents": ["/login"],
          "logic": "contain"
        },{
          "category": "ip",
           "logic": "equal",
           "contents": ["X.X.1.1"]
        }
      ],
      "action": {
        "category": "block"
      },

     "priority": 1,
     "timestamp": 1499817600
    }
  ]
}
```

## Status Code

Table 4-156 describes the normal status code returned by the API.

**Table 4-156** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.8.2 Adding a Precise Protection Rule

## Function Description

This API is used to add a precise protection rule.

## URI

- URI format

  POST /v1/{project_id}/waf/policy/{policy_id}/custom
- Parameter description

**Table 4-157** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |

## Request

Request parameters

**Table 4-158** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | Yes | String | Specifies the name of a precise protection rule. The maximum length is 256 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed. |
| time | No | Boolean | Specifies the effect time of the precise protection rule.<br>● **false**: The rule takes effect immediately.<br>● **true**: The rule takes effect at the scheduled time. |
| start | No | Long | Specifies the time when the precise protection rule takes effect. If **time** is set to **true**, either the start time or the end time must be set. |
| end | No | Long | Specifies the time when the precise protection rule expires. If **time** is set to **true**, either the start time or the end time must be set. |
| conditions | Yes | **Table 3** | Specifies the condition parameters. |
| action | Yes | **Table 4** | Specifies the protective action after the precise protection rule is matched. |
| priority | No | Integer | Specifies the priority of a rule being executed. Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority. The value ranges from **0** to **65535**. |

**Table 4-159** conditions

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | Yes | String | Specifies the condition type. The value can be **path**, **user-agent**, **ip**, **params**, **cookie**, **referer**, or **header**. |
| index | No | String | • If **category** is set to **cookie**, **index** indicates cookie name.<br>• If **category** is set to **params**, **index** indicates param name.<br>• If **category** is set to **header**, **index** indicates an option in the header. |
| logic | Yes | String | **contain**, **not_contain**, **equal**, **not_equal**, **prefix**, **not_prefix**, **suffix**, and **not_suffix** indicate **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, and **Suffix is not** respectively.<br>If **category** is set to **ip**, **logic** can only be **equal** or **not_equal**. |
| contents | Yes | List | Specifies content matching the condition. Currently, only one value is accepted. |

**Table 4-160** action

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | Yes | String | Specifies the protective action.<br>• **block**: block.<br>• **pass**: allow. |

## Response

Response parameters

**Table 4-161** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a precise protection rule. |
| policy_id | String | Specifies the ID of the policy to which the rule belongs. |
| name | String | Specifies the rule name. |
| conditions | **Table 6** | Specifies the condition parameters in the precise protection rule. |
| action | **Table 7** | Specifies the protective action after the precise protection rule is matched. |
| priority | Integer | Specifies the priority of a rule being executed. Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority. The value ranges from **0** to **65535**. |
| time | Boolean | Specifies the effect time of the precise protection rule.<br>● **false**: The rule takes effect immediately.<br>● **true**: The rule takes effect at the scheduled time. |
| start | Long | Specifies the time when the precise protection rule takes effect. |
| end | Long | Specifies the time when the precise protection rule expires. |
| timestamp | Long | Specifies the time when a precise protection rule is added. |

**Table 4-162** conditions

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the condition type. The value can be **path**, **user-agent**, **ip**, **params**, **cookie**, **referer**, or **header**. |
| index | String | ● If **category** is set to **cookie**, **index** indicates cookie name.<br>● If **category** is set to **params**, **index** indicates param name.<br>● If **category** is set to **header**, **index** indicates an option in the header. |
| logic | String | **contain**, **not_contain**, **equal**, **not_equal**, **prefix**, **not_prefix**, **suffix**, and **not_suffix** indicate **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, and **Suffix is not** respectively.<br>If **category** is set to **ip**, **logic** can only be **equal** or **not_equal**. |
| contents | List | Specifies content matching the condition. |

**Table 4-163** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the protective action.<br>● **block**: block.<br>● **pass**: allow. |

## Examples

A rule named **rule1** is used as an example.

- Request example

```
{
    "name": "rule1",
    "time": true,
    "start": 1499817600,
    "end": 1567817600,
     "conditions": [{
        "category": "path",
        "contents": ["/login"],
        "logic": "contain"
      },{
        "category": "ip",
         "logic": "equal",
         "contents": ["X.X.1.1"]
      }
     ],
     "action": {
       "category": "block"
     },
    "priority": 10
}
```

- Response example

```
{
     "id": "7374ad99c6c448e9a9ca35cb46660a39",
     "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
     "name": "rule1",
     "time": true,
     "start": 1499817600,
     "end": 1567817600,
     "conditions": [{
        "category": "path",
        "contents": ["/login"],
        "logic": "contain"
      },{
        "category": "ip",
         "logic": "equal",
         "contents": ["X.X.1.1"]
      }
     ],
     "action": {
       "category": "block"
     },

    "priority": 10,
    "timestamp": 1499817600
}
```

## Status Code

**Table 4-164** describes the normal status code returned by the API.

**Table 4-164** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.8.3 Deleting a Precise Protection Rule

## Function Description

This API is used to delete a precise protection rule.

## URI

- URI format

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

- Parameter description

**Table 4-165** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| custom_rule_id | Yes | String | Specifies the ID of a precise protection rule. |

## Request

Request parameters

None

## Response

Response parameters

None

## Status Code

**Table 4-166** describes the normal status code returned by the API.

**Table 4-166** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 204 | No Content | The server successfully processed the request and is not returning any content. |

For details about error status codes, see **Status Codes**.

# 4.1.8.4 Querying a Precise Protection Rule

## Function Description

This API is used to query details about a precise protection rule.

## URI

- URI format
  GET /v1/{project_id}/waf/policy/{policy_id}/custom/{custom_rule_id}
- Parameter description

**Table 4-167** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| custom_rule_id | Yes | String | Specifies the ID of a precise protection rule. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-168** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a precise protection rule. |
| policy_id | String | Specifies the policy ID. |
| name | String | Specifies the rule name. |
| time | Boolean | Specifies the effect time of the precise protection rule.<br>● **false**: The rule takes effect immediately.<br>● **true**: The rule takes effect at the scheduled time. |
| start | Long | Specifies the time when the precise protection rule takes effect. |
| end | Long | Specifies the time when the precise protection rule expires. |

| Parameter | Type | Description |
|---|---|---|
| conditions | Table 3 | Specifies the condition parameters. |
| action | Table 4 | Specifies the protective action after the precise protection rule is matched. |
| priority | Integer | Specifies the priority of a rule being executed. Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority. The value ranges from **0** to **65535**. |
| timestamp | Long | Specifies the time when a precise protection rule is added. |

**Table 4-169** conditions

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the condition type. The value can be **path**, **user-agent**, **ip**, **params**, **cookie**, **referer**, or **header**. |
| index | String | ● If **category** is set to **cookie**, **index** indicates cookie name.<br>● If **category** is set to **params**, **index** indicates param name.<br>● If **category** is set to **header**, **index** indicates an option in the header. |
| logic | String | **contain**, **not_contain**, **equal**, **not_equal**, **prefix**, **not_prefix**, **suffix**, and **not_suffix** indicate **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, and **Suffix is not** respectively.<br>If **category** is set to **ip**, **logic** can only be **equal** or **not_equal**. |

| Parameter | Type | Description |
|---|---|---|
| contents | List | Specifies content matching the condition. |

**Table 4-170** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the protective action.<br>● **block**: block.<br>● **pass**: allow. |

## Example

Rule ID **7374ad99c6c448e9a9ca35cb46660a39** is used as an example.

Response example

```
{
    "id": "7374ad99c6c448e9a9ca35cb46660a39",
    "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
    "name": "rule1",
    "time": true,
    "start": 1499817600,
    "end": 1567817600,
    "conditions": [{
        "category ": "path",
        "contents": ["/login"],
        "logic": "contain"
      },{
        "category": "ip",
        "logic": "equal",
        "contents": ["X.X.1.1"]
      }, {
        "category": "referer",
        "logic": "prefix",
        "contents": ["https://www.waf.com/xxx"]
      }, {
        "category": "user-agent",
        "logic": "contain",
        "contents": ["Mozilla/5.0"]
      }, {
        "category": "cookie",
        "index": "SID",
        "logic": 3,
        "contents": ["234SDFASR4R32412FSR325S"]
      }, {
        "category": "header",
        "index": "x-language",
        "logic": "equal",
        "contents": ["en-us"]
      }, {
        "category": "params",
        "index": "name",
        "logic": "equal",
        "contents": ["abc"]
      }
    ],
    "action": {
      "category": "block"
    },
  "priority": 10,
  "timestamp": 1499817600
}
```

## Status Code

Table 4-171 describes the normal status code returned by the API.

**Table 4-171** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.8.5 Updating a Precise Protection Rule

### Function Description

This API is used to update a precise protection rule.

### URI

- URI format
  PUT /v1/{project_id}/waf/policy/{policy_id}/custom/{custom_rule_id}
- Parameter description

**Table 4-172** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| custom_rule_id | Yes | String | Specifies the ID of a precise protection rule. |

### Request

Request parameters

**Table 4-173** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | Yes | String | Specifies the rule name. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| time | No | Boolean | Specifies the effect time of the precise protection rule.<br>● **false**: The rule takes effect immediately.<br>● **true**: The rule takes effect at the scheduled time. |
| start | No | Long | Specifies the time when the precise protection rule takes effect. If **time** is set to **true**, either the start time or the end time must be set. |
| end | No | Long | Specifies the time when the precise protection rule expires. If **time** is set to **true**, either the start time or the end time must be set. |
| conditions | Yes | **Table 3** | Specifies the condition parameters. |
| action | Yes | **Table 4** | Specifies the protective action after the precise protection rule is matched. |
| priority | No | Integer | Specifies the rule priority. The value ranges from **0** to **65535**. The default value is **50**. Smaller values correspond to higher priorities. |

**Table 4-174 conditions**

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | Yes | String | Specifies the condition type. The value can be **path**, **user-agent**, **ip**, **params**, **cookie**, **referer**, or **header**. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| index | No | String | - If **category** is set to **cookie**, **index** indicates cookie name.<br>- If **category** is set to **params**, **index** indicates param name.<br>- If **category** is set to **header**, **index** indicates an option in the header. |
| logic | Yes | String | **contain**, **not_contain**, **equal**, **not_equal**, **prefix**, **not_prefix**, **suffix**, and **not_suffix** indicate **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, and **Suffix is not** respectively.<br>If **category** is set to **ip**, **logic** can only be **equal** or **not_equal**. |
| contents | Yes | List | Specifies content matching the condition. Currently, only one value is accepted. |

**Table 4-175 action**

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | Yes | String | Specifies the protective action.<br>- **block**: block.<br>- **pass**: allow. |

## Response

Response parameters

**Table 4-176** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a precise protection rule. |

| Parameter | Type | Description |
|---|---|---|
| policy_id | String | Specifies the policy ID. |
| name | String | Specifies the rule name. |
| time | Boolean | Specifies the effect time of the precise protection rule.<br>● **false**: The rule takes effect immediately.<br>● **true**: The rule takes effect at the scheduled time. |
| start | Long | Specifies the time when the precise protection rule takes effect. |
| end | Long | Specifies the time when the precise protection rule expires. |
| conditions | **Table 6** | Specifies the condition parameters. |
| action | **Table 7** | Specifies the protective action after the precise protection rule is matched. |
| priority | Integer | Specifies the priority of a rule being executed. Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority. The value ranges from **0** to **65535**. |
| timestamp | Long | Specifies the time when a precise protection rule is added. |

**Table 4-177 conditions**

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the condition type. The value can be **path**, **user-agent**, **ip**, **params**, **cookie**, **referer**, or **header**. |

| Parameter | Type | Description |
|---|---|---|
| index | String | - If **category** is set to **cookie**, **index** indicates cookie name.<br>- If **category** is set to **params**, **index** indicates param name.<br>- If **category** is set to **header**, **index** indicates an option in the header. |
| logic | String | **contain**, **not_contain**, **equal**, **not_equal**, **prefix**, **not_prefix**, **suffix**, and **not_suffix** indicate **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, and **Suffix is not** respectively.<br>If **category** is set to **ip**, **logic** can only be **equal** or **not_equal**. |
| contents | List | Specifies content matching the condition. |

**Table 4-178** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Specifies the protective action.<br>- **block**: block.<br>- **pass**: allow. |

## Examples

A rule named **rule1** is used as an example.

- Request example

```
{
    "name": "rule1",
    "time": true,
    "start": 1499817600,
    "end": 1567817600,
    "conditions": [{
       "category": "path",
       "contents": ["/login"],
       "logic": "contain"
     },{
       "category": "ip",
        "logic": "equal",
        "contents": ["X.X.1.1"]
```

```
      }
    ],
    "action": {
      "category": "block"
    },
   "priority": 10
}
```

- Response example

```
{
    "id": "7374ad99c6c448e9a9ca35cb46660a39",
    "policy_id": "9tre832yf96784ec8abd8ba61a98064ef",
    "name": "rule1",
    "time": true,
    "start": 1499817600,
    "end": 1567817600,
    "conditions": [{
        "category": "path",
        "contents": ["/login"],
        "logic": "contain"
      },{
        "category": "ip",
         "logic": "equal",
         "contents": ["X.X.1.1"]
      }
    ],
    "action": {
      "category": "block"
    },

   "priority": 10,
   "timestamp": 1499817600
}
```

## Status Code

Table 4-179 describes the normal status code returned by the API.

**Table 4-179** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.9 Data Masking Rules

## 4.1.9.1 Querying Data Masking Rules

## Function Description

This API is used to query all data masking rules in a policy.

## URI

- URI format

GET /v1/{project_id}/waf/policy/{policy_id}/privacy?offset={offset}&limit={limit}

- Parameter description

**Table 4-180** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |
| limit | No | Long | Specifies the maximum number of records displayed on each page. Its value ranges from **0** to **50**. The default value is **10**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-181** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of rules. |
| items | **Table 3** | Specifies the data masking rule objects. |

**Table 4-182 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a data masking rule. |

| Parameter | Type | Description |
|---|---|---|
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies the URL to which the data masking rule applies (exact match by default). |
| category | String | Specifies the masked field. The options are **params** and **header**. |
| index | String | Specifies the masked subfield. |
| timestamp | Long | Specifies the time when a data masking rule is added. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
  "total": 2,
  "items": [{
      "id": "e1c0e55865544d1f8c95cf71df108c6b",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
      "path": "/login",
      "category": "params",
      "index": "password",
      "timestamp": 123243414132
    }, {
      "id": "d947d31c3e794b70a25e5e2057997f8e",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c89",
      "path": "/register",
      "category": "header",
      "index": "x-auth-token",
      "timestamp": 1343243243123
    }
  ]
}
```

## Status Code

**Table 4-183** describes the normal status code returned by the API.

**Table 4-183** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.9.2 Adding a Data Masking Rule

## Function Description

This API is used to add a data masking rule.

## URI

- URI format

  POST /v1/{project_id}/waf/policy/{policy_id}/privacy
- Parameter description

**Table 4-184** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |

## Request

Request parameters

**Table 4-185** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| path | Yes | String | Specifies the URL to which the data masking rule applies (exact match by default). |
| category | Yes | String | Specifies the masked field. The options are **params** and **header**. |
| index | Yes | String | Specifies the masked subfield. |

## Response

Response parameters

**Table 4-186** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a data masking rule. |

| Parameter | Type | Description |
|---|---|---|
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies the URL to which the data masking rule applies (exact match by default). |
| category | String | Specifies the masked field. The options are **params** and **header**. |
| index | String | Specifies the masked subfield. |
| timestamp | Long | Specifies the time when a data masking rule is added. |

## Examples

- Request example

```
{
  "path": "/login",
  "category": "params",
  "index": "name"
}
```

- Response example

```
{
    "id": "e1c0e55865544d1f8c95cf71df108c6b",
    "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
    "path": "/login",
    "category":"params",
    "index": "name",
    "timestamp": 123243414132
}
```

## Status Code

**Table 4-187** describes the normal status code returned by the API.

**Table 4-187** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.9.3 Deleting a Data Masking Rule

## Function Description

This API is used to delete a data masking rule.

## URI

- URI format

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

- Parameter description

**Table 4-188** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| privacy_rule_id | Yes | String | Specifies the ID of a data masking rule. |

## Request

Request parameters

None

## Response

Response parameters

None

## Status Code

**Table 4-189** describes the normal status code returned by the API.

**Table 4-189** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 204 | No Content | The server successfully processed the request and is not returning any content. |

For details about error status codes, see **Status Codes**.

# 4.1.9.4 Querying a Data Masking Rule

## Function Description

This API is used to query details about a data masking rule.

## URI

- URI format
  GET /v1/{project_id}/waf/policy/{policy_id}/privacy/{privacy_rule_id}
- Parameter description

**Table 4-190** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| privacy_rule_id | Yes | String | Specifies the ID of a data masking rule. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-191** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a data masking rule. |
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies the URL to which the data masking rule applies (exact match by default). |
| category | String | Specifies the masked field. The options are **params** and **header**. |
| index | String | Specifies the masked subfield. |
| timestamp | Long | Specifies the time when a data masking rule is added. |

## Example

Rule ID **e1c0e55865544d1f8c95cf71df108c6b** is used as an example.

Response example

```
{
  "id": "e1c0e55865544d1f8c95cf71df108c6b",
  "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
  "path": "/login",
  "category": "params",
  "index": "password",
  "timestamp": 12324435345
}
```

## Status Code

**Table 4-192** describes the normal status code returned by the API.

**Table 4-192** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.9.5 Updating a Data Masking Rule

## Function Description

This API is used to update a data masking rule.

## URI

- URI format

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

- Parameter description

**Table 4-193** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| privacy_rule_id | Yes | String | Specifies the ID of a data masking rule. |

## Request

Request parameters

**Table 4-194** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| path | Yes | String | Specifies the URL to which the data masking rule applies (exact match by default). |
| category | Yes | String | Specifies the masked field. The options are **params** and **header**. |
| index | Yes | String | Specifies the masked subfield. |

## Response

Response parameters

**Table 4-195** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a data masking rule. |
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies the URL to which the data masking rule applies (exact match by default). |
| category | String | Specifies the masked field. The options are **params** and **header**. |
| index | String | Specifies the masked subfield. |
| timestamp | Long | Specifies the time when a data masking rule is added. |

## Examples

- Request example

```
{
  "path": "/login",
  "category": "params",
  "index": "password"
}
```

- Response example

```
{
  "id": "e1c0e55865544d1f8c95cf71df108c6b",
  "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
  "path": "/login",
  "category": "params",
  "index": "password",
  "timestamp": 123434534543
}
```

## Status Code

**Table 4-196** describes the normal status code returned by the API.

**Table 4-196** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.10 Web Tamper Protection Rules

## 4.1.10.1 Querying Web Tamper Protection Rules

### Function Description

This API is used to query all web tamper protection rules in a policy.

### URI

- URI format

  GET /v1/{project_id}/waf/policy/{policy_id}/antitamper?offset={offset}&&limit={limit}

- Parameter description

**Table 4-197** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |
| limit | No | Long | Specifies the maximum number of records displayed on each page. Its value ranges from **0** to **50**. The default value is **10**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-198** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of web tamper protection rules in a policy. |
| items | **Table 3** | Specifies the web tamper protection rule objects. |

**Table 4-199 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a web tamper protection rule. |
| policy_id | String | Specifies the ID of the policy to which the rule belongs. |
| hostname | String | Specifies the domain name. |
| path | String | Specifies the URL protected by the web tamper protection rule, excluding a domain name. |
| timestamp | Long | Specifies the time when the cache is refreshed. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
  "total": 2,
  "items": [{
      "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
      "hostname": "www.aaa.com",
      "path": "/a",
      "timestamp": 1499817600
```

```
    }, {
      "id": "44d887434169475794b2717438f7fa78",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
      "hostname": "www.bbb.com",
      "path": "/b",
      "timestamp": 1499817600
    }
  ]
}
```

## Status Code

**Table 4-200** describes the normal status code returned by the API.

**Table 4-200** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.10.2 Adding a Web Tamper Protection Rule

## Function Description

This API is used to add a web tamper protection rule.

## URI

- URI format

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

- Parameter description

**Table 4-201** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |

## Request

Request parameters

**Table 4-202** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| hostname | Yes | String | Specifies the domain name. |
| path | Yes | String | Specifies the URL protected by the web tamper protection rule, excluding a domain name. |

## Response

Response parameters

**Table 4-203** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a web tamper protection rule. |
| policy_id | String | Specifies the policy ID. |
| hostname | String | Specifies the domain name. |
| path | String | Specifies the URL protected by the web tamper protection rule, excluding a domain name. |
| timestamp | Long | Specifies the time when the cache is refreshed. |

## Examples

Domain name **www.abc.com** is used as an example.

- Request example
```
{
  "hostname": "www.abc.com",
  "path": "/a"
}
```
- Response example
```
{
      "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
      "hostname": "www.abc.com",
      "path": "/a",
      "timestamp": 1499817600
}
```

## Status Code

Table 4-204 describes the normal status code returned by the API.

**Table 4-204** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.10.3 Deleting a Web Tamper Protection Rule

## Function Description

This API is used to delete a web tamper protection rule.

## URI

- URI format

  DELETE /v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamper_rule_id}

- Parameter description

**Table 4-205** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| antitamper_rule_id | Yes | String | Specifies the ID of a web tamper protection rule. |

## Request

Request parameters

None

## Response

Response parameters

None

## Status Code

**Table 4-206** describes the normal status code returned by the API.

**Table 4-206** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 204 | No Content | The server successfully processed the request and is not returning any content. |

For details about error status codes, see **Status Codes**.

## 4.1.10.4 Querying a Web Tamper Protection Rule

### Function Description

This API is used to query details about a web tamper protection rule.

### URI

- URI format

  GET /v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamper_rule_id}
- Parameter description

**Table 4-207** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| antitamper_rule_id | Yes | String | Specifies the ID of a web tamper protection rule. |

### Request

Request parameters

None

### Response

Response parameters

**Table 4-208** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a web tamper protection rule. |

| Parameter | Type | Description |
|---|---|---|
| policy_id | String | Specifies the policy ID. |
| hostname | String | Specifies the domain name. |
| path | String | Specifies the URL protected by the web tamper protection rule, excluding a domain name. |
| timestamp | Long | Specifies the time when the cache is refreshed. |

## Example

Rule ID **3a9b5c0f96784ec8abd8ba61a98064ef** is used as an example.

Response example

```
{
    "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
    "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
    "hostname": "www.aaa.com",
    "path": "/a",
    "timestamp": 1499817600
}
```

## Status Code

**Table 4-209** describes the normal status code returned by the API.

**Table 4-209** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.10.5 Refreshing the Web Tamper Protection Rule Cache

## Function Description

This API is used to refresh cache in a web tamper protection rule in the event of changes on the protected webpage.

## URI

- URI format

  POST /v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamper_rule_id}/cache

- Parameter description

**Table 4-210** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| antitamper_rule_id | Yes | String | Specifies the ID of a web tamper protection rule. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-211** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a web tamper protection rule. |
| policy_id | String | Specifies the policy ID. |
| hostname | String | Specifies the domain name. |
| path | String | Specifies the URL protected by the web tamper protection rule, excluding a domain name. |
| timestamp | Long | Specifies the time when the cache is refreshed. |

## Example

Response example

```
{
    "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
    "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
    "hostname": "www.aaa.com",
    "path": "/a",
    "timestamp": 1499817600
}
```

## Status Code

Table 4-212 describes the normal status code returned by the API.

**Table 4-212** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.11 False Alarm Masking Rules

## 4.1.11.1 Querying False Alarm Masking Rules

## Function Description

This API is used to query all false alarm masking rules in a policy.

## URI

- URI format

  GET /v1/{project_id}/waf/policy/{policy_id}/ignore?path={path}&offset={offset}&limit={limit}

- Parameter description

**Table 4-213** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| path | No | String | Specifies the misreported URL. |
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |
| limit | No | Long | Specifies the maximum number of records displayed on each page. Its value ranges from **0** to **50**. The default value is **10**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-214** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of policies. |
| items | **Table 3** | Specifies the false alarm masking rule objects. |

**Table 4-215 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a false alarm masking rule. |
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies a misreported URL excluding a domain name. |
| event_id | String | Specifies the event ID. |
| event_type | String | Specifies the event type. |
| rule | String | Specifies the rule ID, which consists of six digits and cannot be empty. |
| timestamp | Long | Specifies the time when a false alarm masking rule is added. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
  "total": 2,
  "items": [{
      "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
      "event_id": "02d3ac3cd99f440daf8d38e03cf0e2a6",
      "event_type": "xss",
      "rule": "100001",
      "timestamp": 1499817600,
      "path": "/a"
    }, {
      "id": "44d887434169475794b2717438f7fa78",
      "policy_id": "yuc0e55865544d1f8c95cf71df108c6b",
      "event_id": "f8c74b656a9d4d329dbcefe0969cc427",
      "event_type": "sqli",
      "rule": "100002",
      "timestamp": 1499817600,
      "path": "/a"
    }
  ]
}
```

## Status Code

**Table 4-216** describes the normal status code returned by the API.

**Table 4-216** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.11.2 Adding a False Alarm Masking Rule

### Function Description

This API is used to add a false alarm masking rule.

### URI

- URI format

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

- Parameter description

**Table 4-217** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |

### Request

Request parameters

**Table 4-218** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| path | Yes | String | Specifies a misreported URL excluding a domain name. |
| event_id | Yes | String | Specifies the event ID.<br>ID of a misreported event in **Events** whose type is not **Custom**. Click **Handle False Alarm** in the row containing the attack event to obtain the event ID. |

## Response

Response parameters

**Table 4-219** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a false alarm masking rule. |
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies a misreported URL excluding a domain name. |
| event_id | String | Specifies the event ID. |
| event_type | String | Specifies the event type. |
| timestamp | Long | Specifies the time when a false alarm masking rule is added. |
| rule | String | Specifies the rule ID, which consists of six digits and cannot be empty. |

## Examples

Rule ID **100001** is used as example.

- Request example

```
{
  "path": "/a",
  "event_id": "3737fb122f2140f39292f597ad3b7e9a"

}
```

- Response example

```
{
  "id": "6cdc116040d444f6b3e1bf1dd629f1d0",
  "policy_id": "44d887434169475794b2717438f7fa78",
  "path": "/a",
  "event_id": "3737fb122f2140f39292f597ad3b7e9a",
  "event_type": "xss",
  "rule": "100001",
  "timestamp": 1499817600
}
```

## Status Code

**Table 4-220** describes the normal status code returned by the API.

**Table 4-220** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.11.3 Deleting a False Alarm Masking Rule

## Function Description

This API is used to delete a false alarm masking rule.

## URI

- URI format
  DELETE /v1/{project_id}/waf/policy/{policy_id}/ignore/{ignore_rule_id}
- Parameter description

**Table 4-221** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| ignore_rule_id | Yes | String | Specifies the ID of a false alarm masking rule. |

## Request

Request parameters

None

## Response

Response parameters

None

## Status Code

Table 4-222 describes the normal status code returned by the API.

**Table 4-222** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 204 | No Content | The server successfully processed the request and is not returning any content. |

For details about error status codes, see **Status Codes**.

### 4.1.11.4 Querying a False Alarm Masking Rule

## Function Description

This API is used to query details about a false alarm masking rule.

## URI

- URI format
  GET /v1/{project_id}/waf/policy/{policy_id}/ignore/{ignore_id}
- Parameter description

**Table 4-223** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| ignore_id | Yes | String | Specifies the ID of a false alarm masking rule. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-224** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a false alarm masking rule. |
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies a misreported URL excluding a domain name. |
| event_id | String | Specifies the event ID. |
| event_type | String | Specifies the event type. |
| timestamp | Long | Specifies the time when a false alarm masking rule is added. |
| rule | String | Specifies the rule ID, which consists of six digits and cannot be empty. |

## Example

- Response example

```
{
  "id": "6cdc116040d444f6b3e1bf1dd629f1d0",
  "policy_id": "44d887434169475794b2717438f7fa78",
  "path": "/a",
  "event_id": "3737fb122f2140f39292f597ad3b7e9a",
  "event_type": "xss",
  "rule": "100001",
  "timestamp": 1499817600
}
```

## Status Code

**Table 4-225** describes the normal status code returned by the API.

**Table 4-225** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.11.5 Updating a False Alarm Masking Rule

## Function Description

This API is used to update a false alarm masking rule.

## URI

- URI format

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

- Parameter description

**Table 4-226** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| policy_id | Yes | String | Specifies the policy ID. |
| ignore_id | Yes | String | Specifies the ID of a false alarm masking rule. |

## Request

Request parameters

**Table 4-227** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| path | No | String | Specifies a misreported URL excluding a domain name. |
| event_id | No | String | Specifies the event ID.<br>It is the ID of a misreported event in **Events** whose type is not **Custom**. Click **Handle False Alarm** in the row containing the attack event to obtain the event ID. |

## Response

Response parameters

**Table 4-228** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a false alarm masking rule. |
| policy_id | String | Specifies the policy ID. |
| path | String | Specifies a misreported URL excluding a domain name. |
| event_id | String | Specifies the event ID. |
| event_type | String | Specifies the event type. |
| timestamp | Long | Specifies the time when a false alarm masking rule is added. |
| rule | String | Specifies the rule ID, which consists of six digits and cannot be empty. |

## Examples

- Request example

```
{
  "path": "/a",
  "event_id": "3737fb122f2140f39292f597ad3b7e9a"
}
```

- Response example

```
{
  "id": "6cdc116040d444f6b3e1bf1dd629f1d0",
  "policy_id": "44d887434169475794b2717438f7fa78",
  "path": "/a",
  "event_id": "3737fb122f2140f39292f597ad3b7e9a",
  "event_type": "xss",
  "rule": "100001",
  "timestamp": 1499817600
}
```

## Status Code

**Table 4-229** describes the normal status code returned by the API.

**Table 4-229** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.12 Event Logs

## 4.1.12.1 Querying Attack Event Logs

### Function Description

This API is used to query attack event logs.

### URI

- URI format

  GET /v1/{project_id}/waf/event?from={from}&to={to}&hosts={hostname}&attacks={attack}&sips={sip}&offset={offset}&limit={limit}

  **NOTE**

  An example of a URI is as follows:

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- Parameter description

**Table 4-230** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| from | Yes | Long | Specifies the start time (UTC) in milliseconds. For example, **1548172800000**. |
| to | Yes | Long | Specifies the end time (UTC) in milliseconds. For example, **1548431999000**. |
| hosts | No | Array | Specifies the domain IDs. |
| attacks | No | Array | Specifies the list of attack types. For example, **sqli** and **xss**. |
| sips | No | Array | Specifies the attack source IP addresses. For example, *X.X.***12.23** and *X.X.***20.85**. |
| nsips | No | Array | Specifies the excluded attack source IP addresses. For example, *X.X.***12.1** and *X.X.***20.2**. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |
| limit | No | Long | Specifies the maximum number of records displayed on each page. Its value ranges from **0** to **50**. The default value is **10**. |
| marker | No | String | Specifies the ID of the last event record on the previous page. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-231** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of event logs. |
| items | **Table 3** | Specifies the event log objects. |

**Table 4-232 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the event ID. |
| time | Integer | Specifies the attack time since Unix Epoch in milliseconds. |
| policy_id | String | Specifies the policy ID. |
| sip | String | Specifies an attack source IP address. |
| host | String | Specifies an attacked domain name. |

| Parameter | Type | Description |
|---|---|---|
| host_id | String | Specifies a domain name ID. |
| url | String | Specifies the attacked URL, excluding a domain name. |
| attack | String | Specifies the attack type.<br>● **cc** refers to CC attack.<br>● **cmdi** refers to command injection.<br>● **custom** refers to Precise Protection events.<br>● **illegal** refers to invalid requests.<br>● **sqli** refers to SQL injection.<br>● **lfi** refers to local file inclusion.<br>● **robot** refers to malicious crawlers.<br>● **antitamper** refers to Web Tamper Protection events.<br>● **rfi** refers to remote file inclusion.<br>● **vuln** refers to other types of attacks.<br>● **xss** refers to XSS attack.<br>● **whiteblackip** refers to Blacklist and Whitelist events.<br>● **webshell** refers to webshells. |
| rule | String | Specifies the matched rule ID that consists of six digits. |
| payload | String | Specifies the hit load. |

| Parameter | Type | Description |
|---|---|---|
| action | String | Specifies the protective action.<br>● **Block**: WAF blocks and logs detected attacks.<br>● **Log only**: WAF logs detected attacks only.<br>● **Allow**: WAF allows the requests that meet the specified conditions.<br>● **Verification code**: A verification code is displayed when the number of requests reaches the maximum limit in a CC attack protection rule. Upon completing the verification, you are no longer restricted by the maximum number of requests allowed.<br>● **Filter**: WAF implements data masking.<br>● **Mismatch**: The cached web page in the WAF engine does not match the original web page. |
| payload_location | String | Specifies the location in the request packet where the attack occurs. The options are as follows: **body**, **url**, **params**, and **header**. |
| request_line | String | Specifies the attack request method. |
| headers | Object | Specifies the attack request header. |
| cookie | String | Specifies the cookie. |
| body | String | Specifies the body of an attack request. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
  "total": 2,
  "items": [
  {
    "id": "0000-0000-0000-13-56ef71f5745764348192f844658dd144",
    "time": 1499817600,
    "policy_id": "xxx",
    "sip": "X.X.1.1",
    "host": "a.com",
    "host_id": "123",
    "url": "/login",
    "attack": "sqli",
    "rule": "20001",
    "payload": "1 or 1=1",
    "action": "block",
    "payload_location": "params",
    "request_line": "GET / ",
    "headers": {
      "Connection": "keep-alive",
      "User-Agent": "curl"
    },
    "cookie": "sid=123; uid=456",
    "body": "user=admin&pass=abc123"
  },
  {
    "id": "0000-0000-0000-13-56ef71f5745764348192f844658dd144",
    "time": 1499817600,
    "host": "a.com",
    "host_id": "a",
    "policy_id": "xxx",
    "sip": "X.X.1.2",
    "url": "/login",
    "attack": "sqli",
    "rule": "20001",
    "payload": "1 or 1=1",
    "action": "log",
    "payload_location": "params",
    "request_line": "GET / ",
    "headers": {
      "Connection": "keep-alive",
      "User-Agent": "curl"
    },
    "cookie": "sid=123; uid=456",
    "body": "user=admin&pass=abc123"
  }
 ]
}
```

## Status Code

**Table 4-233** describes the normal status code returned by the API.

**Table 4-233** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.12.2 Querying Attack Event Logs by ID

## Function Description

This API is used to query attack event logs by ID.

## URI

- URI format

  GET /v1/{project_id}/waf/event/{event_id}

- Parameter description

**Table 4-234** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| event_id | Yes | String | Specifies the event ID. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-235** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the event ID. |
| time | Integer | Specifies the attack time since Unix Epoch in milliseconds. |
| policy_id | String | Specifies the policy ID. |
| sip | String | Specifies an attack source IP address. |
| host | String | Specifies an attacked domain name. |
| host_id | String | Specifies a domain name ID. |
| url | String | Specifies the attacked URL, excluding a domain name. |
| attack | String | Specifies the attack type. |
| rule | String | Specifies the ID of the matched rule. |
| payload | String | Specifies the hit load. |

| Parameter | Type | Description |
|---|---|---|
| action | String | Specifies the protective action.<br>● **Block**: WAF blocks and logs detected attacks.<br>● **Log only**: WAF logs detected attacks only.<br>● **Allow**: WAF allows the requests that meet the specified conditions.<br>● **Verification code**: A verification code is displayed when the number of requests reaches the maximum limit in a CC attack protection rule. Upon completing the verification, you are no longer restricted by the maximum number of requests allowed.<br>● **Filter**: WAF implements data masking.<br>● **Mismatch**: The cached web page in the WAF engine does not match the original web page. |
| payload_location | String | Specifies the location in the request packet where the attack occurs. The options are as follows: **body**, **url**, **params**, and **header**. |
| request_line | String | Specifies the attack request method. |
| headers | Object | Specifies the attack request header. |
| cookie | String | Specifies the cookie. |
| body | String | Specifies the body of an attack request. |

## Example

Event ID **0000-0000-0000-13-56ef71f5745764348192f844658dd144** is used as an example.

Response example

```
{
    "id": "0000-0000-0000-13-56ef71f5745764348192f844658dd144",
     "time": 1499817600,
     "policy_id": "xxx",
     "sip": "X.X.1.1",
     "host": "a.com",
     "host_id": "123",
     "url": "/login",
     "attack": "sqli",
     "rule": "20001",
     "payload": "1 or 1=1",
     "action": "block",
     "payload_location": "params",
     "request_line": "GET / ",
     "headers": {
       "Connection": "keep-alive",
       "User-Agent": "curl"
     },
     "cookie": "sid=123; uid=456",
     "body": "user=admin&pass=abc123"
   }
```

## Status Code

**Table 4-236** describes the normal status code returned by the API.

**Table 4-236** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.12.3 Querying Event Distribution

## Function Description

This API is used to query event distribution.

## URI

- URI format

  GET /v1/{project_id}/waf/event/attack/type?from={from}&to={to}&hosts={hostids}

  **NOTE**

  An example of a URI is as follows:

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- Parameter description

**Table 4-237** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| from | Yes | Long | Specifies the start time (UTC) in milliseconds. For example, **1548172800000**. |
| to | Yes | Long | Specifies the end time (UTC) in milliseconds. For example, **1548431999000**. |
| hosts | No | Array | Specifies the domain IDs. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-238** Parameter description

| Parameter | Type | Description |
|---|---|---|
| xss | Integer | Specifies the number of XSS attacks detected within the time range. |
| sqli | Integer | Specifies the number of SQL injection attacks detected within the time range. |
| cmdi | Integer | Specifies the number of command injection attacks detected within the time range. |
| cc | Integer | Specifies the number of CC attacks detected within the time range. |
| custom | Integer | Specifies the number of Precise Protection events detected within the time range. |

| Parameter | Type | Description |
|---|---|---|
| illegal | Integer | Specifies the number of invalid requests detected within the time range. |
| lfi | Integer | Specifies the number of local file inclusion attacks detected within the time range. |
| robot | Integer | Specifies the number of malicious crawlers detected within the time range. |
| antitamper | Integer | Specifies the number of webpage tampering attacks detected within the time range. |
| rfi | Integer | Specifies the number of remote file inclusion attacks detected within the time range. |
| vuln | Integer | Specifies the number of other attacks detected within the time range. |
| whiteblackip | Integer | Specifies the number of Blacklist and Whitelist events detected within the time range. |
| webshell | Integer | Specifies the number of webshell attacks detected within the time range. |

## Example

Response example

```
{
    "xss": 150,
    "sqli": 321,
    "cmdi": 120,
    "robot": 10,
    "whiteblackip": 30,
    "custom": 50,
    "cc": 60,
    "illegal": 10
}
```

## Status Code

Table 4-239 describes the normal status code returned by the API.

**Table 4-239** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.12.4 Querying Request Statistics and Attack Statistics in a Specified Time Range

## Function Description

This API is used to query request statistics and attack statistics in a specified time range.

## URI

- URI format

  GET /v1/{project_id}/waf/event/timeline?from={from}&to={to}&timezone={timezone}&hosts={hostids}

  **NOTE**

  An example of a URI is as follows:

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- Parameter description

**Table 4-240** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| from | Yes | Long | Specifies the start time (UTC) in milliseconds. For example, **1548172800000**. |
| to | Yes | Long | Specifies the end time (UTC) in milliseconds. For example, **1548431999000**. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| timezone | No | String | Time zone. For example, the time zone for London is +00:00. The default value is **+00:00**. |
| hosts | No | Array | Specifies the domain IDs. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-241** Parameter description

| Parameter | Type | Description |
|---|---|---|
| requests | **Table 3** | Specifies request statistics. |
| attacks | **Table 4** | Specifies attack statistics. |

**Table 4-242 requests**

| Parameter | Type | Description |
|---|---|---|
| time | Integer | Specifies the end time since Unix Epoch in milliseconds. |
| num | Integer | Specifies the number of requests. |

**Table 4-243 attacks**

| Parameter | Type | Description |
|---|---|---|
| time | Integer | Specifies the end time since Unix Epoch in milliseconds. |
| num | Integer | Specifies the number of attacks. |

## Example

Response example

```
{
  "requests": [
       {"time": 1499817600, "num": 123400},
       {"time": 1499817601, "num": 123401},
       {"time": 1499817602, "num": 123402}
  ],
  "attacks": [
       {"time": 1499817600, "num": 1234},
       {"time": 1499817601, "num": 1235},
       {"time": 1499817602, "num": 1236}
  ]
}
```

## Status Code

**Table 4-244** describes the normal status code returned by the API.

**Table 4-244** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.12.5 Querying the Total Number of Attacks

## Function Description

This API is used to query the total number of attacks.

## URI

- URI format

  GET /v1/{project_id}/waf/event/attack/num?from={from}&to={to}&hosts={hostids}

  **NOTE**

  An example of a URI is as follows:

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- Parameter description

**Table 4-245** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| from | Yes | String | Specifies the start time (UTC) in milliseconds. For example, **1548172800000**. |
| to | Yes | String | Specifies the end time (UTC) in milliseconds. For example, **1548431999000**. |
| hosts | No | Array | Specifies the domain IDs. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-246** Parameter description

| Parameter | Type | Description |
|---|---|---|
| attack_num | Integer | Specifies the total number of attacks. |

## Example

Response example

```
{
  "attack_num":  150
}
```

## Status Code

**Table 4-247** describes the normal status code returned by the API.

**Table 4-247** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.12.6 Querying Top N Attack Source IP Addresses

## Function Description

This API is used to query the top N attack source IP addresses.

## URI

- URI format

  GET /v1/{project_id}/waf/event/attack/source?top={top}&from={from}&to={to}&hosts={hostids}

  **NOTE**

  An example of a URI is as follows:

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- Parameter description

**Table 4-248** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| top | No | Integer | Specifies the top *n* attack source IP addresses to be queried. The default value is **5**. |
| from | Yes | Long | Specifies the start time (UTC) in milliseconds. For example, **1548172800000**. |
| to | Yes | Long | Specifies the end time (UTC) in milliseconds. For example, **1548431999000**. |
| hosts | No | Array | Specifies the domain IDs. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-249** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of attack source IP addresses. |
| items | **Table 3** | Specifies the array of items. |

**Table 4-250 items**

| Parameter | Type | Description |
|---|---|---|
| ip | String | Specifies the attack source IP addresses. |
| num | Integer | Specifies the number of attacks came from the attack source IP addresses. |

## Example

Response example

```
{
  "total": 4,
  "items": [
     {"ip": "X.X.1.1", "num": 1000},
     {"ip": "X.X.1.2", "num": 1000},
     {"ip": "X.X.1.3", "num": 1000},
     {"ip": "X.X.1.4", "num": 1000}
   ]
}
```

## Status Code

**Table 4-251** describes the normal status code returned by the API.

**Table 4-251** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.12.7 Querying the Number of Attack Source IP Addresses

## Function Description

This API is used to query the number of attack source IP addresses.

## URI

- URI format

  GET /v1/{project_id}/waf/event/attack/source/num?from={from}&to={to}&hosts={hostids}

  NOTE

  An example of a URI is as follows:

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- Parameter description

**Table 4-252** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| from | Yes | Long | Specifies the start time (UTC) in milliseconds. For example, **1548172800000**. |
| to | Yes | Long | Specifies the end time (UTC) in milliseconds. For example, **1548431999000**. |
| hosts | No | Array | Specifies the domain IDs. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-253** Parameter description

| Parameter | Type | Description |
|---|---|---|
| sip | Integer | Specifies the number of attack source IP addresses. |

## Example

Response example

```
{
  "sip":  50
}
```

## Status Code

**Table 4-254** describes the normal status code returned by the API.

**Table 4-254** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.12.8 Querying the Total Number of Requests per Second

## Function Description

This API is used to query the total number of requests per second.

## URI

- URI format

  GET /v1/{project_id}/waf/event/request/peak?from={from}&to={to}&hosts={hostids}

  NOTE

  An example of a URI is as follows:

  GET /v1/3ac26c59e15a4a11bb680a103a29ddb6/waf/event/attack/type?from=1543976973635&to=1563976973635&hosts=3211757cafa3437aae24d760022e79ba&hosts=93029844064b43739b51ca63036fbc4b&hosts=34fe5f5c60ef4e43a9975296765d1217

- Parameter description

**Table 4-255** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| from | Yes | Long | Specifies the start time (UTC) in milliseconds. For example, **1548172800000**. |
| to | Yes | Long | Specifies the end time (UTC) in milliseconds. For example, **1548431999000**. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| hosts | No | Array | Specifies the domain IDs. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-256** Parameter description

| Parameter | Type | Description |
|---|---|---|
| qps | Integer | Specifies the total number of requests per second. |

## Example

Response example

```
{
"qps": 800
}
```

## Status Code

**Table 4-257** describes the normal status code returned by the API.

**Table 4-257** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.12.9 Querying the List of Event Log Files

## Function Description

This API is used to query the list of event log files.

## URI

- URI format
  GET /v1/{project_id}/waf/event/dump?offset={offset}&limit={limit}
- Parameter description

**Table 4-258** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| offset | No | Long | Specifies the number of returned pages. Its value ranges from **0** to **65535**. The default value is **0**. |
| limit | No | Long | Specifies the maximum number of records displayed on each page. Its value ranges from **0** to **50**. The default value is **10**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-259** Parameter description

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of log files. |
| items | **Table 3** | Specifies the log file objects. |

**Table 4-260 items**

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the ID of a log file. |
| filename | String | Specifies the name of a log file. |

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Specifies the total number of events in a log file. |
| url | String | Specifies the URL to download a log file. |
| timestamp | Long | Specifies the time when a log file is generated. |

## Example

**total** with a value of **2** is used as an example.

Response example

```
{
  "total": 2,
  "items": [{
      "id": "3a9b5c0f96784ec8abd8ba61a98064ef",
      "filename": "",
      "total": "100",
      "url": "https://obs_server/obs-waf-log/-2019-01-15-xxxxxxxxxx.csv?
AWSAccessKeyId=XXXXXXXXXXXX&Expires=1547632&Signature=nC7ipaGzLQs",
      "timestamp": 1499817600
    }, {
      "id": "44d887434169475794b2717438f7fa78",
      "filename": "W-2019-01-14.csv",
      "total": "200",
      "url": "https://obs_server/obs-waf-log/-2019-01-14-xxxxxxxxxx.csv?
AWSAccessKeyId=XXXXXXXXXXXX&Expires=1547632&Signature=nC7ipaGzLQs",
      "timestamp": 1499817601
    }
  ]
}
```

# 4.1.13 Alarm Notification

Only notifications that tenants have subscribed to can be viewed and modified.

## 4.1.13.1 Querying Alarm Notification Configurations

## Function Description

This API is used to query alarm notification configurations.

## URI

- URI format

  GET /v1/{project_id}/waf/config/alert
- Parameter description

**Table 4-261** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-262** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the unique ID of an alarm configuration. |
| enabled | Boolean | Specifies whether to send an alarm notification.<br>● **true**: Send the alarm notification.<br>● **false**: Do not send the alarm notification. |
| topic_urn | String | Specifies the SMN topic to which an alarm is sent. |
| sendfreq | Integer | Specifies the minimum interval between two alarms in minutes. The options are **5**, **15**, **30**, and **60**. |
| times | Integer | Specifies the alarm threshold. Alarm notifications are sent when the number of attacks is greater than or equal to the threshold within the configured period. This value is greater than or equal to **1**. |

| Parameter | Type | Description |
|---|---|---|
| threat | List<String> | Specifies the list of event types.<br>● **all** refers to all types of events.<br>● **cc** refers to CC attack.<br>● **cmdi** refers to command injection.<br>● **custom** refers to Precise Protection events.<br>● **illegal** refers to invalid requests.<br>● **sqli** refers to SQL injection.<br>● **lfi** refers to local file inclusion.<br>● **robot** refers to malicious crawlers.<br>● **antitamper** refers to Web Tamper Protection events.<br>● **rfi** refers to remote file inclusion.<br>● **vuln** refers to other types of attacks.<br>● **xss** refers to XSS attack.<br>● **whiteblackip** refers to Blacklist and Whitelist events.<br>● **webshell** refers to webshells. |
| locale | String | Specifies the language configuration. Only **zh-cn** and **en-us** are supported. The default value is **en-us**. |

## Example

Response example

```
{
    "id": "37b4bbe8a562453aa0163a96e6b71dd6",
    "enabled": true,
    "topic_urn": "urn:smn:eude:fca6f667ac5f4d9798d1641dfd38106b:wbtest",
    "sendfreq": 5,
    "times": 200,
    "threat": ["xss", "sqli", "cmdi"],
    "locale": "en-us"
}
```

## Status Code

Table 4-263 describes the normal status code returned by the API.

**Table 4-263** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

### 4.1.13.2 Updating Alarm Notification Configurations

## Function Description

This API is used to update alarm notification configurations.

## URI

- URI format
  PUT /v1/{project_id}/waf/config/alert/{alertconfig_id}
- Parameter description

**Table 4-264** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| alertconfig_id | Yes | String | Specifies the ID of the alarm notification configuration to be updated. For details about how to query the alarm configuration ID, see **Querying Alarm Notification Configurations**. |

## Request

Request parameters

**Table 4-265** Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| enabled | Yes | Boolean | Specifies whether to send an alarm notification.<br>● **true**: Send the alarm notification.<br>● **false**: Do not send the alarm notification. |
| topic_urn | Yes | String | Specifies the SMN topic to which an alarm is sent.<br>**NOTE**<br>The selected topic must be a topic whose subscription information has been configured on the SMN console. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| sendfreq | Yes | Integer | Specifies the minimum interval between two alarms in minutes. The options are **5**, **15**, **30**, and **60**. |
| times | Yes | Integer | Specifies the alarm threshold. Alarm notifications are sent when the number of attacks is greater than or equal to the threshold within the configured period. This value is greater than or equal to **1**. |
| threat | Yes | List<String> | Specifies the list of event types.<br>● **all** refers to all types of events.<br>● **cc** refers to CC attack.<br>● **cmdi** refers to command injection.<br>● **custom** refers to Precise Protection events.<br>● **illegal** refers to invalid requests.<br>● **sqli** refers to SQL injection.<br>● **lfi** refers to local file inclusion.<br>● **robot** refers to malicious crawlers.<br>● **antitamper** refers to Web Tamper Protection events.<br>● **rfi** refers to remote file inclusion.<br>● **vuln** refers to other types of attacks.<br>● **xss** refers to XSS attack.<br>● **whiteblackip** refers to Blacklist and Whitelist events.<br>● **webshell** refers to webshells. |
| locale | No | String | Specifies the language configuration. Only **zh-cn** and **en-us** are supported. The default value is **en-us**. |

## Response

Response parameters

**Table 4-266** Parameter description

| Parameter | Type | Description |
|---|---|---|
| id | String | Specifies the unique ID of an alarm configuration. |
| enabled | Boolean | Specifies whether to send an alarm notification.<br>● **true**: Send the alarm notification.<br>● **false**: Do not send the alarm notification. |
| topic_urn | String | Specifies the user-defined SMN topic. Users can receive alarm notifications by SMS or email. |
| sendfreq | Integer | Specifies the minimum interval between two alarms in minutes. The options are **5**, **15**, **30**, and **60**. |
| times | Integer | Specifies the alarm threshold. Alarm notifications are sent when the number of attacks is greater than or equal to the threshold within the configured period. This value is greater than or equal to **1**. |
| threat | List<String> | Specifies the list of event types.<br>● **all** refers to all types of events.<br>● **cc** refers to CC attack.<br>● **cmdi** refers to command injection.<br>● **custom** refers to Precise Protection events.<br>● **illegal** refers to invalid requests.<br>● **sqli** refers to SQL injection.<br>● **lfi** refers to local file inclusion.<br>● **robot** refers to malicious crawlers.<br>● **antitamper** refers to Web Tamper Protection events.<br>● **rfi** refers to remote file inclusion.<br>● **vuln** refers to other types of attacks.<br>● **xss** refers to XSS attack.<br>● **whiteblackip** refers to Blacklist and Whitelist events.<br>● **webshell** refers to webshells. |
| locale | String | Specifies the language configuration. Only **zh-cn** and **en-us** are supported. The default value is **en-us**. |

## Examples

- Request example

```
{
    "enabled": true,
    "topic_urn": "urn:smn:eude:fca6f667ac5f4d9798d1641dfd38106b:wbtest",
    "sendfreq": 5,
    "times": 200,
    "threat": ["xss", "sqli", "cmdi"]
}
```

- Response example

```
{
    "id": "37b4bbe8a562453aa0163a96e6b71dd6",
    "enabled": true,
    "topic_urn": "urn:smn:eude:fca6f667ac5f4d9798d1641dfd38106b:wbtest",
    "sendfreq": 5,
    "times": 200,
    "threat": ["xss", "sqli", "cmdi"],
    "locale": "en-us"
}
```

## Status Code

**Table 4-267** describes the normal status code returned by the API.

**Table 4-267** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.14 Obtaining Option Details

## 4.1.14.1 Querying Event Type in Alarm Notifications

## Function Description

This API is used to query event type in an alarm notification.

## URI

- URI format

  GET /v1/{project_id}/waf/map/threat?lang={lang}

- Parameter description

**Table 4-268** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| lang | No | String | Specifies the language configuration. The options are **zh-cn** and **en-us**. The default value is **en-us**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-269** Parameter description

| Parameter | Type | Description |
|---|---|---|
| threats | List | Specifies the list of event types. |
| locale | **Table 3** | Specifies event names. |

**Table 4-270 locale**

| Parameter | Type | Description |
|---|---|---|
| xss | String | Specifies XSS attack. |
| sqli | String | Specifies SQL injection. |
| cmdi | String | Specifies command injection. |
| cc | String | Specifies CC attack. |
| custom | String | Specifies Precise Protection. |
| illegal | String | Specifies invalid requests. |
| lfi | String | Specifies local file inclusion. |
| robot | String | Specifies malicious crawlers. |
| antitamper | String | Specifies Web Tamper Protection. |
| rfi | String | Specifies remote file inclusion. |

| Parameter | Type | Description |
|---|---|---|
| vuln | String | Specifies other types of attacks. |
| whiteblackip | String | Specifies Blacklist and Whitelist. |
| webshell | String | Specifies webshells. |

## Example

Response example

```
{
  "threats": ["xss", "sqli", "cmdi"],
  "locale": {
       "xss":  "Cross Site Scripting",
       "sqli": "SQL Injection",
       "cmdi": "Command Injection"
   }
}
```

## Status Code

**Table 4-271** describes the normal status code returned by the API.

**Table 4-271** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

## 4.1.14.2 Querying the Source IP Header

## Function Description

This API is used to query the source IP header.

## URI

- URI format

  GET /v1/{project_id}/waf/map/sipheader?lang={lang}

- Parameter description

**Table 4-272** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| lang | No | String | Specifies the language configuration. The options are **zh-cn** and **en-us**. The default value is **en-us**. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-273** Parameter description

| Parameter | Type | Description |
|---|---|---|
| sipheadermap | **Table 3** | Specifies the list of source IP headers. |
| locale | **Table 4** | Specifies additional information. |

**Table 4-274 sipheadermap**

| Parameter | Type | Description |
|---|---|---|
| default | Array | Specifies the default HTTP request header to identify the real source IP address. |
| cloudflare | Array | Specifies the HTTP request header used by Cloudflare to identify the real source IP address. |
| akamai | Array | Specifies the HTTP request header used by Akamai to identify the real source IP address. |

| Parameter | Type | Description |
|---|---|---|
| custom | Array | Specifies the custom HTTP request header to identify the real source IP address. |

**Table 4-275 locale**

| Parameter | Type | Description |
|---|---|---|
| default | String | The value is **Default**. |
| cloudflare | String | The value is **CloudFlare**. |
| akamai | String | The value is **Akamai**. |
| custom | String | The value is **Custom**. |

## Example

Response example

```
{
  "sipheadermap": {
      "default": ["X-Forwarded-For"],
      "cloudflare": ["CF-Connecting-IP", "X-Forwarded-For"],
      "akamai": ["True-Client-IP"],
      "custom": []
  },
  "locale": {
       "default": "Default",
       "cloudflare": "CloudFlare",
       "akamai": "Akamai",
       "custom": "Custom"
   }
}
```

## Status Code

**Table 4-276** describes the normal status code returned by the API.

**Table 4-276** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.1.15 Interconnecting with Cloud Eye

### 4.1.15.1 Querying the Instance Name and Status

## Function Description

This API is used to query the name and status of the instance for interconnecting with Cloud Eye.

## URI

- URI format
  GET /v1/{project_id}/waf/instance/{instance_id}/metrics
- Parameter description

**Table 4-277** Path parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Specifies the project ID. |
| instance_id | Yes | String | Specifies the instance ID. |

## Request

Request parameters

None

## Response

Response parameters

**Table 4-278** Parameter description

| Parameter | Type | Description |
|---|---|---|
| waf_instance_id | String | Specifies the identifier of a metric dimension. |
| name | String | Specifies the name of a resource instance. |
| status | String | Specifies the status of a resource instance. |

## Example

Response example

```
{
    "waf_instance_id": "dhbvhdfbvdhbasdkjvfhwoow",
    "name": "www.test.com",
    "status": "enable"
}
```

## Status Code

**Table 4-279** describes the normal status code returned by the API.

**Table 4-279** Status code

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |

For details about error status codes, see **Status Codes**.

# 4.2 Dedicated Mode

## 4.2.1 Dedicated Instance Management

### 4.2.1.1 Querying Dedicated WAF Instances

## Function

This API is used to query the list of dedicated WAF instances.

## URI

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

**Table 4-280** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

**Table 4-281** 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 4-282** 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.<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-283** 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 4-284** 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.<br>● **0**: Normal.<br>● **1**: Frozen. Resources and data will be retained, but the instance cannot be used.<br>● **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:<br>● **0**: Creating<br>● **1**: Running<br>● **2**: Deleting<br>● **3**: Deleted<br>● **4**: Creation failed<br>● **5**: Frozen<br>● **6**: Abnormal<br>● **7**: Updating<br>● **8**: Update failed |

| Parameter | Type | Description |
|---|---|---|
| access_status | Integer | Access status of the domain names protected with the dedicated WAF instance. The value can be **0** or **1**.<br>● **0**: the domain name is not connected with the dedicated WAF instance.<br>● **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**.<br>● **0**: The instance cannot be upgraded.<br>● **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. |
| instance_name | String | Names of the dedicated WAF instance. |

**Table 4-285** IdHostnameEntry

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain name ID. |
| hostname | String | Protected Domain Name |

**Status code: 400**

**Table 4-286** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-287** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-288** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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**.

# 4.2.1.2 Creating a Dedicated WAF Instance

## Function

This API is used to create a dedicated WAF instance.

## URI

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

**Table 4-289** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |

**Table 4-290** 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 4-291** 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.<br>Default: **application/json;charset=utf8** |

**Table 4-292** 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. |
| available_zone | Yes | String | AZ where the dedicated engine is to be created |
| arch | Yes | String | CPU architecture of the dedicated WAF instance, for example, x86. |
| instancename | Yes | String | Prefix of dedicated WAF engine names |
| specification | Yes | String | Specifications of the dedicated engine version. The value can be **waf.instance.enterprise** or **waf.instance.professional**. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cpu_flavor | Yes | String | ID of the specifications of the ECS hosting the dedicated engine. You can go to the management console and confirm supported specifications. |
| 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 | Yes | Boolean | Whether this is resource tenant.<br>● **true**: resource tenant. |

## Response Parameters

**Status code: 200**

**Table 4-293** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| instances | Array of **instanceInfo** objects | instances |

**Table 4-294** instanceInfo

| Parameter | Type | Description |
|---|---|---|
| id | String | ID of the dedicated WAF instance |
| name | String | Name of the dedicated WAF instance |

**Status code: 400**

**Table 4-295** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-296** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-297** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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",
  "cpu_flavor" : "c3ne.2xlarge.2",
  "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**.

# 4.2.1.3 Querying Details about a Dedicated WAF Instance

## Function

Querying Details about a Dedicated WAF Engine

## URI

GET /v1/{project_id}/premium-waf/instance/{instance_id}

**Table 4-298** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| instance_id | Yes | String | ID of the dedicated WAF instance. It can be obtained by calling the WAF ListInstance API |

**Table 4-299** 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 4-300** 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.<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-301** 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. |

| Parameter | Type | Description |
|---|---|---|
| status | Integer | Billing status of the dedicated WAF instance.<br>- **0**: Normal.<br>- **1**: Frozen. Resources and data will be retained, but the instance cannot be used.<br>- **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:<br>- **0**: Creating<br>- **1**: Running<br>- **2**: Deleting<br>- **3**: Deleted<br>- **4**: Creation failed<br>- **5**: Frozen<br>- **6**: Abnormal<br>- **7**: Updating<br>- **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 4-302** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-303** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-304** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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**.

## 4.2.1.4 Renaming a Dedicated WAF Instance

## Function

Renaming a Dedicated WAF Engine

## URI

PUT /v1/{project_id}/premium-waf/instance/{instance_id}

**Table 4-305** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| instance_id | Yes | String | ID of the dedicated WAF instance. It can be obtained by calling the WAF ListInstance API |

**Table 4-306** 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 4-307** 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.<br>Default: **application/json;charset=utf8** |

**Table 4-308** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| instancename | Yes | String | New name of the dedicated WAF engine |

## Response Parameters

**Status code: 200**

**Table 4-309** 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 |

| Parameter | Type | Description |
|---|---|---|
| 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.<br>● **0**: Normal.<br>● **1**: Frozen. Resources and data will be retained, but the instance cannot be used.<br>● **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:<br>● **0**: Creating<br>● **1**: Running<br>● **2**: Deleting<br>● **3**: Deleted<br>● **4**: Creation failed<br>● **5**: Frozen<br>● **6**: Abnormal<br>● **7**: Updating<br>● **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. |

| Parameter | Type | Description |
|---|---|---|
| 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 4-310** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-311** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-312** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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**.

### 4.2.1.5 Deleting a Dedicated WAF Instance

## Function

This API is used to delete a dedicated WAF instance.

## URI

DELETE /v1/{project_id}/premium-waf/instance/{instance_id}

**Table 4-313** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| instance_id | Yes | String | ID of the dedicated WAF instance. It can be obtained by calling the WAF ListInstance API |

**Table 4-314** 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 4-315** 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.<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-316** 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. |

| Parameter | Type | Description |
|---|---|---|
| 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.<br>● **0**: Normal.<br>● **1**: Frozen. Resources and data will be retained, but the instance cannot be used.<br>● **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:<br>● **0**: Creating<br>● **1**: Running<br>● **2**: Deleting<br>● **3**: Deleted<br>● **4**: Creation failed<br>● **5**: Frozen<br>● **6**: Abnormal<br>● **7**: Updating<br>● **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. |

| Parameter | Type | Description |
|---|---|---|
| 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 4-317** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-318** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-319** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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**.

# 4.2.2 Domain Names Protected by WAF

## 4.2.2.1 Adding a Domain Name to a Dedicated WAF Instance

## Function

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

## URI

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

**Table 4-320** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

**Table 4-321** 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 4-322** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| Content-Type | Yes | String | Content type<br>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 4-323** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificateid | No | String | HTTPS certificate ID. It can be obtained by calling the ListCertificates API.<br>● This parameter is not required if Client Protocol is set to HTTP.<br>● This parameter is mandatory if Client Protocol is set to HTTPS. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificatename | No | String | Certificate name.<br>- This parameter is not required if Client Protocol is set to HTTP.<br>- This parameter is mandatory if Client Protocol is set to HTTPS. |
| hostname | Yes | String | Domain name. For example, www.example.com or *.example.com. |
| proxy | Yes | Boolean | Whether a proxy is used.<br>- true: The proxy is enabled.<br>- false: The proxy is disabled. |
| policyid | No | String | ID of the policy initially used to the domain name. It can be obtained by calling the ListPolicy API. |
| server | Yes | Array of **PremiumWafServer** objects | Origin server list |
| access_progress | No | Array of **Access_progress** objects | Redundant parameter. It is used for console only. |

**Table 4-324** PremiumWafServer

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| front_protocol | Yes | String | Client protocol used to request access to the origin server.<br>Enumeration values:<br>- **HTTP**<br>- **HTTPS** |
| back_protocol | Yes | String | Server protocol used when WAF forwards client requests to the origin server.<br>Enumeration values:<br>- **HTTP**<br>- **HTTPS** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| address | Yes | String | Public IP address or domain name of the origin server that the client accesses. |
| port | Yes | Integer | Port number used by the web server. The value ranges from 0 to 65535, for example, 8080. |
| type | Yes | String | The origin server address is an IPv4 or IPv6 address.<br>Enumeration values:<br>● **ipv4**<br>● **ipv6** |
| vpc_id | Yes | String | VPC ID. Perform the following steps to obtain the VPC ID:<br>● 1.Find the name of the VPC where the dedicated engine is located. The VPC name is in the VPC\Subnet column. Log in to the WAF console and choose Instance Management > Dedicated Engine > VPC\Subnet.<br>● 2.Log in to the VPC console and click the VPC name. On the page displayed, copy the VPC ID in the VPC Information area. |

**Table 4-325** Access_progress

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| step | No | Integer | Step |
| status | No | Integer | Status |

## Response Parameters

**Status code: 200**

**Table 4-326** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Protected domain name ID |

| Parameter | Type | Description |
|---|---|---|
| policyid | String | Policy ID |
| hostname | String | Protected domain name |
| domainid | String | Tenant ID |
| projectid | String | Project ID |
| protocol | String | HTTP protocol |
| protect_status | Integer | WAF status of the protected domain name.<br>● -1: Bypassed. Requests are directly sent to the backend servers without passing through WAF.<br>● 0: Suspended. WAF only forwards requests for the domain name but does not detect attacks.<br>● 1: Enabled. WAF detects attacks based on the configured policy. |
| access_status | Integer | Whether a domain name is connected to WAF.<br>● 0: disconnected<br>● 1: connected |
| web_tag | String | Website name. |
| proxy | Boolean | Whether a proxy is used.<br>● true: The proxy is enabled.<br>● false: The proxy is disabled. |
| server | Array of **PremiumWafServer** objects | Origin server list |
| flag | **Flag** object | Special domain name identifier. This parameter is used for console only. |
| block_page | **BlockPage** object | Alarm configuration page |
| extend | Map<String,String> | Extended attribute |

**Table 4-327** PremiumWafServer

| Parameter | Type | Description |
|---|---|---|
| front_protocol | String | Client protocol used to request access to the origin server.<br>Enumeration values:<br>● **HTTP**<br>● **HTTPS** |
| back_protocol | String | Server protocol used when WAF forwards client requests to the origin server.<br>Enumeration values:<br>● **HTTP**<br>● **HTTPS** |
| address | String | Public IP address or domain name of the origin server that the client accesses. |
| port | Integer | Port number used by the web server. The value ranges from 0 to 65535, for example, 8080. |
| type | String | The origin server address is an IPv4 or IPv6 address.<br>Enumeration values:<br>● **ipv4**<br>● **ipv6** |
| vpc_id | String | VPC ID. Perform the following steps to obtain the VPC ID:<br>● 1.Find the name of the VPC where the dedicated engine is located. The VPC name is in the VPC\Subnet column. Log in to the WAF console and choose Instance Management > Dedicated Engine > VPC \Subnet.<br>● 2.Log in to the VPC console and click the VPC name. On the page displayed, copy the VPC ID in the VPC Information area. |

**Table 4-328** Flag

| Parameter | Type | Description |
|---|---|---|
| pci_3ds | String | Whether your website passes PCI 3DS check.<br>- true: Your website passed the PCI 3DS check.<br>- false: Your website failed the PCI 3DS check.<br>Enumeration values:<br>- **true**<br>- **false** |
| pci_dss | String | Whether your website passes PCI DSS check<br>- true: Your website passed the PCI DSS check.<br>- false: Your website failed the PCI DSS check.<br>Enumeration values:<br>- **true**<br>- **false** |
| cname | String | The CNAME record the domain name is using<br>- old: The domain name uses the old CNAME record.<br>- new: The domain name uses a new CNAME record.<br>Enumeration values:<br>- **old**<br>- **new** |
| is_dual_az | String | Whether WAF supports multi-AZ DR.<br>- true: WAF supports multi-AZ disaster recovery (DR).<br>- false: WAF does not support multi-AZ DR.<br>Enumeration values:<br>- **true**<br>- **false** |

**Table 4-329** BlockPage

| Parameter | Type | Description |
|---|---|---|
| template | String | Template name |
| custom_page | **CustomPage** object | Custom alarm page |
| redirect_url | String | Redirection URL |

**Table 4-330** CustomPage

| Parameter | Type | Description |
|---|---|---|
| status_code | String | Status code |
| content_type | String | Content type of alarm page |
| content | String | Page content |

**Status code: 400**

**Table 4-331** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-332** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-333** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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",
  "projectid" : "550500b49078408682d0d4f7d923f3e1",
  "domainid" : "d4ecb00b031941ce9171b7bc3386883f",
  "enterprise_project_id" : "0",
  "protect_status" : 1,
  "access_status" : 0,
  "web_tag" : "",
  "access_progress" : [ ]
}
```

## 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**.

## 4.2.2.2 Querying Domain Names Protected by Dedicated WAF Instances

## Function

This API is used for querying domain names protected by dedicated WAF engines.

## URI

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

**Table 4-334** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

**Table 4-335** 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 | String | Page number of the data to be returned in a query. The value range is 0 to 100000. The default value is 1, indicating that data on the first page is returned.<br>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.<br>Default: **10** |
| hostname | No | String | Protected domain name |
| policyname | No | String | Policy name |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| protect_status | No | Integer | WAF status of the protected domain name.<br>● -1: Bypassed. Requests are directly sent to the backend servers without passing through WAF.<br>● 0: Suspended: WAF only forwards requests for the domain name but does not detect attacks.<br>● 1: Enabled. WAF detects attacks based on the configured policy. |

## Request Parameters

**Table 4-336** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| Content-Type | Yes | String | Content type<br>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 4-337** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Total number of protected domain names |
| items | Array of **SimplePremiumWafHost** objects | Details about the protected domain name |

**Table 4-338** SimplePremiumWafHost

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain name ID |
| hostname | String | Domain name |
| policyid | String | Policy ID |
| protect_status | Integer | WAF status of the protected domain name.<br>● -1: Bypassed. Requests are directly sent to the backend servers without passing through WAF.<br>● 0: Suspended. WAF only forwards requests for the domain name but does not detect attacks.<br>● 1: Enabled. WAF detects attacks based on the configured policy. |
| access_status | Integer | Whether a domain name is connected to WAF.<br>● 0: disconnected<br>● 1: connected |
| flag | Map<String,String> | Special domain name identifier. This parameter is used for console only. |
| mode | String | Identifier of dedicated WAF engine in special WAF mode, such as ELB. |
| block_page | **BlockPage** object | Alarm configuration page |
| traffic_mark | **TrafficMark** object | Stream tag |
| extend | Map<String,String> | Extended field |
| circuit_breaker | **CircuitBreaker** object | Circuit breaker configuration |
| timeout_config | **TimeoutConfig** object | Timeout settings |
| access_progress | Array of **Access_progress** objects | Redundant parameter. It is used for console only. |

**Table 4-339** BlockPage

| Parameter | Type | Description |
|---|---|---|
| template | String | Template name |

| Parameter | Type | Description |
|---|---|---|
| custom_page | **CustomPage** object | Custom alarm page |
| redirect_url | String | Redirection URL |

**Table 4-340** CustomPage

| Parameter | Type | Description |
|---|---|---|
| status_code | String | Status code |
| content_type | String | Content type of alarm page |
| content | String | Page content |

**Table 4-341** TrafficMark

| Parameter | Type | Description |
|---|---|---|
| sip | Array of strings | IP address in the known attack source rule |
| cookie | String | cookie |
| params | String | Parameters |

**Table 4-342** CircuitBreaker

| Parameter | Type | Description |
|---|---|---|
| switch | Boolean | Circuit breaker switch |
| dead_num | Integer | Threshold for the number of unreachable origin servers. |
| dead_ratio | Number | Threshold for the percentage of unreachable origin servers. |
| block_time | Integer | Time to trigger the circuit breaker for unreachable origin servers. |
| superposition_num | Integer | Number of reached thresholds to trigger the circuit breaker. |
| suspend_num | Integer | Threshold for suspended connections. |
| sus_block_time | Integer | Time to trigger the circuit breaker for suspended connections. |

**Table 4-343** 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 4-344** Access_progress

| Parameter | Type | Description |
|---|---|---|
| step | Integer | Step |
| status | Integer | Status |

**Status code: 400**

**Table 4-345** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-346** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-347** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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" : "xx-xx-1",
    "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**.

### 4.2.2.3 Querying Domain Name Settings in Dedicated Mode

## Function

This API is used for querying domain name settings in dedicated mode.

## URI

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

**Table 4-348** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| host_id | Yes | String | ID of the domain name protected by the dedicated WAF engine |

**Table 4-349** 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 4-350** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| Content-Type | Yes | String | Content type<br>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 4-351** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain name ID |
| policyid | String | ID of the policy initially used to the domain name. It can be obtained by calling the ListPolicy API. |
| hostname | String | Domain name added to dedicated WAF. |
| domainid | String | User domain ID |
| project_id | String | Project ID |
| access_code | String | CNAME prefix |
| protocol | String | HTTP protocol |
| server | Array of **PremiumWaf Server** objects | Origin server details |
| certificateid | String | HTTPS certificate ID. It can be obtained by calling the ListCertificates API.<br>● This parameter is not required if Client Protocol is set to HTTP.<br>● This parameter is mandatory if Client Protocol is set to HTTPS. |
| certificatename | String | Certificate name.<br>● This parameter is not required if Client Protocol is set to HTTP.<br>● This parameter is mandatory if Client Protocol is set to HTTPS. |
| proxy | Boolean | Whether the proxy is enabled.<br>● true: The proxy is enabled.<br>● false: The proxy is disabled. |
| locked | Integer | Locked Status<br>Default: **0** |
| protect_status | Integer | WAF status of the protected domain name.<br>● -1: Bypassed. Requests are directly sent to the backend servers without passing through WAF.<br>● 0: Suspended. WAF only forwards requests for the domain name but does not detect attacks.<br>● 1: Enabled. WAF detects attacks based on the configured policy. |

| Parameter | Type | Description |
|---|---|---|
| access_status | Integer | Specifies whether a domain name is connected to WAF.<br>● 0: disconnected<br>● 1: connected |
| web_tag | String | Website name. |
| timestamp | Long | Time a domain name is added to WAF. |
| flag | **Flag** object | Special domain name identifier. This parameter is used for console only. |
| block_page | **BlockPage** object | Alarm configuration page |
| extend | Map<String,String> | Extended attribute |
| traffic_mark | **TrafficMark** object | Stream tag |
| timeout_config | **TimeoutConfig** object | Timeout settings |
| access_progress | Array of **Access_progress** objects | Redundant parameter. It is used for console only. |

**Table 4-352** PremiumWafServer

| Parameter | Type | Description |
|---|---|---|
| front_protocol | String | Client protocol used to request access to the origin server.<br>Enumeration values:<br>● **HTTP**<br>● **HTTPS** |
| back_protocol | String | Server protocol used when WAF forwards client requests to the origin server.<br>Enumeration values:<br>● **HTTP**<br>● **HTTPS** |
| address | String | Public IP address or domain name of the origin server that the client accesses. |
| port | Integer | Port number used by the web server. The value ranges from 0 to 65535, for example, 8080. |

| Parameter | Type | Description |
|---|---|---|
| type | String | The origin server address is an IPv4 or IPv6 address.<br>Enumeration values:<br>- **ipv4**<br>- **ipv6** |
| vpc_id | String | VPC ID. Perform the following steps to obtain the VPC ID:<br>- 1.Find the name of the VPC where the dedicated engine is located. The VPC name is in the VPC\Subnet column. Log in to the WAF console and choose Instance Management > Dedicated Engine > VPC \Subnet.<br>- 2.Log in to the VPC console and click the VPC name. On the page displayed, copy the VPC ID in the VPC Information area. |

**Table 4-353** Flag

| Parameter | Type | Description |
|---|---|---|
| pci_3ds | String | Whether your website passes PCI 3DS check.<br>- true: Your website passed the PCI 3DS check.<br>- false: Your website failed the PCI 3DS check.<br>Enumeration values:<br>- **true**<br>- **false** |
| pci_dss | String | Whether your website passes PCI DSS check<br>- true: Your website passed the PCI DSS check.<br>- false: Your website failed the PCI DSS check.<br>Enumeration values:<br>- **true**<br>- **false** |

| Parameter | Type | Description |
|---|---|---|
| cname | String | The CNAME record the domain name is using<br>- old: The domain name uses the old CNAME record.<br>- new: The domain name uses a new CNAME record.<br>Enumeration values:<br>- **old**<br>- **new** |
| is_dual_az | String | Whether WAF supports multi-AZ DR.<br>- true: WAF supports multi-AZ disaster recovery (DR).<br>- false: WAF does not support multi-AZ DR.<br>Enumeration values:<br>- **true**<br>- **false** |

**Table 4-354** BlockPage

| Parameter | Type | Description |
|---|---|---|
| template | String | Template name |
| custom_page | **CustomPage** object | Custom alarm page |
| redirect_url | String | Redirection URL |

**Table 4-355** CustomPage

| Parameter | Type | Description |
|---|---|---|
| status_code | String | Status code |
| content_type | String | Content type of alarm page |
| content | String | Page content |

**Table 4-356** TrafficMark

| Parameter | Type | Description |
|---|---|---|
| sip | Array of strings | IP address in the known attack source rule |

| Parameter | Type | Description |
|---|---|---|
| cookie | String | cookie |
| params | String | Parameters |

**Table 4-357** 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 4-358** Access_progress

| Parameter | Type | Description |
|---|---|---|
| step | Integer | Step |
| status | Integer | Status |

**Status code: 400**

**Table 4-359** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-360** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-361** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false"
  },
  "description" : "",
  "policyid" : "df15d0eb84194950a8fdc615b6c012dc",
  "domainid" : "0ee78615ca08419f81f539d97c9ee353",
  "projectid" : "550500b49078408682d0d4f7d923f3e1",
  "protect_status" : 1,
  "access_status" : 0,
  "certificateid" : "360f992501a64de0a65c50a64d1ca7b3",
  "certificatename" : "certificatename75315",
  "web_tag" : "",
  "timeout_config" : {
    "connect_timeout" : 30,
    "read_timeout" : 180,
    "send_timout" : 180
  }
}
```

## 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**.

# 4.2.2.4 Modifying a Domain Name Protected by a Dedicated WAF Instance

## Function

This API is used for modifying domain name settings in dedicated mode.

## URI

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

**Table 4-362** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| host_id | Yes | String | ID of the domain name protected by the dedicated WAF engine |

**Table 4-363** 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 4-364** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| Content-Type | Yes | String | Content type<br>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 4-365** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| proxy | No | Boolean | Whether a proxy is used.<br>● true: The proxy is enabled.<br>● false: The proxy is disabled. |
| certificateid | No | String | HTTPS certificate ID. It can be obtained by calling the ListCertificates API. |
| certificatename | No | String | HTTPS certificate name. It can be obtained by calling the ListCertificates API. |
| locked | No | Integer | Whether the host is locked. |
| protect_status | No | Integer | WAF status of the protected domain name.<br>● -1: Bypassed. Requests are directly sent to the backend servers without passing through WAF.<br>● 0: Suspended. WAF only forwards requests for the domain name but does not detect attacks.<br>● 1: Enabled. WAF detects attacks based on the configured policy. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| access_status | No | Integer | Whether a domain name is connected to WAF.<br>● 0: disconnected<br>● 1: connected |
| timestamp | No | Integer | Time stamp |
| block_page | No | **BlockPage** object | Alarm configuration page |
| traffic_mark | No | **TrafficMark** object | Stream tag |
| flag | No | Map<String,String> | Special domain name identifier. This parameter is used for console only. |
| extend | No | Map<String,String> | Extended field |
| circuit_breaker | No | **CircuitBreaker** object | Circuit breaker configuration |
| timeout_config | No | **TimeoutConfig** object | Timeout settings |

**Table 4-366** BlockPage

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| template | Yes | String | Template name |
| custom_page | No | **CustomPage** object | Custom alarm page |
| redirect_url | No | String | Redirection URL |

**Table 4-367** CustomPage

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| status_code | Yes | String | Status code |
| content_type | Yes | String | Content type of alarm page |
| content | Yes | String | Page content |

**Table 4-368** TrafficMark

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| sip | No | Array of strings | IP address in the known attack source rule |
| cookie | No | String | cookie |
| params | No | String | Parameters |

**Table 4-369** CircuitBreaker

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| switch | No | Boolean | Circuit breaker switch |
| dead_num | No | Integer | Threshold for the number of unreachable origin servers. |
| dead_ratio | No | Number | Threshold for the percentage of unreachable origin servers. |
| block_time | No | Integer | Time to trigger the circuit breaker for unreachable origin servers. |
| superposition_num | No | Integer | Number of reached thresholds to trigger the circuit breaker. |
| suspend_num | No | Integer | Threshold for suspended connections. |
| sus_block_time | No | Integer | Time to trigger the circuit breaker for suspended connections. |

**Table 4-370** 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 4-371** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain name ID |
| policyid | String | ID of the policy initially used to the domain name. It can be obtained by calling the ListPolicy API. |
| hostname | String | Domain name added to dedicated WAF. |
| domainid | String | User domain ID |
| project_id | String | Project ID |
| access_code | String | CNAME prefix |
| protocol | String | HTTP protocol |
| server | Array of **PremiumWaf Server** objects | Origin server details |
| certificateid | String | HTTPS certificate ID. It can be obtained by calling the ListCertificates API.<br>● This parameter is not required if Client Protocol is set to HTTP.<br>● This parameter is mandatory if Client Protocol is set to HTTPS. |
| certificatename | String | Certificate name.<br>● This parameter is not required if Client Protocol is set to HTTP.<br>● This parameter is mandatory if Client Protocol is set to HTTPS. |
| proxy | Boolean | Whether the proxy is enabled.<br>● true: The proxy is enabled.<br>● false: The proxy is disabled. |
| locked | Integer | Locked Status<br>Default: **0** |

| Parameter | Type | Description |
|---|---|---|
| protect_status | Integer | WAF status of the protected domain name.<br>- -1: Bypassed. Requests are directly sent to the backend servers without passing through WAF.<br>- 0: Suspended. WAF only forwards requests for the domain name but does not detect attacks.<br>- 1: Enabled. WAF detects attacks based on the configured policy. |
| access_status | Integer | Specifies whether a domain name is connected to WAF.<br>- 0: disconnected<br>- 1: connected |
| web_tag | String | Website name. |
| timestamp | Long | Time a domain name is added to WAF. |
| flag | **Flag** object | Special domain name identifier. This parameter is used for console only. |
| block_page | **BlockPage** object | Alarm configuration page |
| extend | Map<String,String> | Extended attribute |
| traffic_mark | **TrafficMark** object | Stream tag |
| timeout_config | **TimeoutConfig** object | Timeout settings |
| access_progress | Array of **Access_progress** objects | Redundant parameter. It is used for console only. |

**Table 4-372** PremiumWafServer

| Parameter | Type | Description |
|---|---|---|
| front_protocol | String | Client protocol used to request access to the origin server.<br>Enumeration values:<br>- **HTTP**<br>- **HTTPS** |

| Parameter | Type | Description |
|---|---|---|
| back_protocol | String | Server protocol used when WAF forwards client requests to the origin server.<br>Enumeration values:<br>● **HTTP**<br>● **HTTPS** |
| address | String | Public IP address or domain name of the origin server that the client accesses. |
| port | Integer | Port number used by the web server. The value ranges from 0 to 65535, for example, 8080. |
| type | String | The origin server address is an IPv4 or IPv6 address.<br>Enumeration values:<br>● **ipv4**<br>● **ipv6** |
| vpc_id | String | VPC ID. Perform the following steps to obtain the VPC ID:<br>● 1.Find the name of the VPC where the dedicated engine is located. The VPC name is in the VPC\Subnet column. Log in to the WAF console and choose Instance Management > Dedicated Engine > VPC \Subnet.<br>● 2.Log in to the VPC console and click the VPC name. On the page displayed, copy the VPC ID in the VPC Information area. |

**Table 4-373** Flag

| Parameter | Type | Description |
|---|---|---|
| pci_3ds | String | Whether your website passes PCI 3DS check.<br>● true: Your website passed the PCI 3DS check.<br>● false: Your website failed the PCI 3DS check.<br>Enumeration values:<br>● **true**<br>● **false** |

| Parameter | Type | Description |
|---|---|---|
| pci_dss | String | Whether your website passes PCI DSS check<br>- true: Your website passed the PCI DSS check.<br>- false: Your website failed the PCI DSS check.<br>Enumeration values:<br>- **true**<br>- **false** |
| cname | String | The CNAME record the domain name is using<br>- old: The domain name uses the old CNAME record.<br>- new: The domain name uses a new CNAME record.<br>Enumeration values:<br>- **old**<br>- **new** |
| is_dual_az | String | Whether WAF supports multi-AZ DR.<br>- true: WAF supports multi-AZ disaster recovery (DR).<br>- false: WAF does not support multi-AZ DR.<br>Enumeration values:<br>- **true**<br>- **false** |

**Table 4-374** BlockPage

| Parameter | Type | Description |
|---|---|---|
| template | String | Template name |
| custom_page | **CustomPage** object | Custom alarm page |
| redirect_url | String | Redirection URL |

**Table 4-375** CustomPage

| Parameter | Type | Description |
|---|---|---|
| status_code | String | Status code |
| content_type | String | Content type of alarm page |

| Parameter | Type | Description |
|---|---|---|
| content | String | Page content |

**Table 4-376** TrafficMark

| Parameter | Type | Description |
|---|---|---|
| sip | Array of strings | IP address in the known attack source rule |
| cookie | String | cookie |
| params | String | Parameters |

**Table 4-377** 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 4-378** Access_progress

| Parameter | Type | Description |
|---|---|---|
| step | Integer | Step |
| status | Integer | Status |

**Status code: 400**

**Table 4-379** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-380** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-381** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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,
  "web_tag" : ""
}
```

## 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**.

# 4.2.2.5 Deleting a Domain Name from a Dedicated WAF Instance

## Function

This API is used for deleting a domain name from a dedicated WAF instance.

## URI

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

**Table 4-382** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| host_id | Yes | String | ID of the domain name protected by the dedicated WAF engine |

**Table 4-383** 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. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| keepPolicy | No | Boolean | Whether to retain the rule<br>Default: **false** |

## Request Parameters

**Table 4-384** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| Content-Type | Yes | String | Content type<br>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 4-385** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain name ID |
| hostname | String | Domain name |
| policyid | String | Policy ID |
| region | String | Region ID |
| protect_status | Integer | WAF status of the protected domain name.<br>● -1: Bypassed. Requests are directly sent to the backend servers without passing through WAF.<br>● 0: Suspended. WAF only forwards requests for the domain name but does not detect attacks.<br>● 1: Enabled. WAF detects attacks based on the configured policy. |

| Parameter | Type | Description |
|---|---|---|
| access_status | Integer | Whether a domain name is connected to WAF.<br>● 0: disconnected<br>● 1: connected |
| flag | Map<String,String> | Special domain name identifier. This parameter is used for console only. |

**Status code: 400**

**Table 4-386** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-387** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-388** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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" : "xx-xx-1",
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false"
  },
  "description" : "",
  "policyid" : "df15d0eb84194950a8fdc615b6c012dc",
  "protect_status" : 1,
  "access_status" : 0,
  "web_tag" : "",
  "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**.

# 4.2.3 Protection Status and Domain Name Access

## 4.2.3.1 Modifying the Protection Status of a Domain Name in Dedicated Mode

### Function

This API is used for modifying the protection status of a domain name in dedicated mode.

### URI

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

**Table 4-389** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| host_id | Yes | String | ID of the domain name protected by the dedicated WAF engine |

**Table 4-390** 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 4-391** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| Content-Type | Yes | String | Content type<br>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 4-392** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| protect_status | Yes | Integer | WAF status of the protected domain name.<br>● -1: Bypassed. Requests are directly sent to the backend servers without passing through WAF.<br>● 0: Suspended. WAF only forwards requests for the domain name but does not detect attacks.<br>● 1: Enabled. WAF detects attacks based on the configured policy. |

## Response Parameters

**Status code: 200**

**Table 4-393** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| protect_status | Integer | WAF status of the protected domain name.<br>● -1: Bypassed. Requests are directly sent to the backend servers without passing through WAF.<br>● 0: Suspended. WAF only forwards requests for the domain name but does not detect attacks.<br>● 1: Enabled. WAF detects attacks based on the configured policy. |

**Status code: 400**

**Table 4-394** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-395** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-396** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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**.

### 4.2.3.2 Modifying the Access Status of a Domain Name in Dedicated Mode

## Function

This API is used for modifying the access status of a domain name in dedicated mode.

## URI

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

**Table 4-397** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| host_id | Yes | String | ID of the domain name protected by the dedicated WAF engine |

## 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). |

**Table 4-399** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| access_status | No | Integer | Whether WAF is connected.<br>● 0: disconnected<br>● 1: connected |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| protect_status | No | Integer | WAF status of the protected domain name.<br>● -1: Bypassed. Requests are directly sent to the backend servers without passing through WAF.<br>● 0: Suspended. WAF only forwards requests for the domain name but does not detect attacks.<br>● 1: Enabled. WAF detects attacks based on the configured policy. |

## Response Parameters

**Status code: 200**

**Table 4-400** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| access_status | Integer | Whether WAF is connected.<br>● 0: disconnected<br>● 1: connected |

**Status code: 400**

**Table 4-401** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-402** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-403** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
PUT https://{Endpoint}/v1/{project_id}/premium-waf/host/{host_id}/access_status

{
  "access_status" : 1
}
```

## Example Responses

**Status code: 200**

ok

```
{
  "access_status" : 1,
  "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**.

# 4.2.4 Policy Management

### 4.2.4.1 Querying the Policy List

## Function

This API is used to query the list of policies.

## URI

GET /v1/{project_id}/waf/policy

**Table 4-404** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

**Table 4-405** 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 of the data to be returned in a query. The value range is 0 to 100000. The default value is 1, indicating that data on the first page is returned.<br>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.<br>Default: **10** |
| name | No | String | Policy name |

## 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-407** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Total number of policies |
| items | Array of **PolicyResponse** objects | Policy objects |

**Table 4-408** PolicyResponse

| Parameter | Type | Description |
|---|---|---|
| id | String | Policy ID |
| name | String | Policy name |
| action | **PolicyAction** object | This API is used to set policy actions. |
| options | **PolicyOption** object | This API is used to set policy options. |

| Parameter | Type | Description |
|---|---|---|
| level | Integer | Protection level<br>- 1: WAF detects wget, cURL, and more but does not detect XSS and command injection attacks in the header, so you may miss more vulnerabilities that in fact exist. If you find out that configured protection rules are affecting your services, adjust the protection level to 1.<br>- 2: WAF detects remote file inclusion, third-party software vulnerabilities, webshell, and cp and ftp commands. This is the default value.<br>- 3: If you need a stricter protection level, set this parameter to 3. This may increase the false positive rate but decrease the false negative rate, such as nc, nmap, and kill. |
| full_detection | Boolean | Detection mode in the precise protection rule<br>- true: full detection. WAF blocks all requests that hit the configured precise protection rule when it finishes all threat detections.<br>- false: instant detection. WAF immediately ends threat detection and blocks the request that hits the configured precise protection rule. |
| bind_host | Array of **BindHost** objects | Basic information about the protected domain. |
| timestamp | Long | Time a policy is created |
| extend | Map<String,String> | Extended field |

**Table 4-409** PolicyAction

| Parameter | Type | Description |
|---|---|---|
| category | String | Protection categories. Available values include:<br>- log: WAF only logs detected attacks.<br>- block: WAF blocks attacks.<br>Enumeration values:<br>- **block**<br>- **log** |

**Table 4-410** PolicyOption

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Whether basic web protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| common | Boolean | Whether general check is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler | Boolean | Whether anti-crawler protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_engine | Boolean | Whether the search engine is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_scanner | Boolean | Whether the anti-crawler detection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_script | Boolean | Whether the JavaScript anti-crawler is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_other | Boolean | Whether other crawler check is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| webshell | Boolean | Whether webshell detection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |

| Parameter | Type | Description |
|---|---|---|
| cc | Boolean | Whether the CC attack protection rules are enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| custom | Boolean | Whether precise protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| whiteblackip | Boolean | Whether blacklist and whitelist protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| geoip | Boolean | Whether geolocation access control is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| ignore | Boolean | Whether false alarm masking is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| privacy | Boolean | Whether data masking is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| antitamper | Boolean | Whether the web tamper protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| antileakage | Boolean | Whether the information leakage prevention is enabled<br>Enumeration values:<br>- **true**<br>- **false** |

| Parameter | Type | Description |
|---|---|---|
| bot_enable | Boolean | Whether bot mitigation is enabled<br>Enumeration values:<br>● **true**<br>● **false** |

**Table 4-411** BindHost

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain ID |
| hostname | String | Protected domain name |
| waf_type | String | Domain name mode: cloud (cloud mode)/ premium (dedicated mode) |
| mode | String | This parameter is required only by the dedicated mode. |

**Status code: 400**

**Table 4-412** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-413** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-414** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "41cba8aee2e94bcdbf57460874205494",
    "name" : "policy_2FHwFOKz",
    "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
    },
    "hosts" : [ ],
    "extend" : { },
    "timestamp" : 1650527546218,
    "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**.

# 4.2.4.2 Creating a Policy

## Function

This API is used for creating a protection policy.

## URI

POST /v1/{project_id}/waf/policy

**Table 4-415** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

**Table 4-416** 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 4-417** 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<br>Default: **application/json;charset=utf8** |

**Table 4-418** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | Yes | String | Policy name |

## Response Parameters

**Status code: 200**

**Table 4-419** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Policy ID |
| name | String | Policy name |
| action | **PolicyAction** object | This API is used to set policy actions. |
| options | **PolicyOption** object | This API is used to set policy options. |

| Parameter | Type | Description |
|---|---|---|
| level | Integer | Protection level<br>- 1: WAF detects wget, cURL, and more but does not detect XSS and command injection attacks in the header, so you may miss more vulnerabilities that in fact exist. If you find out that configured protection rules are affecting your services, adjust the protection level to 1.<br>- 2: WAF detects remote file inclusion, third-party software vulnerabilities, webshell, and cp and ftp commands. This is the default value.<br>- 3: If you need a stricter protection level, set this parameter to 3. This may increase the false positive rate but decrease the false negative rate, such as nc, nmap, and kill. |
| full_detection | Boolean | Detection mode in the precise protection rule<br>- true: full detection. WAF blocks all requests that hit the configured precise protection rule when it finishes all threat detections.<br>- false: instant detection. WAF immediately ends threat detection and blocks the request that hits the configured precise protection rule. |
| bind_host | Array of **BindHost** objects | Basic information about the protected domain |
| timestamp | Integer | Time a policy is created |
| extend | Map<String,String> | Extended field |

**Table 4-420** PolicyAction

| Parameter | Type | Description |
|---|---|---|
| category | String | Protection categories. Available values include:<br>- log: WAF only logs detected attacks.<br>- block: WAF blocks attacks.<br>Enumeration values:<br>- **block**<br>- **log** |

**Table 4-421** PolicyOption

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Whether basic web protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| common | Boolean | Whether general check is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler | Boolean | Whether anti-crawler protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_engine | Boolean | Whether the search engine is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_scanner | Boolean | Whether the anti-crawler detection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_script | Boolean | Whether the JavaScript anti-crawler is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_other | Boolean | Whether other crawler check is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| webshell | Boolean | Whether webshell detection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |

| Parameter | Type | Description |
|---|---|---|
| cc | Boolean | Whether the CC attack protection rules are enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| custom | Boolean | Whether precise protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| whiteblackip | Boolean | Whether blacklist and whitelist protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| geoip | Boolean | Whether geolocation access control is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| ignore | Boolean | Whether false alarm masking is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| privacy | Boolean | Whether data masking is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| antitamper | Boolean | Whether the web tamper protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| antileakage | Boolean | Whether the information leakage prevention is enabled<br>Enumeration values:<br>● **true**<br>● **false** |

| Parameter | Type | Description |
|---|---|---|
| bot_enable | Boolean | Whether bot mitigation is enabled<br>Enumeration values:<br>● **true**<br>● **false** |

**Table 4-422** BindHost

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain ID |
| hostname | String | Protected domain name |
| waf_type | String | Domain name mode: cloud (cloud mode)/ premium (dedicated mode) |
| mode | String | This parameter is required only by the dedicated mode. |

**Status code: 400**

**Table 4-423** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-424** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 403**

**Table 4-425** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-426** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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,
    "precise" : false,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true
  },
  "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 | Insufficient resource quota. |
| 500 | Internal server error. |

## Error Codes

See **Error Codes**.

# 4.2.4.3 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 4-427** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-428** 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 4-429** 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-430** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Policy ID |
| name | String | Policy name |
| action | **PolicyAction** object | This API is used to set policy actions. |
| options | **PolicyOption** object | This API is used to set policy options. |

| Parameter | Type | Description |
|---|---|---|
| level | Integer | Protection level<br>- 1: WAF detects wget, cURL, and more but does not detect XSS and command injection attacks in the header, so you may miss more vulnerabilities that in fact exist. If you find out that configured protection rules are affecting your services, adjust the protection level to 1.<br>- 2: WAF detects remote file inclusion, third-party software vulnerabilities, webshell, and cp and ftp commands. This is the default value.<br>- 3: If you need a stricter protection level, set this parameter to 3. This may increase the false positive rate but decrease the false negative rate, such as nc, nmap, and kill. |
| full_detection | Boolean | Detection mode in the precise protection rule<br>- true: full detection. WAF blocks all requests that hit the configured precise protection rule when it finishes all threat detections.<br>- false: instant detection. WAF immediately ends threat detection and blocks the request that hits the configured precise protection rule. |
| bind_host | Array of **BindHost** objects | Basic information about the protected domain |
| timestamp | Integer | Time a policy is created |
| extend | Map<String,String> | Extended field |

**Table 4-431** PolicyAction

| Parameter | Type | Description |
|---|---|---|
| category | String | Protection categories. Available values include:<br>- log: WAF only logs detected attacks.<br>- block: WAF blocks attacks.<br>Enumeration values:<br>- **block**<br>- **log** |

**Table 4-432** PolicyOption

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Whether basic web protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| common | Boolean | Whether general check is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler | Boolean | Whether anti-crawler protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_engine | Boolean | Whether the search engine is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_scanner | Boolean | Whether the anti-crawler detection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_script | Boolean | Whether the JavaScript anti-crawler is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| crawler_other | Boolean | Whether other crawler check is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| webshell | Boolean | Whether webshell detection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |

| Parameter | Type | Description |
|---|---|---|
| cc | Boolean | Whether the CC attack protection rules are enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| custom | Boolean | Whether precise protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| whiteblackip | Boolean | Whether blacklist and whitelist protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| geoip | Boolean | Whether geolocation access control is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| ignore | Boolean | Whether false alarm masking is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| privacy | Boolean | Whether data masking is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| antitamper | Boolean | Whether the web tamper protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| antileakage | Boolean | Whether the information leakage prevention is enabled<br>Enumeration values:<br>- **true**<br>- **false** |

| Parameter | Type | Description |
|---|---|---|
| bot_enable | Boolean | Whether bot mitigation is enabled<br>Enumeration values:<br>● **true**<br>● **false** |

**Table 4-433** BindHost

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain ID |
| hostname | String | Protected domain name |
| waf_type | String | Domain name mode: cloud (cloud mode)/ premium (dedicated mode) |
| mode | String | This parameter is required only by the dedicated mode. |

**Status code: 400**

**Table 4-434** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-435** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-436** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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",
    "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
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ ],
  "share_info" : {
    "is_receiver" : false,
    "provider_display" : {
      "share_count" : 0,
      "accept_count" : 0,
      "process_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**.

## 4.2.4.4 Updating a 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 4-437** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-438** 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 4-439** 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<br>Default: **application/json;charset=utf8** |

**Table 4-440** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | No | String | Policy name |
| action | No | **PolicyAction** object | This API is used to set policy actions. |
| options | No | **PolicyOption** object | This API is used to set policy options. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| level | No | Integer | Protection level<br>- 1: WAF detects wget, cURL, and more but does not detect XSS and command injection attacks in the header, so you may miss more vulnerabilities that in fact exist. If you find out that configured protection rules are affecting your services, adjust the protection level to 1.<br>- 2: WAF detects remote file inclusion, third-party software vulnerabilities, webshell, and cp and ftp commands. This is the default value.<br>- 3: If you need a stricter protection level, set this parameter to 3. This may increase the false positive rate but decrease the false negative rate, such as nc, nmap, and kill. |
| full_detection | No | Boolean | Detection mode in the precise protection rule<br>- true: full detection. WAF blocks all requests that hit the configured precise protection rule when it finishes all threat detections.<br>- false: instant detection. WAF immediately ends threat detection and blocks the request that hits the configured precise protection rule. |

**Table 4-441** PolicyAction

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | No | String | Protection categories. Available values include:<br>- log: WAF only logs detected attacks.<br>- block: WAF blocks attacks.<br>Enumeration values:<br>- **block**<br>- **log** |

**Table 4-442** PolicyOption

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| webattack | No | Boolean | Whether basic web protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| common | No | Boolean | Whether general check is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler | No | Boolean | Whether anti-crawler protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler_engine | No | Boolean | Whether the search engine is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler_scanner | No | Boolean | Whether the anti-crawler detection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| crawler_script | No | Boolean | Whether the JavaScript anti-crawler is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler_other | No | Boolean | Whether other crawler check is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| webshell | No | Boolean | Whether webshell detection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| cc | No | Boolean | Whether the CC attack protection rules are enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| custom | No | Boolean | Whether precise protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| whiteblackip | No | Boolean | Whether blacklist and whitelist protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| geoip | No | Boolean | Whether geolocation access control is enabled<br>Enumeration values:<br>- **true**<br>- **false** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ignore | No | Boolean | Whether false alarm masking is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| privacy | No | Boolean | Whether data masking is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| antitamper | No | Boolean | Whether the web tamper protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| antileakage | No | Boolean | Whether the information leakage prevention is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| bot_enable | No | Boolean | Whether bot mitigation is enabled<br>Enumeration values:<br>● **true**<br>● **false** |

## Response Parameters

**Status code: 200**

**Table 4-443** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Policy ID |
| name | String | Policy name |
| action | **PolicyAction** object | This API is used to set policy actions. |

| Parameter | Type | Description |
|---|---|---|
| options | **PolicyOption** object | This API is used to set policy options. |
| level | Integer | Protection level<br>● 1: WAF detects wget, cURL, and more but does not detect XSS and command injection attacks in the header, so you may miss more vulnerabilities that in fact exist. If you find out that configured protection rules are affecting your services, adjust the protection level to 1.<br>● 2: WAF detects remote file inclusion, third-party software vulnerabilities, webshell, and cp and ftp commands. This is the default value.<br>● 3: If you need a stricter protection level, set this parameter to 3. This may increase the false positive rate but decrease the false negative rate, such as nc, nmap, and kill. |
| full_detection | Boolean | Detection mode in the precise protection rule<br>● true: full detection. WAF blocks all requests that hit the configured precise protection rule when it finishes all threat detections.<br>● false: instant detection. WAF immediately ends threat detection and blocks the request that hits the configured precise protection rule. |
| bind_host | Array of **BindHost** objects | Basic information about the protected domain |
| timestamp | Integer | Time a policy is created |
| extend | Map<String,String> | Extended field |

**Table 4-444** PolicyAction

| Parameter | Type | Description |
|---|---|---|
| category | String | Protection categories. Available values include:<br>- log: WAF only logs detected attacks.<br>- block: WAF blocks attacks.<br>Enumeration values:<br>- **block**<br>- **log** |

**Table 4-445** PolicyOption

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Whether basic web protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| common | Boolean | Whether general check is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler | Boolean | Whether anti-crawler protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler_engine | Boolean | Whether the search engine is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler_scanner | Boolean | Whether the anti-crawler detection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler_script | Boolean | Whether the JavaScript anti-crawler is enabled<br>Enumeration values:<br>- **true**<br>- **false** |

| Parameter | Type | Description |
|---|---|---|
| crawler_other | Boolean | Whether other crawler check is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| webshell | Boolean | Whether webshell detection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| cc | Boolean | Whether the CC attack protection rules are enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| custom | Boolean | Whether precise protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| whiteblackip | Boolean | Whether blacklist and whitelist protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| geoip | Boolean | Whether geolocation access control is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| ignore | Boolean | Whether false alarm masking is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| privacy | Boolean | Whether data masking is enabled<br>Enumeration values:<br>- **true**<br>- **false** |

| Parameter | Type | Description |
|---|---|---|
| antitamper | Boolean | Whether the web tamper protection is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| antileakage | Boolean | Whether the information leakage prevention is enabled<br>Enumeration values:<br>● **true**<br>● **false** |
| bot_enable | Boolean | Whether bot mitigation is enabled<br>Enumeration values:<br>● **true**<br>● **false** |

**Table 4-446** BindHost

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain ID |
| hostname | String | Protected domain name |
| waf_type | String | Domain name mode: cloud (cloud mode)/ premium (dedicated mode) |
| mode | String | This parameter is required only by the dedicated mode. |

**Status code: 400**

**Table 4-447** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-448** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-449** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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,
    "precise" : false,
    "whiteblackip" : false,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true
  },
  "hosts" : [ "c0268b883a854adc8a2cd352193b0e13" ],
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ {
    "id" : "c0268b883a854adc8a2cd352193b0e13",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud"
  } ],
  "share_info" : {
    "is_receiver" : false,
    "provider_display" : {
      "share_count" : 0,
      "accept_count" : 0,
      "process_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**.

## 4.2.4.5 Deleting a Policy

## Function

This API is used for deleting a protection policy.

## URI

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

**Table 4-450** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-451** 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 4-452** 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-453** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Policy ID |
| name | String | Policy name |
| action | **PolicyAction** object | This API is used to set policy actions. |
| options | **PolicyOption** object | This API is used to set policy options. |

| Parameter | Type | Description |
|---|---|---|
| level | Integer | Protection level<br>- 1: WAF detects wget, cURL, and more but does not detect XSS and command injection attacks in the header, so you may miss more vulnerabilities that in fact exist. If you find out that configured protection rules are affecting your services, adjust the protection level to 1.<br>- 2: WAF detects remote file inclusion, third-party software vulnerabilities, webshell, and cp and ftp commands. This is the default value.<br>- 3: If you need a stricter protection level, set this parameter to 3. This may increase the false positive rate but decrease the false negative rate, such as nc, nmap, and kill. |
| full_detection | Boolean | Detection mode in the precise protection rule<br>- true: full detection. WAF blocks all requests that hit the configured precise protection rule when it finishes all threat detections.<br>- false: instant detection. WAF immediately ends threat detection and blocks the request that hits the configured precise protection rule. |
| bind_host | Array of **BindHost** objects | Basic information about the protected domain |
| timestamp | Integer | Time a policy is created |
| extend | Map<String,String> | Extended field |

**Table 4-454** PolicyAction

| Parameter | Type | Description |
|---|---|---|
| category | String | Protection categories. Available values include:<br>- log: WAF only logs detected attacks.<br>- block: WAF blocks attacks.<br>Enumeration values:<br>- **block**<br>- **log** |

**Table 4-455** PolicyOption

| Parameter | Type | Description |
|---|---|---|
| webattack | Boolean | Whether basic web protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| common | Boolean | Whether general check is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler | Boolean | Whether anti-crawler protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler_engine | Boolean | Whether the search engine is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler_scanner | Boolean | Whether the anti-crawler detection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler_script | Boolean | Whether the JavaScript anti-crawler is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| crawler_other | Boolean | Whether other crawler check is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| webshell | Boolean | Whether webshell detection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |

| Parameter | Type | Description |
|---|---|---|
| cc | Boolean | Whether the CC attack protection rules are enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| custom | Boolean | Whether precise protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| whiteblackip | Boolean | Whether blacklist and whitelist protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| geoip | Boolean | Whether geolocation access control is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| ignore | Boolean | Whether false alarm masking is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| privacy | Boolean | Whether data masking is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| antitamper | Boolean | Whether the web tamper protection is enabled<br>Enumeration values:<br>- **true**<br>- **false** |
| antileakage | Boolean | Whether the information leakage prevention is enabled<br>Enumeration values:<br>- **true**<br>- **false** |

| Parameter | Type | Description |
|---|---|---|
| bot_enable | Boolean | Whether bot mitigation is enabled<br>Enumeration values:<br>● **true**<br>● **false** |

**Table 4-456** BindHost

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain ID |
| hostname | String | Protected domain name |
| waf_type | String | Domain name mode: cloud (cloud mode)/ premium (dedicated mode) |
| mode | String | This parameter is required only by the dedicated mode. |

**Status code: 400**

**Table 4-457** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-458** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-459** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "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
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1649316510603,
  "full_detection" : false,
  "bind_host" : [ ]
}
```

## 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**.

# 4.2.5 Blacklist and Whitelist Rule Management

## 4.2.5.1 Querying the Blacklist and Whitelist Rule List

## Function

This API is used to query blacklist and whitelist rules.

## URI

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

**Table 4-460** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-461** 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. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| page | No | Integer | Page number of the data to be returned in a query. The value range is 0 to 100000. The default value is 1, indicating that data on the first page is returned.<br>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.<br>Default: **10** |
| name | No | String | Rule name |

## Request Parameters

**Table 4-462** 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-463** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Number of rules |
| items | Array of **WhiteBlackIpResponseBody** objects | Rules |

**Table 4-464** WhiteBlackIpResponseBody

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| timestamp | Long | Rule creation timestamp |
| description | String | Rule description |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |
| addr | String | Blacklist/Whitelist |
| white | Integer | Protective action<br>● 0: WAF blocks the requests that hit the rule.<br>● 1: WAF allows the requests that hit the rule.<br>● 2: WAF only logs the requests that hit the rule. |

**Status code: 400**

**Table 4-465** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-466** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-467** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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",
    "policyname" : "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**.

## 4.2.5.2 Creating a Blacklist or Whitelist Rule

## Function

This API is used for creating a blacklist or whitelist rule.

## URI

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

**Table 4-468** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-469** 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 4-470** 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<br>Default: **application/json;charset=utf8** |

**Table 4-471** 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. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| addr | Yes | String | IP address or IP address ranges in the blacklist or whitelist rule, for example, 10.123.120.66 or 10.123.120.0/16. |
| description | No | String | Rule description |
| white | Yes | Integer | Protective action<br>● 0: WAF blocks the requests that hit the rule.<br>● 1: WAF allows the requests that hit the rule.<br>● 2: WAF only logs the requests that hit the rule. |

## Response Parameters

**Status code: 200**

**Table 4-472** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| addr | String | IP address or IP address ranges in the blacklist or whitelist rule, for example, 10.123.120.66 or 10.123.120.0/16. |
| white | Integer | Protective action<br>● 0: WAF blocks the requests that hit the rule.<br>● 1: WAF allows the requests that hit the rule.<br>● 2: WAF only logs the requests that hit the rule. |
| timestamp | Long | Time a rule is created. The value is a 13-digit timestamp in millisecond. |

**Status code: 400**

**Table 4-473** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-474** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-475** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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,
  "size" : 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**.

### 4.2.5.3 Querying a Blacklist or Whitelist Rule

## Function

This API is used to query a blacklist/whitelist protection rule by ID.

## URI

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

**Table 4-476** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | project_id |
| policy_id | Yes | String | policyid |
| rule_id | Yes | String | whiteblackIpRuleId |

## Request Parameters

**Table 4-477** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-478** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| addr | String | IP addresses in the blacklist or whitelist rule |
| description | String | Rule description |
| white | Integer | Protective action<br>● 0: WAF blocks the requests that hit the rule.<br>● 1: WAF allows the requests that hit the rule.<br>● 2: WAF only logs the requests that hit the rule. |

**Status code: 400**

**Table 4-479** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-480** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-481** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

None

## 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**.

# 4.2.5.4 Updating a Blacklist or Whitelist Rule

## Function

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

## URI

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

**Table 4-482** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | ID of the blacklist or whitelist rule. It can be obtained by calling the ListWhiteblackipRule API. |

**Table 4-483** 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 4-484** 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<br>Default: **application/json;charset=utf8** |

**Table 4-485** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | Yes | String | Rule name |
| addr | Yes | String | IP address or IP address ranges in the blacklist or whitelist rule, for example, 10.123.120.66 or 10.123.120.0/16. |
| description | No | String | Rule description |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| white | Yes | Integer | Protective action<br>● 0: WAF blocks the requests that hit the rule.<br>● 1: WAF allows the requests that hit the rule.<br>● 2: WAF only logs the requests that hit the rule. |

## Response Parameters

**Status code: 200**

**Table 4-486** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| addr | String | IP addresses in the blacklist or whitelist rule |
| description | String | Rule description |
| white | Integer | Protective action<br>● 0: WAF blocks the requests that hit the rule.<br>● 1: WAF allows the requests that hit the rule.<br>● 2: WAF only logs the requests that hit the rule. |

**Status code: 400**

**Table 4-487** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-488** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-489** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

{
  "name" : "demo",
  "white" : 0,
  "description" : "demo",
  "addr" : "10.1.1.2"
}
```

## Example Responses

**Status code: 200**

ok

```
{
  "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 | ok |
| 400 | Request failed. |
| 401 | The token does not have required permissions. |

| Status Code | Description |
|---|---|
| 500 | Internal server error. |

## Error Codes

See **Error Codes**.

# 4.2.5.5 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 4-490** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | ID of the blacklist or whitelist rule. It can be obtained by calling the ListWhiteblackipRule API. |

**Table 4-491** 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 4-492** 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-493** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Blacklist or whitelist rule ID |
| policyid | String | Policy ID |
| name | String | Rule name |
| 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 (disabled) or 1 (enabled). |
| addr | String | IP address or IP address ranges in the blacklist or whitelist rule, for example, 10.123.120.66 or 10.123.120.0/16. |
| white | Integer | Protective action<br>● 0: WAF blocks the requests that hit the rule.<br>● 1: WAF allows the requests that hit the rule.<br>● 2: WAF only logs the requests that hit the rule. |

**Status code: 400**

**Table 4-494** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-495** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-496** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "id" : "5d43af25404341058d5ab17b7ba78b56",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650531872900,
  "description" : "demo",
  "status" : 1,
  "addr" : "10.1.1.2",
  "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**.

# 4.2.6 CC Attack Protection Rule Management

## 4.2.6.1 Querying the CC Attack Protection Rule List

## Function

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

## URI

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

**Table 4-497** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-498** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| page | No | Integer | Page number of the data to be returned in a query. The value range is 0 to 100000. The default value is 1, indicating that data on the first page is returned.<br>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.<br>Default: **10** |

## Request Parameters

**Table 4-499** 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-500** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Total number of CC prevention rules in a policy |
| items | Array of **CcrulesListInfo** objects | Objects of a CC prevention rule |

**Table 4-501** CcrulesListInfo

| Parameter | Type | Description |
|---|---|---|
| id | String | ID of a CC prevention rule |
| policyid | String | ID of the policy to which the rule belongs |
| url | String | URL to which the rule applies, excluding a domain name.<br>● 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*.<br>● Exact match: The path to be entered must match the path to be protected. If the path to be protected is /admin, set url to /admin. |
| limit_num | String | Number of requests allowed from a web visitor in a rate limiting period |
| limit_period | String | Rate limiting period |
| lock_time | String | How long a web visitor will be locked The value range is [0 to 2^32), in seconds. |
| tag_type | String | Protection mode.<br>● ip: A website visitor is identified by the IP address.<br>● cookie: A website visitor is identified by the cookie key value.<br>● other: A website visitor is identified by the Referer field (user-defined request source). |
| tag_index | String | Protection mode tag. When tag_type is set to cookie, this parameter indicates the cookie name. |
| action | **action** object | Action to take if the number of requests reaches the upper limit. |
| timestamp | Long | Rule creation timestamp |

**Table 4-502** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Action type<br>- block: WAF blocks the requests.<br>- captcha: Verification code. The user needs to enter the correct verification code after blocking to restore the correct access page.<br>- If tag_type is set to other, the value can only be block. |
| detail | String | Action details. If detail is null, the default block page is displayed by default.<br>- This parameter is not required if category is set to captcha.<br>- This parameter is required if category is set to block. |

**Table 4-503** detail

| Parameter | Type | Description |
|---|---|---|
| redirect_url | String | URL to which the page is redirected. |
| response | **response** object | Redirected page |

**Table 4-504** response

| Parameter | Type | Description |
|---|---|---|
| content_type | String | Content type. The value can only be application/json, text/html, or text/xml. |
| content | String | Content |

**Status code: 400**

**Table 4-505** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-506** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-507** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "total" : 1,
  "items" : [ {
    "aging_time" : 0,
    "description" : "",
    "id" : "a5f3fd28db564696b199228f0ac346b2",
    "limit_num" : 10,
    "limit_period" : 60,
    "lock_time" : 0,
    "mode" : 0,
    "policyid" : "1f016cde588646aca3fb19f277c44d03",
    "prefix" : false,
    "producer" : 1,
    "status" : 1,
    "tag_type" : "ip",
    "timestamp" : 1656494435686,
    "total_num" : 0,
    "unaggregation" : false,
    "url" : "/path"
  } ]
}
```

## 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**.

## 4.2.6.2 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 4-508** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

## Request Parameters

**Table 4-509** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

**Table 4-510** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| description | No | String | Rule description |
| limit_num | No | Integer | Frequency limits<br>Minimum: **0**<br>Maximum: **10000** |
| limit_period | No | Integer | Frequency limit unit<br>Minimum: **0**<br>Maximum: **10000** |
| url | No | String | url<br>Minimum: **0**<br>Maximum: **10000** |
| mode | No | 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.<br>Enumeration values:<br>● **0**<br>● **1** |
| action | No | **action** object | Action to take if the number of requests reaches the upper limit. |
| tag_type | No | String | Protection mode.<br>● ip: A website visitor is identified by the IP address.<br>● cookie: A website visitor is identified by the cookie key value.<br>● other: A website visitor is identified by the Referer field (user-defined request source).<br>Enumeration values:<br>● **ip**<br>● **other**<br>● **cookie** |

**Table 4-511** action

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | No | String | Protective action |

## Response Parameters

**Status code: 200**

**Table 4-512** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Number of CC prevention rules in the policy |
| items | Array of **CcrulesListInfo** objects | Objects of a CC prevention rule |

**Table 4-513** CcrulesListInfo

| Parameter | Type | Description |
|---|---|---|
| id | String | ID of a CC prevention rule |
| policyid | String | ID of the policy to which the rule belongs |
| url | String | URL to which the rule applies, excluding a domain name.<br>● 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*.<br>● Exact match: The path to be entered must match the path to be protected. If the path to be protected is /admin, set url to /admin. |
| limit_num | String | Number of requests allowed from a web visitor in a rate limiting period |
| limit_period | String | Rate limiting period |
| lock_time | String | How long a web visitor will be locked The value range is [0 to 2^32), in seconds. |

| Parameter | Type | Description |
|---|---|---|
| tag_type | String | Protection mode.<br>● ip: A website visitor is identified by the IP address.<br>● cookie: A website visitor is identified by the cookie key value.<br>● other: A website visitor is identified by the Referer field (user-defined request source). |
| tag_index | String | Protection mode tag. When tag_type is set to cookie, this parameter indicates the cookie name. |
| action | **action** object | Action to take if the number of requests reaches the upper limit. |
| timestamp | Long | Rule creation timestamp |

**Table 4-514** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Action type<br>● block: WAF blocks the requests.<br>● captcha: Verification code. The user needs to enter the correct verification code after blocking to restore the correct access page.<br>● If tag_type is set to other, the value can only be block. |
| detail | String | Action details. If detail is null, the default block page is displayed by default.<br>● This parameter is not required if category is set to captcha.<br>● This parameter is required if category is set to block. |

**Table 4-515** detail

| Parameter | Type | Description |
|---|---|---|
| redirect_url | String | URL to which the page is redirected. |
| response | **response** object | Redirected page |

**Table 4-516** response

| Parameter | Type | Description |
|---|---|---|
| content_type | String | Content type. The value can only be application/json, text/html, or text/xml. |
| content | String | Content |

**Status code: 400**

**Table 4-517** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-518** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-519** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

{
  "action" : {
    "category" : "captcha"
  },
  "description" : "",
  "limit_num" : 10,
  "limit_period" : 60,
  "mode" : 0,
  "tag_type" : "ip",
  "url" : "/path"
}
```

## Example Responses

**Status code: 200**

ok

```
{
  "aging_time" : 0,
  "description" : "",
  "id" : "a5f3fd28db564696b199228f0ac346b2",
  "limit_num" : 10,
  "limit_period" : 60,
  "lock_time" : 0,
  "mode" : 0,
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "prefix" : false,
  "producer" : 1,
  "status" : 1,
  "tag_type" : "ip",
  "timestamp" : 1656494435686,
  "total_num" : 0,
  "unaggregation" : false,
  "url" : "/path"
}
```

## 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**.

## 4.2.6.3 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 4-520** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | ccRuleId |

## Request Parameters

**Table 4-521** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-522** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | ID of a CC prevention rule |
| policyid | String | ID of the policy to which the rule belongs |
| url | String | URL to which the rule applies, excluding a domain name.<br>● 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*.<br>● 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. |
| limit_num | String | Number of requests allowed from a web visitor in a rate limiting period |

| Parameter | Type | Description |
|---|---|---|
| limit_period | String | Rate limiting period |
| lock_time | String | How long a web visitor will be locked The value range is [0 to 2^32), in seconds. |
| tag_type | String | Protection mode.<br>● ip: A website visitor is identified by the IP address.<br>● cookie: A website visitor is identified by the cookie key value.<br>● other: A website visitor is identified by the Referer field (user-defined request source). |
| tag_index | String | Protection mode tag. When tag_type is set to cookie, this parameter indicates the cookie name. |
| action | action object | Action to take if the number of requests reaches the upper limit. |
| timestamp | Long | Rule creation timestamp |

**Table 4-523** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Action type:<br>● block: WAF blocks the requests.<br>● captcha: Verification code. WAF requires visitors to enter a correct verification code to continue their access to requested page on your website.<br>● If tag_type is set to other, the value can only be block. |
| detail | String | Action details. If detail is null, the default block page is displayed by default.<br>● This parameter is not required if category is set to captcha.<br>● This parameter is required if category is set to block. |

**Table 4-524** detail

| Parameter | Type | Description |
|---|---|---|
| redirect_url | String | URL to which the page is redirected. |

| Parameter | Type | Description |
|---|---|---|
| response | **response** object | Redirected page |

**Table 4-525** response

| Parameter | Type | Description |
|---|---|---|
| content_type | String | Content type. The value can only be application/json, text/html, or text/xml. |
| content | String | Contents |

**Status code: 400**

**Table 4-526** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-527** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-528** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "aging_time" : 0,
  "description" : "",
  "id" : "a5f3fd28db564696b199228f0ac346b2",
  "limit_num" : 10,
  "limit_period" : 60,
  "lock_time" : 0,
  "mode" : 0,
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "prefix" : false,
  "producer" : 1,
  "status" : 1,
  "tag_type" : "ip",
  "timestamp" : 1656494435686,
  "total_num" : 0,
  "unaggregation" : false,
  "url" : "/path"
}
```

## 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**.

## 4.2.6.4 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 4-529** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | policyid |
| rule_id | Yes | String | ccRuleId |

## Request Parameters

**Table 4-530** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

**Table 4-531** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| description | No | String | Rule description |
| limit_num | No | Integer | Frequency limits<br>Minimum: **0**<br>Maximum: **10000** |
| limit_period | No | Integer | Frequency limit unit<br>Minimum: **0**<br>Maximum: **10000** |
| url | No | String | url<br>Minimum: **0**<br>Maximum: **10000** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| mode | No | 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.<br>Enumeration values:<br>- **0**<br>- **1** |
| action | No | **action** object | Action to take if the number of requests reaches the upper limit. |
| tag_type | No | String | Protection mode.<br>- ip: A website visitor is identified by the IP address.<br>- cookie: A website visitor is identified by the cookie key value.<br>- other: A website visitor is identified by the Referer field (user-defined request source).<br>Enumeration values:<br>- **ip**<br>- **other**<br>- **cookie** |

**Table 4-532** action

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | No | String | Protective action |

## Response Parameters

**Status code: 200**

**Table 4-533** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | ID of a CC prevention rule |
| policyid | String | ID of the policy to which the rule belongs |
| url | String | URL to which the rule applies, excluding a domain name.<br>● 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*.<br>● 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. |
| limit_num | String | Number of requests allowed from a web visitor in a rate limiting period |
| limit_period | String | Rate limiting period |
| lock_time | String | How long a web visitor will be locked The value range is [0 to 2^32), in seconds. |
| tag_type | String | Protection mode.<br>● ip: A website visitor is identified by the IP address.<br>● cookie: A website visitor is identified by the cookie key value.<br>● other: A website visitor is identified by the Referer field (user-defined request source). |
| tag_index | String | Protection mode tag. When tag_type is set to cookie, this parameter indicates the cookie name. |
| action | **action** object | Action to take if the number of requests reaches the upper limit. |

**Table 4-534** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Action type:<br>- block: WAF blocks the requests.<br>- captcha: Verification code. WAF requires visitors to enter a correct verification code to continue their access to requested page on your website.<br>- If tag_type is set to other, the value can only be block. |
| detail | String | Action details. If detail is null, the default block page is displayed by default.<br>- This parameter is not required if category is set to captcha.<br>- This parameter is required if category is set to block. |

**Table 4-535** detail

| Parameter | Type | Description |
|---|---|---|
| redirect_url | String | URL to which the page is redirected. |
| response | **response** object | Redirected page |

**Table 4-536** response

| Parameter | Type | Description |
|---|---|---|
| content_type | String | Content type. The value can only be application/json, text/html, or text/xml. |
| content | String | Content |

**Status code: 400**

**Table 4-537** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-538** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-539** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

{
  "action" : {
    "category" : "captcha"
  },
  "description" : "",
  "limit_num" : 10,
  "limit_period" : 60,
  "mode" : 0,
  "tag_type" : "ip",
  "url" : "/path1"
}
```

## Example Responses

**Status code: 200**

ok

```
{
  "aging_time" : 0,
  "description" : "",
  "id" : "a5f3fd28db564696b199228f0ac346b2",
  "limit_num" : 10,
  "limit_period" : 60,
  "lock_time" : 0,
  "mode" : 0,
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "prefix" : false,
  "producer" : 1,
  "status" : 1,
  "tag_type" : "ip",
  "total_num" : 0,
  "unaggregation" : false,
  "url" : "/path1"
}
```

## 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**.

## 4.2.6.5 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 4-540** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | ccRuleId |

## Request Parameters

**Table 4-541** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 400**

**Table 4-542** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-543** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-544** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "aging_time" : 0,
  "description" : "",
  "id" : "a5f3fd28db564696b199228f0ac346b2",
  "limit_num" : 10,
  "limit_period" : 60,
  "lock_time" : 0,
  "mode" : 0,
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "prefix" : false,
  "producer" : 1,
  "status" : 1,
  "tag_type" : "ip",
  "timestamp" : 1656494435686,
  "total_num" : 0,
  "unaggregation" : false,
  "url" : "/path1"
}
```

## 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**.

# 4.2.7 Precise Protection Rule Management

## 4.2.7.1 Querying Precise Protection Rules

### Function

This API is used to query precise protection rules.

### URI

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

**Table 4-545** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-546** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| page | No | Integer | Page number of the data to be returned in a query. The value range is 0 to 100000. The default value is 1, indicating that data on the first page is returned.<br>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.<br>Default: **10** |

## Request Parameters

**Table 4-547** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-548** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Total number of precise protection rules in a policy. |
| items | Array of objects | Objects of a precise protection rule. |

**Table 4-549** CustomRuleBody

| Parameter | Type | Description |
|---|---|---|
| id | String | ID of a precise protection rule. |
| policyid | String | ID of the policy to which the rule belongs. |
| conditions | Array of **conditions** objects | List of rule conditions. All conditions must be met. |
| action | **action** object | Protective action of the precise protection rule. |
| priority | Integer | Priority of a rule. Smaller values correspond to higher priorities. 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. |
| start | Long | Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is true. |
| terminal | Long | Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is true. |

**Table 4-550** conditions

| Parameter | Type | Description |
|---|---|---|
| category | String | Field type. The option can be path, user-agent, ip, params, cookie, referer, or header. |
| index | String | The parameter value varies depending on the value of category:<br>● If category is set to cookie, index indicates cookie name.<br>● If category is set to params, index indicates param name.<br>● If category is set to header, index indicates an option in the header. |
| check_all_indexes_logic | Integer | check_all_indexes_logic is not required only when you use custom subfields or the field type is url or ip. Otherwise, the value can be:<br>● 1: All subfields will be checked.<br>● 2: A random subfield will be checked.<br>● null: A custom subfield will be used. |

| Parameter | Type | Description |
|---|---|---|
| logic | Integer | Logic options for a condition. contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, and not_suffix indicate Include, Exclude, Equal to, Not equal to, Prefix is, Prefix is not, Suffix is, and Suffix is not respectively. If category is set to ip, logic can only be equal or not_equal. |
| contents | Array of strings | Content of the conditions. |

**Table 4-551** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Action type.<br>● block: WAF blocks attacks.<br>● pass: WAF allows requests. |

**Status code: 400**

**Table 4-552** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-553** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-554** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "items" : [ {
    "category" : "block",
    "action_mode" : false,
    "aging_time" : 0,
    "conditions" : [ {
      "category" : "header",
      "index" : "sdfsafsda",
      "logic_operation" : "exist"
    } ],
    "description" : "",
    "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
    "policyid" : "1f016cde588646aca3fb19f277c44d03",
    "priority" : 50,
    "producer" : 1,
    "status" : 1,
    "time" : false,
    "timestamp" : 1656495488880
  } ],
  "total" : 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**.

### 4.2.7.2 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 4-555** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

## Request Parameters

**Table 4-556** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

**Table 4-557** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | No | String | Name of the custom rule |
| time | No | Boolean | Time the precise protection rule takes effect.<br>● false: The rule takes effect immediately.<br>● true: The effective time is customized. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| start | No | Long | Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is true. |
| terminal | No | Long | Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is true. |
| conditions | No | Array of **CustomConditions** objects | Match condition List |
| action | No | **CustomAction** object | Protective action of the precise protection rule |
| priority | No | Integer | Priority of a rule. Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority. The value ranges from 0 to 1000. |

**Table 4-558** CustomConditions

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | No | String | The condition types can be path, user-agent, ip, params, cookie, referer, or header. |
| index | No | String | • If category is set to cookie, index indicates cookie name.<br>• If category is set to params, index indicates param name.<br>• If category is set to header, index indicates an option in the header. |
| check_all_indexes_logic | No | Integer | Available values are 1 and 2. The value 1 indicates all subfields, and the value 2 indicates any subfields. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| logic | No | Integer | contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, and not_suffix indicate Include, Exclude, Equal to, Not equal to, Prefix is, Prefix is not, Suffix is, and Suffix is not respectively. If category is set to ip, logic can only be equal or not_equal. |
| contents | No | Array of strings | Content of the match conditions |
| value_list_id | No | String | ID of the reference table |

**Table 4-559** CustomAction

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | No | String | Action type.<br>● block: WAF blocks attacks.<br>● pass: WAF allows requests. |

## Response Parameters

**Status code: 200**

**Table 4-560** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | ID of a precise protection rule. |
| policyid | String | ID of the policy to which the rule belongs. |
| conditions | Array of **conditions** objects | List of matching conditions. All conditions must be met. |
| action | **action** object | Protective action of the precise protection rule |
| priority | Integer | Priority of a rule. Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority. The value ranges from 0 to 1000. |
| timestamp | Long | Timestamp when the precise protection rule is created. |

| Parameter | Type | Description |
|---|---|---|
| start | Long | Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is true. |
| terminal | Long | Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is true. |

**Table 4-561** conditions

| Parameter | Type | Description |
|---|---|---|
| category | String | Condition type. Its option can be path, user-agent, ip, params, cookie, referer, or header. |
| index | String | ● If category is set to cookie, index indicates cookie name.<br>● If category is set to params, index indicates param name.<br>● If category is set to header, index indicates an option in the header. |
| check_all_indexes_logic | Integer | Available values are 1 and 2. The value 1 indicates all subfields, and the value 2 indicates any subfields. |
| logic | Integer | contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, and not_suffix indicate Include, Exclude, Equal to, Not equal to, Prefix is, Prefix is not, Suffix is, and Suffix is not respectively. If category is set to ip, logic can only be equal or not_equal. |
| contents | Array of strings | Content of the match conditions |

**Table 4-562** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Action type.<br>● block: WAF blocks attacks.<br>● pass: WAF allows requests. |

**Status code: 400**

**Table 4-563** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-564** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-565** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

{
  "description" : "",
  "action" : {
    "category" : "block"
  },
  "priority" : 50,
  "conditions" : [ {
    "category" : "header",
    "logic_operation" : "exist",
    "index" : "sdfsafsda"
  } ],
  "time" : false
}
```

## Example Responses

**Status code: 200**

ok

```
{
  "items" : [ {
    "action" : {
      "category" : "block"
    },
    "action_mode" : false,
    "aging_time" : 0,
    "conditions" : [ {
      "category" : "header",
      "index" : "sdfsafsda",
      "logic_operation" : "exist"
    } ],
    "description" : "",
    "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
    "policyid" : "1f016cde588646aca3fb19f277c44d03",
    "priority" : 50,
    "producer" : 1,
    "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**.

### 4.2.7.3 Querying a Precise Protection Rule by ID

## Function

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

## URI

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

**Table 4-566** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | customRuleId |

## Request Parameters

**Table 4-567** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-568** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | ID of a precise protection rule. |
| policyid | String | ID of the policy to which the rule belongs. |
| conditions | Array of **conditions** objects | List of matching conditions. All conditions must be met. |
| action | **action** object | Protective action of the precise protection rule |
| priority | Integer | Priority of a rule. Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority. The value ranges from 0 to 1000. |
| timestamp | Long | Timestamp when the precise protection rule is created. |
| start | Long | Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is true. |

| Parameter | Type | Description |
|---|---|---|
| terminal | Long | Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is true. |

**Table 4-569** conditions

| Parameter | Type | Description |
|---|---|---|
| category | String | Condition type. Its option can be path, user-agent, ip, params, cookie, referer, or header. |
| index | String | ● If category is set to cookie, index indicates cookie name.<br>● If category is set to params, index indicates param name.<br>● If category is set to header, index indicates an option in the header. |
| check_all_indexes_logic | Integer | Available values are 1 and 2. The value 1 indicates all subfields, and the value 2 indicates any subfields. |
| logic | Integer | contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, and not_suffix indicate Include, Exclude, Equal to, Not equal to, Prefix is, Prefix is not, Suffix is, and Suffix is not respectively. If category is set to ip, logic can only be equal or not_equal. |
| contents | Array of strings | Content of the match conditions |

**Table 4-570** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Action type.<br>● block: WAF blocks attacks.<br>● pass: WAF allows requests. |

**Status code: 400**

**Table 4-571** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-572** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-573** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "action" : {
    "category" : "block"
  },
  "action_mode" : false,
  "aging_time" : 0,
  "conditions" : [ {
    "category" : "header",
    "index" : "sdfsafsda",
    "logic_operation" : "exist"
  } ],
  "description" : "",
  "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "priority" : 50,
  "producer" : 1,
  "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**.

### 4.2.7.4 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 4-574** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | customRuleId |

## Request Parameters

**Table 4-575** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

**Table 4-576** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | No | String | Name of the custom rule |
| time | No | Boolean | Time the precise protection rule takes effect.<br>● false: The rule takes effect immediately.<br>● true: Time to take effect will be set. |
| start | No | Long | Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is true. |
| terminal | No | Long | Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is true. |
| conditions | No | Array of **CustomConditions** objects | Match condition List |
| action | No | **CustomAction** object | Protective action of the precise protection rule |
| priority | No | Integer | Priority of a rule. Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority. The value ranges from 0 to 1000. |

**Table 4-577** CustomConditions

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | No | String | The condition types can be path, user-agent, ip, params, cookie, referer, or header. |
| index | No | String | - If category is set to cookie, index indicates cookie name.<br>- If category is set to params, index indicates param name.<br>- If category is set to header, index indicates an option in the header. |
| check_all_indexes_logic | No | Integer | Available values are 1 and 2. The value 1 indicates all subfields, and the value 2 indicates any subfields. |
| logic | No | Integer | contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, and not_suffix indicate Include, Exclude, Equal to, Not equal to, Prefix is, Prefix is not, Suffix is, and Suffix is not respectively. If category is set to ip, logic can only be equal or not_equal. |
| contents | No | Array of strings | Content of the match conditions |
| value_list_id | No | String | ID of the reference table |

**Table 4-578** CustomAction

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | No | String | Action type.<br>- block: WAF blocks attacks.<br>- pass: WAF allows requests. |

## Response Parameters

**Status code: 200**

**Table 4-579** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | ID of a precise protection rule. |
| policyid | String | ID of the policy to which the rule belongs. |
| conditions | Array of **conditions** objects | List of matching conditions. All conditions must be met. |
| action | **action** object | Protective action of the precise protection rule |
| priority | Integer | Priority of a rule. Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority. The value ranges from 0 to 1000. |
| timestamp | Long | Timestamp when the precise protection rule is created. |
| start | Long | Timestamp (ms) when the precise protection rule takes effect. This parameter is returned only when time is true. |
| terminal | Long | Timestamp (ms) when the precise protection rule expires. This parameter is returned only when time is true. |

**Table 4-580** conditions

| Parameter | Type | Description |
|---|---|---|
| category | String | Condition type. Its option can be path, user-agent, ip, params, cookie, referer, or header. |
| index | String | ● If category is set to cookie, index indicates cookie name.<br>● If category is set to params, index indicates param name.<br>● If category is set to header, index indicates an option in the header. |
| check_all_indexes_logic | Integer | Available values are 1 and 2. The value 1 indicates all subfields, and the value 2 indicates any subfields. |

| Parameter | Type | Description |
|---|---|---|
| logic | Integer | contain, not_contain, equal, not_equal, prefix, not_prefix, suffix, and not_suffix indicate Include, Exclude, Equal to, Not equal to, Prefix is, Prefix is not, Suffix is, and Suffix is not respectively. If category is set to ip, logic can only be equal or not_equal. |
| contents | Array of strings | Content of the match conditions |

**Table 4-581** action

| Parameter | Type | Description |
|---|---|---|
| category | String | Action type.<br>● block: WAF blocks attacks.<br>● pass: WAF allows requests. |

**Status code: 400**

**Table 4-582** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-583** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-584** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

{
  "description" : "",
  "action" : {
    "category" : "block"
  },
  "priority" : 50,
  "conditions" : [ {
    "category" : "header",
    "logic_operation" : "exist",
    "index" : "sdfsafsda1"
  } ],
  "time" : false
}
```

## Example Responses

**Status code: 200**

ok

```
{
  "action" : {
    "category" : "block"
  },
  "action_mode" : false,
  "aging_time" : 0,
  "conditions" : [ {
    "category" : "header",
    "index" : "sdfsafsda1",
    "logic_operation" : "exist"
  } ],
  "description" : "",
  "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "priority" : 50,
  "producer" : 1,
  "status" : 1,
  "time" : false
}
```

## Status Codes

| Status Code | Description |
|---|---|
| 200 | ok |
| 400 | Request failed. |

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

## Error Codes

See **Error Codes**.

# 4.2.7.5 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 4-585** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | customRuleId |

## Request Parameters

**Table 4-586** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 400**

**Table 4-587** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-588** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-589** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "action" : {
    "category" : "block"
  },
  "action_mode" : false,
  "aging_time" : 0,
  "conditions" : [ {
    "category" : "header",
    "index" : "sdfsafsda1",
    "logic_operation" : "exist"
  } ],
  "description" : "",
  "id" : "2a3caa2bc9814c09ad73d02e3485b4a4",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "priority" : 50,
  "producer" : 1,
  "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**.

# 4.2.8 Data Masking Rule Management

## 4.2.8.1 Querying Data Masking Rules

### Function

This API is used to query data masking rules.

### URI

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

**Table 4-590** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-591** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| page | No | Integer | Page number of the data to be returned in a query. The value range is 0 to 100000. The default value is 1, indicating that data on the first page is returned. |
| 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. |

## Request Parameters

**Table 4-592** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-593** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Number of rules |
| items | Array of **PrivacyResponseBody** objects | Rule |

**Table 4-594** PrivacyResponseBody

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| timestamp | Long | Time a rule is created. The value must be a 13-digit timestamp in millisecond. |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |
| url | String | URL protected by the data masking rule |
| category | String | Masked field<br>Enumeration values:<br>● **params**<br>● **cookie**<br>● **header**<br>● **form** |
| index | String | Field name |

**Status code: 400**

**Table 4-595** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-596** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-597** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

OK

```
{
  "total" : 1,
  "items" : [ {
    "category" : "params",
    "description" : "",
    "id" : "41a5674e03a1470a90ac4761ec4657b4",
    "index" : "password",
    "policyid" : "1f016cde588646aca3fb19f277c44d03",
    "status" : 1,
    "timestamp" : 1656504425319,
    "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**.

## 4.2.8.2 Adding a Data Masking Rule

## Function

This API is used to add a data masking rule.

## URI

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

**Table 4-598** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

## Request Parameters

**Table 4-599** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/ json;charset=utf8** |

**Table 4-600** 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<br>Enumeration values:<br>• **params**<br>• **cookie**<br>• **header**<br>• **form** |
| index | Yes | String | Field name |
| description | No | String | Rule description |

## Response Parameters

**Status code: 200**

**Table 4-601** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| url | 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 | String | Masked field<br>Enumeration values:<br>- **params**<br>- **cookie**<br>- **header**<br>- **form** |
| index | String | Field name |

**Status code: 400**

**Table 4-602** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-603** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-604** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

{
  "url" : "/login",
  "category" : "params",
  "index" : "password",
  "description" : ""
}
```

## Example Responses

**Status code: 200**

OK

```
{
  "category" : "params",
  "description" : "",
  "id" : "41a5674e03a1470a90ac4761ec4657b4",
  "index" : "password",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656504425319,
  "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**.

### 4.2.8.3 Querying a Data Masking Rule List by ID

## Function

This API is used to query a data masking rule by ID.

## URI

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

**Table 4-605** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | privacyRuleId |

## Request Parameters

**Table 4-606** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-607** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| url | 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. |

| Parameter | Type | Description |
|---|---|---|
| category | String | Masked field<br>Enumeration values:<br>- **params**<br>- **cookie**<br>- **header**<br>- **form** |
| index | String | Field name |

**Status code: 400**

**Table 4-608** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-609** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-610** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "category" : "params",
  "description" : "",
  "id" : "41a5674e03a1470a90ac4761ec4657b4",
  "index" : "password",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656504425319,
  "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**.

## 4.2.8.4 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 4-611** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | privacyRuleId |

## Request Parameters

**Table 4-612** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

**Table 4-613** 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<br>Enumeration values:<br>- **params**<br>- **cookie**<br>- **header**<br>- **form** |
| index | Yes | String | Field name |
| description | No | String | Rule description |

## Response Parameters

**Status code: 200**

**Table 4-614** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |

| Parameter | Type | Description |
|---|---|---|
| url | 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 | String | Masked field<br>Enumeration values:<br>● **params**<br>● **cookie**<br>● **header**<br>● **form** |
| index | String | Field name |

**Status code: 400**

**Table 4-615** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-616** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-617** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

{
  "url" : "/login",
  "category" : "header",
  "index" : "token",
  "description" : ""
}
```

## Example Responses

**Status code: 200**

ok

```
{
  "category" : "header",
  "description" : "",
  "id" : "41a5674e03a1470a90ac4761ec4657b4",
  "index" : "token",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656504425319,
  "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**.

## 4.2.8.5 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 4-618** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | privacyRuleId |

## Request Parameters

**Table 4-619** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 400**

**Table 4-620** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-621** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-622** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "category" : "header",
  "description" : "",
  "id" : "41a5674e03a1470a90ac4761ec4657b4",
  "index" : "token",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656504425319,
  "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**.

# 4.2.9 Web Tamper Protection Rule Management

## 4.2.9.1 Querying the List of Web Tamper Protection Rules

## Function

This API is used for querying the list of web tamper protection rules.

## URI

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

**Table 4-623** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-624** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| page | No | Integer | Page number of the data to be returned in a query. The value range is 0 to 100000. The default value is 1, indicating that data on the first page is returned.<br>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.<br>Default: **10** |

## Request Parameters

**Table 4-625** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-626** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Total |
| items | Array of **AntiTamperRuleResponseBody** objects | Rules |

**Table 4-627** AntiTamperRuleResponseBody

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| timestamp | Long | Timestamp (ms) |
| description | String | Description of the rule |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |
| hostname | String | URL protected by the web tamper protection rule, excluding a domain name |
| url | String | URL protected by the web tamper protection rule |

**Status code: 400**

**Table 4-628** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-629** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-630** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "total" : 1,
  "items" : [ {
    "description" : "",
    "hostname" : "www.domain.com",
    "id" : "0f59185b76c143f884d21cd0d88e6fa8",
    "policyid" : "1f016cde588646aca3fb19f277c44d03",
    "status" : 1,
    "timestamp" : 1656506256928,
    "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**.

## 4.2.9.2 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 4-631** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

## Request Parameters

**Table 4-632** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

**Table 4-633** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| hostname | Yes | String | Protected website. It can be obtained by calling the ListHost API in cloud mode (the value of the hostname field in the response body). |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| 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 asterisk ()* indicates the path prefix. |
| description | No | String | Rule description |

## Response Parameters

**Status code: 200**

**Table 4-634** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| timestamp | Long | Timestamp (ms) |
| hostname | String | Domain name protected by the web tamper protection rule |
| url | String | URL protected by the web tamper protection rule |
| description | String | Description of the rule |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |

**Status code: 400**

**Table 4-635** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-636** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-637** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

{
  "hostname" : "www.domain.com",
  "url" : "/login",
  "description" : ""
}
```

## Example Responses

**Status code: 200**

ok

```
{
  "description" : "",
  "hostname" : "www.domain.com",
  "id" : "0f59185b76c143f884d21cd0d88e6fa8",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656506256928,
  "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**.

## 4.2.9.3 Querying a Web Tamper Protection Rule by ID

## Function

This API is used to query a web tamper protection rule by ID.

## URI

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

**Table 4-638** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | antitamperRuleId |

## Request Parameters

**Table 4-639** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-640** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |

| Parameter | Type | Description |
|---|---|---|
| policyid | String | Policy ID |
| timestamp | Long | Timestamp (ms) |
| hostname | String | Domain name protected by the web tamper protection rule |
| url | String | URL protected by the web tamper protection rule |
| description | String | Description of the rule |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |

**Status code: 400**

**Table 4-641** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-642** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-643** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "description" : "",
  "hostname" : "www.domain.com",
  "id" : "0f59185b76c143f884d21cd0d88e6fa8",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656506256928,
  "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**.

# 4.2.9.4 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 4-644** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | antitamperRuleId |

## Request Parameters

**Table 4-645** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-646** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| timestamp | Long | Timestamp (ms) |
| hostname | String | Domain name protected by the web tamper protection rule |
| url | String | URL protected by the web tamper protection rule |
| description | String | Description of the rule |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |

**Status code: 400**

**Table 4-647** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-648** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-649** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "description" : "",
  "hostname" : "www.domain.com",
  "id" : "0f59185b76c143f884d21cd0d88e6fa8",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 1,
  "timestamp" : 1656506256928,
  "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**.

## 4.2.9.5 Updating the Cache of a Web Tamper Protection Rule

## Function

This API is used to refresh cache in a web tamper protection rule in the event of changes on the protected webpage.

## URI

POST /v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamperid}/refresh

**Table 4-650** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| antitamperid | Yes | String | Web tamper protection rule ID |

## Request Parameters

**Table 4-651** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | Tenant token |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| Content-Type | Yes | String | Content type<br>Default: **application/ json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-652** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| timestamp | Long | Timestamp (ms) |
| hostname | String | Domain name protected by the web tamper protection rule |
| url | String | URL protected by the web tamper protection rule |
| description | String | Description of the rule |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |

**Status code: 400**

**Table 4-653** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-654** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-655** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamperid}/refresh?
enterprise_project_id=0
```

## Example Responses

**Status code: 200**

ok

```
{
  "description" : "",
  "hostname" : "www.domain.com",
  "id" : "0f59185b76c143f884d21cd0d88e6fa8",
  "policyid" : "1f016cde588646aca3fb19f277c44d03",
  "status" : 0,
  "timestamp" : 1656506256928,
  "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**.

# 4.2.10 False Alarm Masking Rule Management

## 4.2.10.1 Querying False Alarm Masking Rules

### Function

This API is used to query false alarm masking rules.

### URI

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

**Table 4-656** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-657** 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 of the data to be returned in a query. The value range is 0 to 100000. The default value is 1, indicating that data on the first page is returned.<br>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.<br>Default: **10** |

## Request Parameters

**Table 4-658** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-659** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Number of false alarm masking rules in the policy |
| items | Array of **IgnoreRuleBody** objects | False alarm masking rule objects |

**Table 4-660** IgnoreRuleBody

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| timestamp | Long | Timestamp (ms) when the rule is created |
| description | String | Rule description |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |
| url | String | Path of the false alarm masking rule. This parameter is available only when mode is set to 0. |
| rule | String | ID of the built-in rule. You can query the rule ID by choosing Policy > Policy Name > Basic Web Protection > Protection Rules on the WAF console or in the event details. |

| 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 | Logic options in a condition are:<br>● equal: The condition is met when the specified field in a request equals to the content you provide.<br>● not_equal: The condition is met when the specified field in a request does not equal to the content you provide.<br>● contain: The condition is met when the specified field in a request contains the content you provide.<br>● not_contain: The condition is met when the specified field in a request does not contain the content you provide.<br>● prefix: The condition is met when the prefix in the specified field in a request is the content you provide.<br>● not_prefix: The condition is met when the prefix in the specified field in a request is not the content you provide.<br>● suffix: The condition is met when the suffix in the specified field in a request matches the content you provide.<br>● not_suffix: The condition is met when the suffix in the specified field in a request does not match the content you provide.<br>● regular_match: The condition is met when the regular expression is matched.<br>● regular_not_match: The condition is met when the regular expression is not matched. |
| conditions | Array of **Condition** objects | Condition list |
| domains | Array of strings | Protected domain name or website |

**Table 4-661** 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 segment. If the field type is url, the value must be in standard URL format. If the field type is params, cookie, or header, the content format is not limited. |
| logic_operation | String | Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported. |
| check_all_indexes_logic | Integer | If the field type is url or ip, the check_all_indexes_logic field does not exist. In other cases, the value 1 indicates that all subfields will be checked, the value 2 indicates that any subfield will be checked, and the value null indicates that custom subfields will be used. |
| 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, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield. |

**Status code: 400**

**Table 4-662** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-663** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-664** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "c20f67b3e1c040c0b0d8866e568ee8bf",
    "policyid" : "a75e96d8284c4c4f98ada7d391e8342c",
    "timestamp" : 1656507126528,
    "description" : "",
    "status" : 1,
    "rule" : "webshell",
    "mode" : 1,
    "conditions" : [ {
      "category" : "url",
      "contents" : [ "attack" ],
      "logic_operation" : "contain"
    } ],
    "domain" : [ "test3.th.com" ]
  } ]
}
```

## Status Codes

| Status Code | Description |
|---|---|
| 200 | ok |
| 400 | Request failed. |

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

## Error Codes

See **Error Codes**.

# 4.2.10.2 Adding a False Alarm Masking Rule

## Function

This API is used to add a false alarm masking rule.

## URI

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

**Table 4-665** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |

**Table 4-666** 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 4-667** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| Content-Type | Yes | String | Content type<br>Default: **application/ json;charset=utf8** |

**Table 4-668** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| domain | Yes | Array of strings | Domain name or website to e protect. 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 | Version of the false alarm masking rule. The value must be 1(v2). v1 is only compatible with earlier versions where a rule cannot be created. |
| rule | Yes | String | ID of the built-in rule. You can query the rule ID by choosing Policy > Policy Name > Basic Web Protection > Protection Rules on the WAF console or in the event details. |
| description | No | String | Description of a masking rule |

**Table 4-669** CreateCondition

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| category | Yes | String | Field type. The value can be ip, url, params, cookie, or header. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| contents | Yes | 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 segment. If the field type is url, the value must be in standard URL format. If the field type is params, cookie, or header, the content format is not limited. |
| logic_operation | Yes | String | Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported. |
| check_all_indexes_logic | No | Integer | This parameter is not required if a custom subfield is used and the field type is url or ip. In other cases, the value 1 indicates that all subfields will be checked, and the value 2 indicates that any subfield will be checked. |
| index | No | 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, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield. |

## Response Parameters

**Status code: 200**

**Table 4-670** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| timestamp | Long | Timestamp when the rule is created |
| description | String | Rule description |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |
| rule | String | ID of the built-in rule. You can query the rule ID by choosing Policy > Policy Name > Basic Web Protection > Protection Rules on the WAF console or in the event details. |
| mode | Integer | Version of the false alarm masking rule. The value must be 1(v2). v1 is compatible with earlier versions only where a rule cannot be created. |
| conditions | Array of **Condition** objects | Condition list |
| domain | Array of strings | Protected domain name or website |

**Table 4-671** 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 segment. If the field type is url, the value must be in standard URL format. If the field type is params, cookie, or header, the content format is not limited. |
| logic_operation | String | Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported. |

| Parameter | Type | Description |
|---|---|---|
| check_all_indexes_logic | Integer | If the field type is url or ip, the check_all_indexes_logic field does not exist. In other cases, the value 1 indicates that all subfields will be checked, the value 2 indicates that any subfield will be checked, and the value null indicates that custom subfields will be used. |
| 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, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield. |

**Status code: 400**

**Table 4-672** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-673** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-674** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

{
  "domain" : [ "test3.th.com" ],
  "conditions" : [ {
    "category" : "url",
    "logic_operation" : "contain",
    "contents" : [ "attack" ],
    "index" : null
  } ],
  "mode" : 1,
  "description" : "",
  "rule" : "webshell"
}
```

## Example Responses

**Status code: 200**

OK

```
{
  "id" : "c20f67b3e1c040c0b0d8866e568ee8bf",
  "policyid" : "a75e96d8284c4c4f98ada7d391e8342c",
  "timestamp" : 1656507126528,
  "description" : "",
  "status" : 1,
  "rule" : "webshell",
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "attack" ],
    "logic_operation" : "contain"
  } ],
  "domain" : [ "test3.th.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**.

### 4.2.10.3 Querying a False Alarm Masking Rule

## Function

This API is used to query a false alarm masking rule.

## URI

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

**Table 4-675** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | ignoreRuleId |

**Table 4-676** 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 4-677** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-678** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| timestamp | Long | Timestamp when the rule is created |
| description | String | Rule description |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |
| rule | String | ID of the built-in rule. You can query the rule ID by choosing Policy > Policy Name > Basic Web Protection > Protection Rules on the WAF console or in the event details. |
| mode | Integer | Version of the false alarm masking rule. The value must be 1(v2). v1 is compatible with earlier versions only where a rule cannot be created. |
| conditions | Array of **Condition** objects | Condition list |
| domain | Array of strings | Protected domain name or website |

**Table 4-679** 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 segment. If the field type is url, the value must be in standard URL format. If the field type is params, cookie, or header, the content format is not limited. |
| logic_operation | String | Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported. |

| Parameter | Type | Description |
|---|---|---|
| check_all_indexes_logic | Integer | If the field type is url or ip, the check_all_indexes_logic field does not exist. In other cases, the value 1 indicates that all subfields will be checked, the value 2 indicates that any subfield will be checked, and the value null indicates that custom subfields will be used. |
| 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, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield. |

**Status code: 400**

**Table 4-680** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-681** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-682** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "id" : "c20f67b3e1c040c0b0d8866e568ee8bf",
  "policyid" : "a75e96d8284c4c4f98ada7d391e8342c",
  "timestamp" : 1656507126528,
  "description" : "",
  "status" : 1,
  "rule" : "webshell",
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "attack" ],
    "logic_operation" : "contain"
  } ],
  "domain" : [ "test3.th.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**.

### 4.2.10.4 Updating a False Alarm Masking Rule

## Function

This API is used to update a false alarm masking rule.

## URI

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

**Table 4-683** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | ignoreRuleId |

**Table 4-684** 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 4-685** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

**Table 4-686** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| domain | Yes | Array of strings | Domain name or website to e protect. If the array length is 0, the rule takes effect for all domain names or websites. |
| conditions | Yes | Array of **CreateCondition** objects | Condition list |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| mode | Yes | Integer | Version of the false alarm masking rule. The value must be 1(v2). v1 is only compatible with earlier versions where a rule cannot be created. |
| rule | Yes | String | ID of the built-in rule. You can query the rule ID by choosing Policy > Policy Name > Basic Web Protection > Protection Rules on the WAF console or in the event details. |
| description | No | String | Description of a masking rule |

**Table 4-687** 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 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 segment. If the field type is url, the value must be in standard URL format. If the field type is params, cookie, or header, the content format is not limited. |
| logic_operation | Yes | String | Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| check_all_indexes_logic | No | Integer | This parameter is not required if a custom subfield is used and the field type is url or ip. In other cases, the value 1 indicates that all subfields will be checked, and the value 2 indicates that any subfield will be checked. |
| index | No | 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, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield. |

## Response Parameters

**Status code: 200**

**Table 4-688** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Rule ID |
| policyid | String | Policy ID |
| timestamp | Long | Timestamp when the rule is created |
| description | String | Rule description |
| status | Integer | Rule status. The value can be 0 (disabled) or 1 (enabled). |
| rule | String | ID of the built-in rule. You can query the rule ID by choosing Policy > Policy Name > Basic Web Protection > Protection Rules on the WAF console or in the event details. |
| mode | Integer | Version of the false alarm masking rule. The value must be 1(v2). v1 is compatible with earlier versions only where a rule cannot be created. |

| Parameter | Type | Description |
|---|---|---|
| conditions | Array of **Condition** objects | Condition list |
| domain | Array of strings | Protected domain name or website |

**Table 4-689** 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 segment. If the field type is url, the value must be in standard URL format. If the field type is params, cookie, or header, the content format is not limited. |
| logic_operation | String | Matching logics. The matching logic varies depending on field types. If the field type is ip, equal and not_equal are supported. If the field type is url, header, params, or cookie, equal, not_equal, contain, not_contain, prefix, not_prefix, suffix, not_suffix, regular_match, and regular_not_match are supported. |
| check_all_indexes_logic | Integer | If the field type is url or ip, the check_all_indexes_logic field does not exist. In other cases, the value 1 indicates that all subfields will be checked, the value 2 indicates that any subfield will be checked, and the value null indicates that custom subfields will be used. |
| 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, set the value to x-forwarded-for. If the field type is params, header, or cookie and the subfield is of a customized type, the value of index is the custom subfield. |

**Status code: 400**

**Table 4-690** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-691** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-692** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

{
  "domain" : [ "test3.th.com" ],
  "conditions" : [ {
    "category" : "url",
    "logic_operation" : "contain",
    "contents" : [ "attack" ],
    "index" : null
  } ],
  "mode" : 1,
  "description" : "",
  "rule" : "vuln"
}
```

## Example Responses

**Status code: 200**

ok

```
{
  "id" : "c20f67b3e1c040c0b0d8866e568ee8bf",
  "policyid" : "a75e96d8284c4c4f98ada7d391e8342c",
  "timestamp" : 1656507126528,
  "description" : "",
  "status" : 1,
  "rule" : "vuln",
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "attack" ],
    "logic_operation" : "contain"
  } ],
  "domain" : [ "test3.th.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**.

## 4.2.10.5 Deleting a False Alarm Masking Rule

## Function

This API is used to delete a false alarm masking rule.

## URI

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

**Table 4-693** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| policy_id | Yes | String | Protection policy ID. You can call the ListPolicy API to obtain the policy ID. |
| rule_id | Yes | String | ignoreRuleId |

**Table 4-694** 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 4-695** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | auth token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 400**

**Table 4-696** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-697** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-698** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

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

## Example Responses

**Status code: 200**

ok

```
{
  "id" : "c20f67b3e1c040c0b0d8866e568ee8bf",
  "policyid" : "a75e96d8284c4c4f98ada7d391e8342c",
  "timestamp" : 1656507126528,
  "description" : "",
  "status" : 1,
  "rule" : "vuln",
  "mode" : 1,
  "conditions" : [ {
    "category" : "url",
    "contents" : [ "attack" ],
    "logic_operation" : "contain"
  } ],
  "domain" : [ "test3.th.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**.

# 4.2.11 Dashboard

### 4.2.11.1 Querying the Number of Requests and Attacks on Dashboard

## Function

This API is used to query the number of requests and attacks on the dashboard. This API and other APIs related to Dashboard cannot be used to query the number of requests or attacks for a custom time range. You can use them to query statistics for yesterday, today, past 3 days, past 7 days, and past 30 days only.

## URI

GET /v1/{project_id}/waf/overviews/statistics

**Table 4-699** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

**Table 4-700** 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). 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 ID array. 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. By default, it is left empty, and statistics on abnormal requests for all domain names is returned. To query abnormal requests for one or more domain names, configure this parameter. |
| instances | No | String | List of instances to be queried |

## Request Parameters

**Table 4-701** 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-702** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| [items] | Array of **CountItem** objects | Security statistics |

**Table 4-703** CountItem

| Parameter | Type | Description |
|---|---|---|
| key | String | Type |
| num | Integer | Quantity |

**Status code: 400**

**Table 4-704** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-705** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 403**

**Table 4-706** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-707** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/statistics?
enterprise_project_id=0&from=1650470400196&to=1650522936196&hosts=1bac09440a814aa98ed08302c58
0a48b&hosts=5a532f83a2fb476ba51ca1de7b1ebc43
```

## Example Responses

**Status code: 200**

ok

```
[ {
  "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 | 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**.

## 4.2.11.2 Querying Top N Statistics on Dashboard

## Function

This API is used to query top N statistics on the dashboard, including the attacked domain names, attack source IP addresses, attacked URLs, attack source regions, and event distribution. This API and other APIs related to Dashboard cannot be used to query the number of requests or attacks for a custom time range. You can use them to query statistics for yesterday, today, past 3 days, past 7 days, and past 30 days only.

## URI

GET /v1/{project_id}/waf/overviews/classification

**Table 4-708** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. To query the project ID, go to the management console, choose My Credentials > Projects, and query the value in the Project ID column. |

**Table 4-709** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| enterprise_project_id | No | String | Enterprise project ID. 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 number of top results to be returned. Maximum: 10 Minimum: 5 |
| hosts | No | String | List of the domain names to be queried. It is obtained by calling the ListHost API or the ListPremiumHost API. By default, it is left empty, and statistics on abnormal requests for all domain names is returned. To query abnormal requests for one or more domain names, configure this parameter. |
| instances | No | String | List of instances to be queried. This parameter is required only for dedicated or load-balancing WAF instances. |

## Request Parameters

**Table 4-710** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | Tenant token |
| Content-Type | Yes | String | Content type<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-711** 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 | Attacked URL |
| geo | **GeoClassificationItem** object | Source region |

**Table 4-712** DomainClassificationItem

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Total number of DomainItem |
| items | Array of **DomainItem** objects | DomainItem details |

**Table 4-713** DomainItem

| Parameter | Type | Description |
|---|---|---|
| key | String | Domain name |
| num | Integer | Quantity |
| web_tag | String | Website |

**Table 4-714** AttackTypeClassificationItem

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Total number of AttackTypeItem |
| items | Array of **AttackTypeItem** objects | AttackTypeItem details |

**Table 4-715** AttackTypeItem

| Parameter | Type | Description |
|---|---|---|
| key | String | Attack type |
| num | Integer | Quantity |

**Table 4-716** IpClassificationItem

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Total number of IpItem |
| items | Array of **IpItem** objects | IpItem Details |

**Table 4-717** IpItem

| Parameter | Type | Description |
|---|---|---|
| key | String | IP address |
| num | Integer | Quantity |

**Table 4-718** UrlClassificationItem

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Total number of UrlItem |
| items | Array of **UrlItem** objects | UrlItem Details |

**Table 4-719** UrlItem

| Parameter | Type | Description |
|---|---|---|
| key | String | Path |
| num | Integer | Quantity |
| host | String | Domain name |

**Table 4-720** GeoClassificationItem

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Total number of GeoItem |
| items | Array of **GeoItem** objects | GeoItem details |

**Table 4-721** GeoItem

| Parameter | Type | Description |
|---|---|---|
| key | String | Source region |
| num | Integer | Quantity |

**Status code: 400**

**Table 4-722** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-723** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-724** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
GET https://{Endpoint}/v1/{project_id}/waf/overviews/classification?
enterprise_project_id=0&from=1652889600354&to=1655435681354&top=10&hosts=1bac09440a814aa98ed0
8302c580a48b&hosts=5a532f83a2fb476ba51ca1de7b1ebc43
```

## Example Responses

**Status code: 200**

Request succeeded.

```
{
  "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" : "10.142.4.15",
      "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 | Request succeeded. |
| 400 | Request failed. |
| 401 | The token does not have required permissions. |
| 500 | Internal server error. |

## Error Codes

See **Error Codes**.

# 4.2.12 Protection Event Management

## 4.2.12.1 Querying the List of Attack Events

## Function

This API is used to query the attack event list. Currently, this API cannot be used to query all the events. The pagesize parameter cannot be set to -1. A large query data volume will result in large memory consumption. To avoid affecting performance, a maximum of 10,000 data records can be returned. For example, if the number of data records in the specified time period exceeds 10,000, the data records on page 101 and later cannot be returned. In this case, you need to modify the time period and query again.

## URI

GET /v1/{project_id}/waf/event

**Table 4-725** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

**Table 4-726** 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. |
| recent | No | String | Time range for querying logs. This parameter cannot be used together with from and to.<br>Enumeration values:<br>● **yesterday**<br>● **today**<br>● **3days**<br>● **1week**<br>● **1month** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| attacks | No | Array | Attack type.<br>● vuln: other attack types<br>● sqli: SQL injections<br>● lfi: local file inclusion attacks<br>● cmdi: command injections<br>● xss: XSS attacks<br>● robot: malicious crawlers<br>● rfi: remote file inclusion attacks<br>● custom_custom: precise protection<br>● cc: CC attacks<br>● webshell: website Trojans<br>● custom_whiteblackip: attacks blocked based on blacklist and whitelist settings<br>● custom_geoip: attacks blocked based on geolocations<br>● antitamper: anti-tamper events<br>● anticrawler: anti-crawler events<br>● leakage: website data leakage prevention<br>● illegal: unauthorized requests |
| 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. |
| hosts | No | Array | Domain name ID. It can be obtained by calling the ListHost API. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| page | No | Integer | Page number of the data to be returned in a query. The value range is 0 to 100000. The default value is 1, indicating that data on the first page is returned. |
| 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. |

## Request Parameters

**Table 4-727** 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-728** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Number of attack events |
| items | Array of **ListEventItems** objects | Attack event details |

**Table 4-729** ListEventItems

| Parameter | Type | Description |
|---|---|---|
| id | String | Event ID |
| time | Long | Count |
| policyid | String | Policy ID |
| sip | String | Source IP address |
| host | String | Domain name |
| url | String | Attacked URL |
| attack | String | Attack type:<br>● vuln: other attack types<br>● sqli: SQL injections<br>● lfi: local file inclusion attacks<br>● cmdi: command injections<br>● xss: XSS attacks<br>● robot: malicious crawlers<br>● rfi: remote file inclusion attacks<br>● custom_custom: precise protection<br>● webshell: website Trojans<br>● custom_whiteblackip: attacks blocked based on blacklist and whitelist settings<br>● custom_geoip: attacks blocked based on geolocations<br>● antitamper: anti-tamper events<br>● anticrawler: anti-crawler events<br>● leakage: website data leakage prevention<br>● illegal: unauthorized requests |
| rule | String | ID of the matched rule |
| payload | String | Hit payload |
| action | String | 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 |

| Parameter | Type | Description |
|---|---|---|
| host_id | String | Domain name ID |
| response_time | Long | Time to response |
| response_size | Integer | Response body size |
| response_body | String | Response body |
| request_body | String | Request body |

**Status code: 400**

**Table 4-730** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-731** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-732** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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-xxxxxxxxxxxx",
    "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**.

## 4.2.12.2 Querying Attack Event Details

### Function

This API is used to query the details about an attack event.

### URI

GET /v1/{project_id}/waf/event/{eventid}

**Table 4-733** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| eventid | Yes | String | Event ID. You can call the ListEvent API to obtain the event ID. |

**Table 4-734** 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 4-735** 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<br>Default: **application/json;charset=utf8** |

### Response Parameters

**Status code: 200**

**Table 4-736** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| total | Integer | Number of attack events |
| items | Array of **ShowEventItems** objects | Attack event details |

**Table 4-737** ShowEventItems

| Parameter | Type | Description |
|---|---|---|
| time | Long | Timestamp when the attack occurs, in milliseconds. |
| policyid | String | Policy ID |
| sip | String | Source IP address |
| host | String | Domain name |
| url | String | Attacked URL |
| attack | String | Attack type |
| rule | String | ID of the matched rule |
| action | String | 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 | Status code |
| request_body | String | Request body |

**Status code: 400**

**Table 4-738** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-739** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-740** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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-xxxxxxxxx",
    "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,
    "response_body" : "",
    "process_time" : 0,
    "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**.

# 4.2.13 Certificate Management

## 4.2.13.1 Querying the Certificate List

## Function

This API is used to query the list of certificates.

## URI

GET /v1/{project_id}/waf/certificate

**Table 4-741** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

**Table 4-742** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| enterprise_project_id | No | String | ID of the enterprise project. It can be obtained by called the **ListEnterpriseProject** API of EPS. |
| page | No | Integer | Page number of the data to be returned during pagination query. The value ranges from **0** to **100000**. The default value is **1**, indicating that the data on the first page is returned.<br>Default: **1** |
| pagesize | No | Integer | Number of results on each page during pagination query. The value ranges from **1** to **100**. The default value is **10**, indicating that each page contains 10 results.<br>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**. -**true**: Obtain the certificates that have been used for domain names. -**false**: Obtain the certificates that are not used for any domain name.<br>Default: **false** |
| exp_status | No | Integer | Certificate status. The options are **0**, **1**, and **2**. **0**: The certificate is valid. **1**: The certificate has expired; **2**: The certificate will expire within one month. |

## Request Parameters

**Table 4-743** 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-744** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| items | Array of **CertificateBody** objects | Certificates |
| total | Integer | Total number of certificates |

**Table 4-745** CertificateBody

| Parameter | Type | Description |
|---|---|---|
| id | String | Certificate ID |
| name | String | Certificate Name |
| content | String | Certificate file, which is in PEM format. |
| key | String | Private key of the certificate, which is in PEM format. |
| expire_time | Long | Timestamp when the certificate expires |
| exp_status | Integer | Certificate status. The options are **0**, **1**, and **2**. **0**: The certificate is valid. **1**: The certificate has expired; **2**: The certificate will expire within one month. |
| timestamp | Long | Certificate upload timestamp. |

| Parameter | Type | Description |
|---|---|---|
| bind_host | Array of **BindHost** objects | Domain name associated with the certificate |

**Table 4-746** BindHost

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain ID |
| hostname | String | Protected domain name |
| waf_type | String | Domain name mode: cloud (cloud mode)/ premium (dedicated mode) |
| mode | String | This parameter is required only by the dedicated mode. |

**Status code: 400**

**Table 4-747** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-748** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-749** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error Messages |

## Example Requests

```
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 | Insufficient token permissions. |
| 500 | Internal server error. |

## Error Codes

See **Error Codes**.

# 4.2.13.2 Creating a Certificate

## Function

This API is used to create a certificate.

## URI

POST /v1/{project_id}/waf/certificate

**Table 4-750** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |

**Table 4-751** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| enterprise_project_id | No | String | ID of the enterprise project. It can be obtained by called the **ListEnterpriseProject** API of EPS. |

## Request Parameters

**Table 4-752** 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<br>Default: **application/json;charset=utf8** |

**Table 4-753** 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. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| 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 4-754** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Certificate ID |
| name | String | Certificate Name |
| content | String | Certificate file, which is in PEM format. |
| 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 are **0**, **1**, and **2**. **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 4-755** BindHost

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain ID |
| hostname | String | Protected domain name |
| waf_type | String | Domain name mode: cloud (cloud mode)/ premium (dedicated mode) |
| mode | String | This parameter is required only by the dedicated mode. |

**Status code: 400**

**Table 4-756** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-757** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-758** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
POST https://{Endpoint}/v1/{project_id}/waf/certificate?enterprise_project_id=0

{
  "name" : "demo",
  "content" : "-----BEGIN CERTIFICATE-----
MIIDyzCCArOgAwIBAgIJAN5U0Z4Bh5ccMA0GCSqGSIb3DQEBCwUAMHwxCzAJBgNV
BAYTAlpIMRIwEAYDVQQIDAlHVUFOR0RPTkcxETAPBgNVBAcMCERPTkdHVUFOMQ0w
CwYDVQQKDARERUtFMQswCQYDVQQLDAJESzELMAkGA1UEAwwCT0QxHTAbBgkqhkiG
9w0BCQEWDk8IZC5odWF3ZWkuY29tMB4XDTIxMTExNTA4MTk0MVoXDTIyMTExNTA4
MTk0MVowfDELMAkGA1UEBhMCWkgxEjAQBgNVBAgMCUdVQU5HRE9ORzERMA8GA1UE
BwwIRE9OR0dVQU4xDTALBgNVBAoMBERFS0UxCzAJBgNVBAsMAkRLMQswCQYDVQQD
DAJPRDEdMBsGCSqGSIb3DQEJARYOTwhkLmh1YXdlaS5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDcoLFK62//r0RHFyweYBj97S4NsJ8Qj0RG+Y02
OgwhQmRiNNjubJwP8Nqqyd86zr+fsSQxKBaBCosn1PcN2Pj2vPJD6NEk4I6VdOWr /
kFYMlOcimhSfW4wt6VakniOKIYGrCxxvQe1X2OyBxT+ocTLRgEIB8ZbvJyPNseg
feLEUuPYRpQ5kXLgJH2/3NwZFOgBHVv/b07l4fR+sWJMnIA2yIjSBQ0DEAOSusXo FQ/
WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi8L+mKeRL+lcMMbXC/3k6OfMB
tVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9sE+tmJZTPH6lYtAgMBAAGjUDBOMB0G
A1UdDgQWBBQprUUFXW+gIkpzXdrYlsWjfSahWjAfBgNVHSMEGDAWgBQprUUFXW+g
IkpzXdrYlsWjfSahWjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQA2
603KozsQoIKeLvqDJlcAXwWRfNW8SvlaSJAulhHgneMt9bQgIL+3PJWA/iMniOhU o/
kVwkiUIcxw4t7RwP0hVms0OZw59MuqKd3oCSWkYO4vEHs3t40JDWnGDnmQ4sol
RkOWJwL4w8tnPe3qY9JSupjlsu6Y1hlvKtEfN2vEKFnsuMhidkUpUAJWodHhWBQH
wgIDo4/6yTnWZNGK8JDal86Dm5IchXea1EoYBJsHxiJb7HeWQlkre+MCYi1RHOin 4mIXTr0oT4/jWlgklSz6/
ZhGRq+7W7tIl7cvzCe+4XsVZIenAcYoNd/WLfo91PD4 yAsRXrOjW1so1Bj0BkDz -----END CERTIFICATE-----",
  "key" : "-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDcoLFK62//r0RH FyweYBj97S4NsJ8Qj0RG
+Y02OgwhQmRiNNjubJwP8Nqqyd86zr+fsSQxKBaBCosn 1PcN2Pj2vPJD6NEk4I6VdOWr/
kFYMlOcimhSfW4wt6VakniOKIYGrCxxvQe1X2Oy BxT
+ocTLRgEIB8ZbvJyPNsegfeLEUuPYRpQ5kXLgJH2/3NwZFOgBHVv/b07l4fR+ sWJMnIA2yIjSBQ0DEAOSusXoFQ/
WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi 8L+mKeRL+lcMMbXC/
3k6OfMBtVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9sE+tmJ ZTPH6lYtAgMBAAECggEBAL+xZxm/QoqXT
+2stoqV2GEYaMFASpRqxlocjZMmEE/9 jZa+cBWIjHhVPsjRqYFBDcHEebu0JwlrjcjIAvgnIvnO5XgXm1A9Q
+WbscokmcX1 xCvpHgc+MDVn+uWdCd4KW5kEk4EnSsFN5iNSf+1VxNURN+gwSSp/0E+muwA5IISO G6HQ
+p6qs52JAitX5t/7ruKoHYXJxBnf7TUs7768qrh++KPKpPlq044qoYlcGO1n 4urPBHuNLy04GgGw
+vkaqjqOvZrNLVOMMaFWBxsDWBehgSSBQTj+f3NCxneGYtt8 3SCTZQI5nIkb+r/
M455EwKTSXuEsNHoIwx7L6GEPbQECgYEA8IxgK2fYykloICoh
TFJaRAvyjyKa2+Aza4qT9SGY9Y30VPClPjBB1vUu5M9KrFufzlv06nGEcHmpEwOe
8vbRu7nLAQTGYFi8VK63q8w6FlFdAyCG6Sx+BWCfWxJzXsZLAJTfklwi8HsOSlqh
6QNv0xbE2fLjXKf8MHvtrufip40CgYEA6sy87eDrkVgtq4ythAik3i1C5Z3v0fvx mTblG52Z21OyocNq3Tf/
b1ZwoIc1ik6cyBzY6z1bIrbSzArCqm0sb2iD+kJL81O0 /qqdXjBxZUkKiVAMNNp7xJGZHHFKWUxT2+UX/
tlyx4tT4dzrFIkdDXkcMmqfsRxd 1NEVaAaT8SECgYAoU7BPtpIun43YTpfUfr3pSIN6oZeKoxSbw9i4MNC
+4fSDRPC+ 80ImcmZRL7taF+Y7p0jxAOTuIkdJC8NbAiv5J9WzrwQ+5MF2BPB/2bYnRa6tNofH kZDy/
9bXYsl6qw2p5Ety8wVcgZTMvFMGiG/32IpZ65FYWEU8L5qSRwfFhQKBgQC9 ihjZTj/bTHtRiHZppzCvyYm/Igd
+Uwtsy0uXR1n0G1SQENgrTBD/J6AzdfJae6tE P0U8YIM5Oqxf2i/as9ay+IPRecMl4eSxz7jJWAGx6Yx/3AZ
+hAB1ZbNbqniCLYNk d0MvjwmA25ATO+ro4OZ7AdEpQbk3l9aG/WFyYBz9AQKBgQCucFPA1l5eslL8196V
WMr2Qo0tqzl7CGSoWQk2Sa2HZtZdfofXAaaqo+zvJ6RPHtJh0jgJtx536DVV3egI
37YrdQyJbCPZXQ3SPgqWCorUnXBwq/nxS06uwu6JBxUFc57ijmMU4fWYNrvkkmWb 7keAg/
r5Uy1joMAvBN1I6lB8pg== -----END PRIVATE KEY-----"
}
```

## Example Responses

**Status code: 200**

OK

```
{
  "id" : "6e2be127b79f4a418414952ad5d8c59f",
  "name" : "certificatename94319",
  "content" : "-----BEGIN CERTIFICATE-----\nMIIB
+TCCAaOgAwIBAgIUJP9I8OupQ77w0bGL2yWOQXreM4kwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMC
QVUxEzARBgNVBAgMClNvbWUtU3RhdGUxDzANBgNVBAoMBkh1YXdlaTEcMBoGA1UEAwwTd2FmLmh1YXdl
aWNsb3VkLmNvbTAeFw0yMDA3MDkwNTQ2MDRaFw0yMDA4MDgwNTQ2MDRaMFExCzAJBgNVBAYTAkFV
MRMwEQYDVQQIDApTb21lLVN0YXRlMQ8wDQYDVQQKDAZIdWF3ZWkxHDAaBgNVBAMME3dhZi5odWF3Z
WljbG91ZC5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIAkEA0UEbMzbvgOJTKrKcDUw9xjFqxM7BaQFM3SLs
QlmD5hkzygyL1ra
+cWajPJlTCxz9Ph6qldna2+OrIuTdvCcpjwIDAQABo1MwUTAdBgNVHQ4EFgQUE7ZQNcgl3lmryx1s5gy9mnC1rs
YwHwYDVR0jBBgwFoAUE7ZQNcgl3lmryx1s5gy9mnC1rsYwDwYDVR0TAQH/BAUwAwEB/
zANBgkqhkiG9w0BAQsFAANBAM5wGi88jYWLgOnGbae5hH3I9lMBKxGqv17Cbm1tjWuUogVINz86lqvCpuhzLv
D/vzJAqPIuDwqM8uvzjgRfZs8=\n-----END CERTIFICATE-----",
  "key" : "-----BEGIN RSA PRIVATE KEY-----
\nMIIBOQIBAAJBANFBGzM274DiUyqynA1MPcYxasTOwWkBTN0i7EJZg+YZM8oMi9a2vnFmozyZUwsc/
T4eqpXZ2tvjqyLk3bwnKY8CAwEAAQJBAI7LMPaH/HQk/b/bVmY0qsr
+me9nb9BqFLuqwzKbx0hSmWPOWFsd3rOFlSopyHqgYtAsPfvPumEdGbdnCyU8zAECIQD71768K1ejb
+ei2lqZqHaczqdUNQxMh54yot9F2yVWjwIhANS1Y1Jv89WEU/ZvvMS9a4638Msv2c4GGp08RtXNYn0BAiA0H4b
+cwoEbZjHf+HYg6Fo+uxu5TvSaw8287a6Qo0LyQIfVZSlYYWplT6oiX5rdLzBiap4N0gJWdsa2ihmV59LAQIgK8N
+j1daq63b0bJ9k4HruhQtpgxI6U9nFBemH4zTRYM=\n-----END RSA PRIVATE KEY-----",
  "timestamp" : 1650595334578,
  "expire_time" : 1596865564000
}
```

## Status Codes

| Status Code | Description |
|---|---|
| 200 | OK |

| Status Code | Description |
|---|---|
| 400 | Request failed. |
| 401 | Insufficient token permissions. |
| 500 | Internal server error. |

## Error Codes

See **Error Codes**.

## 4.2.13.3 Querying a Certificate

## Function

This API is used to query a certificate.

## URI

GET /v1/{project_id}/waf/certificate/{certificate_id}

**Table 4-759** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| certificate_id | Yes | String | HTTPS certificate ID. It can be obtained by calling the **ListCertificates** API. |

**Table 4-760** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| enterprise_project_id | No | String | ID of the enterprise project. It can be obtained by called the **ListEnterpriseProject** API of EPS. |

## Request Parameters

**Table 4-761** 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-762** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Certificate ID. |
| name | String | Certificate Name |
| content | String | Certificate file, which is in PEM format. |
| 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 are **0**, **1**, and **2**. **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 4-763** BindHost

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain ID |
| hostname | String | Protected domain name |

| Parameter | Type | Description |
|---|---|---|
| waf_type | String | Domain name mode: cloud (cloud mode)/ premium (dedicated mode) |
| mode | String | This parameter is required only by the dedicated mode. |

**Status code: 400**

**Table 4-764** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-765** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-766** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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
+TCCAaOgAwIBAgIUJP9I8OupQ77w0bGL2yWOQXreM4kwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMC
QVUxEzARBgNVBAgMClNvbWUtU3RhdGUxDzANBgNVBAoMBkh1YXdlaTEcMBoGA1UEAwwTd2FmLmh1YXdl
aWNsb3VkLmNvbTAeFw0yMDA3MDkwNTQ2MDRaFw0yMDA4MDgwNTQ2MDRaMFExCzAJBgNVBAYTAkFV
MRMwEQYDVQQIDApTb21lLVN0YXRlMQ8wDQYDVQQKDAZIdWF3ZWkxHDAaBgNVBAMME3dhZi5odWF3Z
WljbG91ZC5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIAkEA0UEbMzbvgOJTKrKcDUw9xjFqxM7BaQFM3SLs
QlmD5hkzygyL1ra
+cWajPJlTCxz9Ph6qldna2+OrIuTdvCcpjwIDAQABo1MwUTAdBgNVHQ4EFgQUE7ZQNcgl3lmryx1s5gy9mnC1rs
YwHwYDVR0jBBgwFoAUE7ZQNcgl3lmryx1s5gy9mnC1rsYwDwYDVR0TAQH/BAUwAwEB/
zANBgkqhkiG9w0BAQsFAANBAM5wGi88jYWLgOnGbae5hH3I9lMBKxGqv17Cbm1tjWuUogVINz86lqvCpuhzLv
D/vzJAqPIuDwqM8uvzjgRfZs8=\n-----END CERTIFICATE-----",
  "key" : "-----BEGIN RSA PRIVATE KEY-----
\nMIIBOQIBAAJBANFBGzM274DiUyqynA1MPcYxasTOwWkBTN0i7EJZg+YZM8oMi9a2vnFmozyZUwsc/
T4eqpXZ2tvjqyLk3bwnKY8CAwEAAQJBAI7LMPaH/HQk/b/bVmY0qsr
+me9nb9BqFLuqwzKbx0hSmWPOWFsd3rOFlSopyHqgYtAsPfvPumEdGbdnCyU8zAECIQD71768K1ejb
+ei2lqZqHaczqdUNQxMh54yot9F2yVWjwIhANS1Y1Jv89WEU/ZvvMS9a4638Msv2c4GGp08RtXNYn0BAiA0H4b
+cwoEbZjHf+HYg6Fo+uxu5TvSaw8287a6Qo0LyQIfVZSlYYWplT6oiX5rdLzBiap4N0gJWdsa2ihmV59LAQIgK8N
+j1daq63b0bJ9k4HruhQtpgxI6U9nFBemH4zTRYM=\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 | Insufficient token permissions. |
| 500 | Internal server error. |

## Error Codes

See **Error Codes**.

## 4.2.13.4 Modifying a Certificate

## Function

This API is used to modify a certificate.

## URI

PUT /v1/{project_id}/waf/certificate/{certificate_id}

**Table 4-767** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| certificate_id | Yes | String | HTTPS certificate ID. It can be obtained by calling the **ListCertificates** API. |

**Table 4-768** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| enterprise_project_id | No | String | ID of the enterprise project. It can be obtained by called 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<br>Default: **application/json;charset=utf8** |

**Table 4-770** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | No | String | Certificate name. The value can contain a maximum of 64 characters. Only digits, letters, hyphens (-), underscores (_), and periods (.) are allowed. |

## Response Parameters

**Status code: 200**

**Table 4-771** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Certificate ID |
| name | String | Certificate Name |
| expire_time | Long | Certificate expiration timestamp |
| timestamp | Long | Time. |

**Status code: 400**

**Table 4-772** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-773** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-774** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
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 |
| 400 | Request failed. |
| 401 | Insufficient token permissions. |
| 500 | Internal server error. |

## Error Codes

See **Error Codes**.

### 4.2.13.5 Deleting a Certificate.

## Function

This API is used to delete a certificate.

## URI

DELETE /v1/{project_id}/waf/certificate/{certificate_id}

**Table 4-775** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| certificate_id | Yes | String | HTTPS certificate ID. It can be obtained by calling the **ListCertificates** API. |

**Table 4-776** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| enterprise_project_id | No | String | ID of the enterprise project. It can be obtained by called the **ListEnterpriseProject** API of EPS. |

## Request Parameters

**Table 4-777** 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<br>Default: **application/json;charset=utf8** |

## Response Parameters

**Status code: 200**

**Table 4-778** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Certificate ID |
| name | String | Certificate name |
| content | String | Certificate file in PEM format |
| key | String | Private key of the certificate, which is in PEM format. |
| expire_time | Long | Certificate expiration timestamp |
| exp_status | Integer | Certificate expiration status. The options are **0**, **1**, and **2**. **0**: The certificate is valid. **1**: The certificate has expired; **2**: The certificate will expire within one month. |
| timestamp | Long | Certificate upload timestamp |

| Parameter | Type | Description |
|---|---|---|
| bind_host | Array of **BindHost** objects | Domain name associated with the certificate |

**Table 4-779** BindHost

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain ID |
| hostname | String | Protected domain name |
| waf_type | String | Domain name mode: cloud (cloud mode)/ premium (dedicated mode) |
| mode | String | This parameter is required only by the dedicated mode. |

**Status code: 400**

**Table 4-780** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-781** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-782** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error Messages |

## Example Requests

```
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 | Insufficient token permissions. |
| 500 | Internal server error. |

## Error Codes

See **Error Codes**.

## 4.2.13.6 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 4-783** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID |
| certificate_id | Yes | String | HTTPS certificate ID. It can be obtained by calling the **ListCertificates** 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 called 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<br>Default: **application/json;charset=utf8** |

**Table 4-786** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cloud_host_ids | No | Array of strings | ID of HTTPS domain name in cloud mode. It can be obtained by calling the **ListHost** API. |
| premium_host_ids | No | Array of strings | ID of the HTTPS domain name in dedicated mode. It can be obtained by calling the **ListPremiumHost** API. |

## Response Parameters

**Status code: 200**

**Table 4-787** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Certificate ID. |
| name | String | Certificate Name |
| timestamp | Long | Time. |
| expire_time | Long | Expiration date |
| bind_host | Array of **CertificateBundingHostBody** objects | Domain name list |

**Table 4-788** CertificateBundingHostBody

| Parameter | Type | Description |
|---|---|---|
| id | String | Domain name ID |
| hostname | String | Domain Name |
| waf_type | String | WAF mode. The value can be **cloud** for the cloud mode or **premium** for the dedicated mode.<br>Enumeration values:<br>● **cloud**<br>● **premium** |

**Status code: 400**

**Table 4-789** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 401**

**Table 4-790** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

**Status code: 500**

**Table 4-791** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error Code |
| error_msg | String | Error Messages |

## Example Requests

```
GET 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**

Request succeeded.

```
{
  "id" : "3ac1402300374a63a05be68c641e92c8",
  "name" : "www.abc.com",
  "timestamp" : 1636343349139,
  "expire_time" : 1650794100000,
  "bind_host" : [ {
    "id" : "e350cf556da34adab1f017523d1c05ed",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud",
    "bandwidth" : 0,
    "qps" : 0
  } ]
}
```

## Status Codes

| Status Code | Description |
|---|---|
| 200 | Request succeeded. |
| 400 | Request failed |

| Status Code | Description |
|---|---|
| 401 | Insufficient token permissions. |
| 500 | Internal server error. |

## Error Codes

See **Error Codes**.

# 5 Permissions and Supported Actions

## 5.1 Introduction

This chapter describes fine-grained permissions management for your WAF. If your account does not need individual IAM users, then you may skip over this chapter.

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using roles and policies. Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions, meeting requirements for secure access control.

**NOTE**

Policy-based authorization is useful if you want to allow or deny the access to an API.

An account has all of the permissions required to call all APIs, but IAM users must have the required permissions specifically assigned. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions allowing the actions can call the API successfully.

## 5.2 Supported Actions

WAF provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: Statements in a policy that allow or deny certain operations.
- APIs: REST APIs that can be called by a user who has been granted specific permissions.
- Actions: Specific operations that are allowed or denied in a custom policy.

- Related actions: Actions on which a specific action depends to take effect. When assigning permissions for the action to a user, you also need to assign permissions for the related actions.
- IAM or enterprise projects: Type of projects for which an action will take effect. Policies that contain actions for both IAM and enterprise projects can be used and take effect for both IAM and Enterprise Management. Policies that only contain actions for IAM projects can be used and only take effect for IAM.

**NOTE**

√: supported; x: not supported

| Permission | API | Action | Dependency Item | IAM Project |
|---|---|---|---|---|
| Querying details about a dedicated WAF instance | GET /v1/{project_id}/premium-waf/instance/{instance_id} | waf:premiumInstance:get | - | √ |
| Deleting a dedicated WAF instance | DELETE /v1/{project_id}/premium-waf/instance/{instance_id} | waf:premiumInstance:delete | - | √ |
| Renaming a dedicated WAF instance | PUT /v1/{project_id}/premium-waf/instance/{instance_id} | waf:premiumInstance:put | - | √ |
| Creating a dedicated WAF instance | POST /v1/{project_id}/premium-waf/instance | waf:premiumInstance:create | - | √ |
| Querying dedicated WAF instances | GET /v1/{project_id}/premium-waf/instance | waf:premiumInstance:list | - | √ |
| Adding a domain name to a dedicated WAF instance | POST /v1/{project_id}/premium-waf/host | waf:instance:create | - | √ |
| Querying domain names protected by dedicated WAF engines | GET /v1/{project_id}/premium-waf/host | waf:instance:list | - | √ |
| Modifying a domain name protected by a dedicated WAF instance | PUT /v1/{project_id}/premium-waf/host/{host_id} | waf:instance:put | - | √ |

| Permission | API | Action | Dependency Item | IAM Project |
|---|---|---|---|---|
| Querying domain name settings in dedicated mode | GET /v1/{project_id}/premium-waf/host/{host_id} | waf:instance:get | - | √ |
| Deleting a domain name from a dedicated WAF instance | DELETE /v1/{project_id}/premium-waf/host/{host_id} | waf:instance:delete | - | √ |
| Modifying the protection status of a domain name in dedicated mode | PUT /v1/{project_id}/premium-waf/host/{host_id}/protect-status | waf:instance:put | - | √ |
| Modifying the access status of a domain name in dedicated mode | PUT /v1/{project_id}/premium-waf/host/{host_id}/access_status | waf:instance:put | - | √ |
| Querying the policy list | GET /v1/{project_id}/waf/policy | waf:policy:list | - | √ |
| Creating a protection policy | POST /v1/{project_id}/waf/policy | waf:policy:create | - | √ |
| Querying a policy by ID | GET /v1/{project_id}/waf/policy/{policy_id} | waf:policy:get | - | √ |
| Updating a policy | PATCH /v1/{project_id}/waf/policy/{policy_id} | waf:policy:put | - | √ |
| Deleting a protection policy | DELETE /v1/{project_id}/waf/policy/{policy_id} | waf:policy:delete | - | √ |
| Querying the blacklist and whitelist rule list | GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip | waf:whiteBlackIpRule:list | - | √ |

| Permission | API | Action | Dependency Item | IAM Project |
|---|---|---|---|---|
| Creating a blacklist or whitelist rule | POST /v1/{project_id}/waf/policy/{policy_id}/whiteblackip | waf:whiteBlackIpRule:create | - | √ |
| Querying a blacklist or whitelist rule | GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id} | waf:whiteBlackIpRule:get | - | √ |
| Updating a blacklist or whitelist rule | PUT /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id} | waf:whiteBlackIpRule:put | - | √ |
| Deleting a blacklist or whitelist rule | DELETE /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id} | waf:whiteBlackIpRule:delete | - | √ |
| Querying the CC attack protection rule list | GET /v1/{project_id}/waf/policy/{policy_id}/cc | waf:ccRule:list | - | √ |
| Creating a CC attack protection rule | POST /v1/{project_id}/waf/policy/{policy_id}/cc | waf:ccRule:create | - | √ |
| Querying a CC attack protection rule by ID | GET /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id} | waf:ccRule:get | - | √ |
| Updating a CC attack protection rule | PUT /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id} | waf:ccRule:put | - | √ |
| Deleting a CC attack protection rule | DELETE /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id} | waf:ccRule:delete | - | √ |
| Querying precise protection rules | GET /v1/{project_id}/waf/policy/{policy_id}/custom | waf:preciseProtectionRule:list | - | √ |

| Permission | API | Action | Dependency Item | IAM Project |
|---|---|---|---|---|
| Creating a precise protection rule | POST /v1/{project_id}/waf/policy/{policy_id}/custom | waf:preciseProtectionRule:create | - | √ |
| Querying a precise protection rule by ID | GET /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id} | waf:preciseProtectionRule:get | - | √ |
| Updating a precise protection rule | PUT /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id} | waf:preciseProtectionRule:put | - | √ |
| Deleting a precise protection rule | DELETE /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id} | waf:preciseProtectionRule:delete | - | √ |
| Querying data masking rules | GET /v1/{project_id}/waf/policy/{policy_id}/privacy | waf:privacyRule:list | - | √ |
| Adding a data masking rule | POST /v1/{project_id}/waf/policy/{policy_id}/privacy | waf:privacyRule:create | - | √ |
| Querying a data masking rule by ID | GET /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id} | waf:privacyRule:get | - | √ |
| Updating a data masking rule | PUT /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id} | waf:privacyRule:put | - | √ |
| Deleting a data masking rule | DELETE /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id} | waf:privacyRule:delete | - | √ |
| Querying the list of web tamper protection rules | GET /v1/{project_id}/waf/policy/{policy_id}/antitamper | waf:antiTamperRule:list | - | √ |

| Permission | API | Action | Dependency Item | IAM Project |
|---|---|---|---|---|
| Creating a web tamper protection rule | POST /v1/{project_id}/waf/policy/{policy_id}/antitamper | waf:antiTamperRule:create | - | √ |
| Querying a web tamper protection rule by ID | GET /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id} | waf:antiTamperRule:get | - | √ |
| Deleting a web tamper protection rule | DELETE /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id} | waf:antiTamperRule:delete | - | √ |
| Updating the cache of a web tamper protection rule | POST /v1/{project_id}/waf/policy/{policy_id}/antitamper/{antitamperid}/refresh | waf:antiTamperRule:create | - | √ |
| Querying false alarm masking rules | GET /v1/{project_id}/waf/policy/{policy_id}/ignore | waf:falseAlarmMaskRule:list | - | √ |
| Adding a false alarm masking rule | POST /v1/{project_id}/waf/policy/{policy_id}/ignore | waf:falseAlarmMaskRule:create | - | √ |
| Querying a false alarm masking rule | GET /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id} | waf:falseAlarmMaskRule:get | - | √ |
| Updating a false alarm masking rule | PUT /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id} | waf:falseAlarmMaskRule:put | - | √ |
| Deleting a false alarm masking rule | DELETE /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id} | waf:falseAlarmMaskRule:delete | - | √ |
| Querying the certificate list | GET /v1/{project_id}/waf/certificate | waf:certificate:get | - | √ |

| Permission | API | Action | Dependency Item | IAM Project |
|---|---|---|---|---|
| Creating a certificate | POST /v1/{project_id}/waf/certificate | waf:certificate:create | - | √ |
| Querying a certificate | GET /v1/{project_id}/waf/certificate/{certificate_id} | waf:certificate:list | - | √ |
| Modifying a certificate | PUT /v1/{project_id}/waf/certificate/{certificate_id} | waf:certificate:put | - | √ |
| Deleting a certificate | DELETE /v1/{project_id}/waf/certificate/{certificate_id} | waf:certificate:delete | - | √ |
| Applying a certificate to a domain name | POST /v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts | waf:certificate:apply | - | √ |
| Querying the number of requests and attacks on dashboard | GET /v1/{project_id}/waf/overviews/statistics | waf:event:get | - | √ |
| Querying top N statistics on dashboard | GET /v1/{project_id}/waf/overviews/classification | waf:event:get | - | √ |
| Querying the list of attack events | GET /v1/{project_id}/waf/event | waf:event:get | - | √ |
| Querying attack event details | GET /v1/{project_id}/waf/event/{eventid} | waf:event:get | - | √ |

# A Appendix

## A.1 Status Codes

| Status Code | Description | Meaning |
|---|---|---|
| 200 | OK | The request has succeeded. |
| 204 | No Content | The server successfully processed the request and is not returning any content. |
| 400 | Bad Request | Incorrect parameter |
| 401 | Unauthorized | Authentication failed. |
| 403 | Forbidden | No permission. The access is denied. |
| 404 | Not Found | The requested resource could not be found. |
| 406 | Not Acceptable | The request is unacceptable. |
| 409 | Conflict | The request could not be processed because of conflict in the current state of the resource. |
| 500 | Internal Error | Internal server error |
| 503 | Server Unavailable | The server is currently unavailable. |

# A.2 Cloud Mode Error Code

## Function Description

A customized message is returned when errors, such as 400 or 500, occur in an extended public cloud API. This section describes the meaning of each error code.

## Response Format

- HTTP status code

```
400
```

- Response body example

```
{
"error_code": "11000000",
"error_msg": "hx error."
}
```

## Error Code Description

| Error Code | Description |
|---|---|
| WAF.1001 | Invalid request |
| WAF.1002 | Invalid page number or page size |
| WAF.1003 | Invalid ID |
| WAF.1004 | Invalid name |
| WAF.1005 | Invalid path |
| WAF.1006 | Invalid rate limiting mode |
| WAF.1007 | Invalid user identifier |
| WAF.1008 | Invalid protective action |
| WAF.1009 | Invalid CC attack protection rule |
| WAF.1012 | Invalid Referer |
| WAF.1013 | Invalid type |
| WAF.1014 | Invalid logic |
| WAF.1015 | Invalid subfield |
| WAF.1016 | Invalid content |
| WAF.1018 | Invalid precise protection rule |
| WAF.1019 | Invalid data masking rule |
| WAF.1020 | Invalid User-Agent |
| WAF.1021 | Invalid IP address |

| Error Code | Description |
|---|---|
| WAF.1022 | Invalid false alarm masking rule |
| WAF.1023 | Invalid number |
| WAF.1025 | Invalid time |
| WAF.1029 | Invalid protection level |
| WAF.1030 | Invalid priority |
| WAF.1031 | Invalid attack type |
| WAF.1600 | Invalid domain name |
| WAF.1601 | Invalid protocol |
| WAF.1602 | Invalid server address |
| WAF.1603 | Invalid port |
| WAF.1604 | Invalid protection status or connection status |
| WAF.1605 | Invalid certificate content format |
| WAF.1606 | Invalid private key format |
| WAF.2001 | IDs do not match. |
| WAF.2002 | The protective action cannot be set to block. |
| WAF.2004 | The user identifier is unavailable in a CC attack protection rule. |
| WAF.2005 | The condition list in the precise protection rule is empty. |
| WAF.2006 | Subfields cannot be set for conditions in the precise protection rule. |
| WAF.2007 | The precise protection rule contains duplicate conditions. |
| WAF.2008 | Wildcard domains are not supported. |
| WAF.3001 | The requested resource was not found. |
| WAF.3002 | The number of resources exceeds the maximum limit allowed. |
| WAF.3003 | The resource is in use. |
| WAF.3004 | The system is busy. |
| WAF.3005 | The domain name already exists. |
| WAF.3006 | The rule name already exists. |
| WAF.3007 | Rules conflict with each other. |

| Error Code | Description |
|---|---|
| WAF.3008 | The rule already exists. |
| WAF.3010 | The policy has been bound to the domain name. |
| WAF.4000 | The API cannot be found. |
| WAF.4001 | The method is not allowed. |
| WAF.5000 | Internal error |
| WAF.5001 | Failed to access data. |
| WAF.5002 | HTTP request failed. |
| WAF.5003 | Elasticsearch request failed. |
| WAF.6000 | Connection failed. |
| WAF.6001 | The request is not permitted. |
| WAF.6002 | Failed to read obtained data. |
| WAF.6003 | Failed to export data. |
| WAF.6004 | Failed to import data. |
| WAF.7001 | The data exceeds the valid length. |
| WAF.9001 | IAM authentication failed. |
| WAF.9002 | No permission |

# A.3 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 |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 400 | WAF. 00011005 | name.illegal | Illegal name | Check name |
| 400 | WAF. 00011006 | host.illegal | Illegal domain name | Check domain name |
| 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 |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 400 | WAF. 00011014 | website.not.register | The website has not been put on record | Filing website |
| 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 |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 400 | WAF. 00013004 | protocol.not.support | Protocol not supported | Through ELB conversion protocol |
| 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.protect.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 |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 400 | WAF. 00014010 | port.protocol. mismatch | Port and protocol mismatch | Select the matching protocol and port |
| 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 |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 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 |
| 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 |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 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 |
| 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 |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 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 |
| 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 |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 403 | WAF. 00022005 | insufficient.quota | Insufficient resources | It is recommended to purchase the upgrade package of corresponding resources |
| 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.4 Obtaining a Project ID

1. Obtain the token.

   For details, see **Token-based Authentication**.

2. Obtain the project ID.

   The API for obtaining the project ID is **GET https://iam.eu-west-0.myhuaweicloud.com/v3/*projects***.

   Add **X-Auth-Token** to the request header, and set the value of **X-Auth-Token** to the token obtained in the preceding step.

The following is an example response. **id** indicates the project ID.

```
{
    "links": {},
    "projects": [
        {
            "is_domain": ,
            "description": "",
            "links": {},
            "enabled": true,
            "id": "",   //Project ID
            "parent_id": "",
            "domain_id": "",
            "name": ""
        },
        ...
   ]
}
```

# A.5 Character Set Specifications

- Character Set Specifications for Key

  The key cannot be left blank or be an empty string.

  – In Deutsche Telekom, a tag key can contain uppercase letters, lowercase letters, digits, hyphens (-), underscores (_), and sign @.

  – In other environments, a tag key cannot contain the following characters: ASCII (0-31), equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (|), and slashes (/).

- Character Set Specifications for Value

  The value cannot be left blank but can be an empty string.

  – In Deutsche Telekom, a tag value can contain uppercase letters, lowercase letters, digits, hyphens (-), and underscores (_).

  – In other environments, a tag value cannot contain the following characters: ASCII (0-31), equal signs (=), asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), commas (,), vertical bars (|), and slashes (/).

# B Change History

| Released On | Description |
|---|---|
| 2022-12-28 | This issue is the second official issue.<br>Added the APIs for the dedicated mode. |
| 2021-07-14 | This issue is the first official release. |