Web Application Firewall

API Reference

Issue	01
Date	2022-08-05

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei 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 updating.

Before you start, ensure that you are familiar with WAF. For details, see *Web Application Firewall User Guide*.

1.2 API Calling

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

1.3 Endpoints

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

1.4 Concepts

- Account

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

- User

  An IAM user is created by an account in IAM to use cloud services. Each IAM user has its own identity credentials (password and access keys).

- Region

  Regions are divided based on geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.

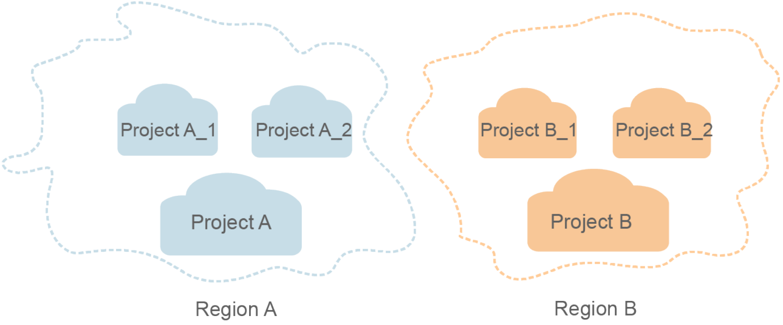
- Availability Zone (AZ)

  An AZ comprises one or multiple physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Compute, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability systems.

- Project

  Projects group and isolate compute, storage, and network resources across physical regions. A default project is provided for each region, and subprojects can be created under each default project. Users can be granted permissions to access all resources in a specific project. For more refined access control, create subprojects under a project and create resources in the subprojects. Users can then be assigned permissions to access only specific resources in the subprojects.

Figure 1-1 Project isolation model



2 API Overview

You can use all functions of WAF through its APIs.

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

3 API Calling

3.1 Making an API Request

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

Request URI

A request URI is in the following format:

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

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

- **URI-scheme**:

  Protocol used to transmit requests. All APIs use HTTPS.

- **Endpoint**:

  Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**.

  For example, the endpoint of IAM in the **my-kualalumpur-1** region is **iam.my-kualalumpur-1.alphaedge.tmone.com.my**.

- **resource-path**:

  Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.

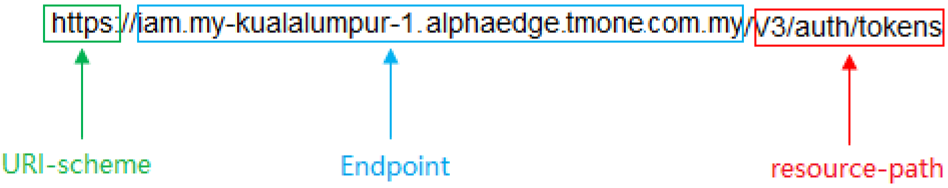
- **query-string**:

  Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in the **my-kualalumpur-1** region, obtain the endpoint of IAM (**iam.my-kualalumpur-1.alphaedge.tmone.com.my**) for this region and the **resource-path** (**/v3/auth/tokens**) in the URI of the API in **Regions and Engpoints**. Then, construct the URI as follows:

```
https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
```

Figure 3-1 Example URI


https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
URI-scheme
Endpoint
resource-path

NOTE

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

Request Methods

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

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

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

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/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://iam.my-kualalumpur-1.alphaedge.tmone.com.my/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. You can learn more information about projects from **Regions and Endpoints**.

NOTE

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

```
POST https://iam.my-kualalumpur-1.alphaedge.tmone.com.my/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://iam.my-kualalumpur-1.alphaedge.tmone.com.my/v3/auth/tokens
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK-based Authentication

NOTE

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

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

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

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

NOTICE

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

3.3 Response

Status Code

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

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

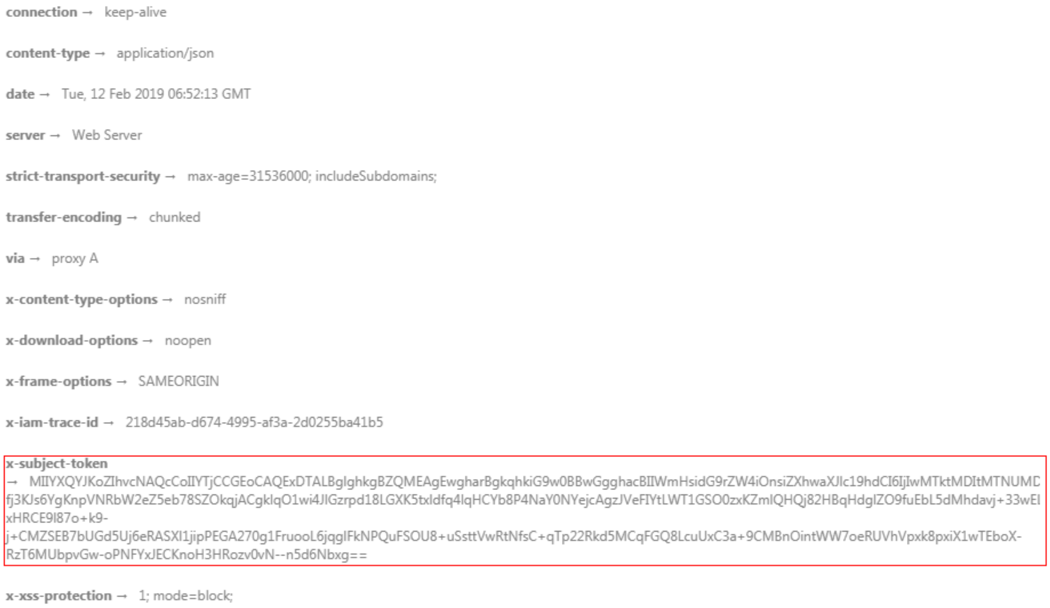
For example, if status code **201** is returned for calling the API used to obtain a user token, the request is successful.

Response Header

Similar to a request, a response also has a header, for example, **Content-Type**.

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

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



```
connection → keep-alive

content-type → application/json

date → Tue, 12 Feb 2019 06:52:13 GMT

server → Web Server

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

transfer-encoding → chunked

via → proxy A

x-content-type-options → nosniff

x-download-options → noopen

x-frame-options → SAMEORIGIN

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

x-subject-token
→ MIIYXQYJKoZIhvcNAQcCoIIYTjCCGEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOnsiZXhwaXJlc19hdCI6IjIwMTktMDItMTNUMD
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkqjACgklqO1wi4JIGzrpd18LGXK5txldfq4lqHCYb8P4NaY0NYejcAgzJVeFIYtLWT1GSO0zxKZmIQHQj82HBqHdgIZO9fuEbL5dMhdavj+33wEl
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jqglFkNPQuFSOU8+uSsttVwRtNfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUVhVpxk8pxiX1wTEboX-
RzT6MUbpvGw-oPNFYxJECKnoH3HRozv0vN--n5d6Nbxg==

x-xss-protection → 1; mode=block;
```

(Optional) Response Body

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

The following shows part of the response body for the API to . 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, an error code and a message will be displayed. The following shows an error response body.

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

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

4 API

4.1 Policy Management

4.1.1 Querying the Protection Policy List

Function

This API is used to query the protection policy list.

URI

GET /v1/{project_id}/waf/policy

Table 4-1 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-2 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number Default: **1**
pagesize	No	Integer	Number of records on each page Default: **10**
name	No	String	Policy name

Request Parameters

Table 4-3 Request header parameters

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

Response Parameters

Status code: 200

Table 4-4 Response body parameters

Parameter	Type	Description
total	Integer	Number of policies
items	Array of **PolicyResponse** objects	Policy details

Table 4-5 PolicyResponse

Parameter	Type	Description
id	String	Policy ID
name	String	Policy name
action	**PolicyAction** object	Operation
options	**PolicyOption** object	Option
level	Integer	Protection level
full_detection	Boolean	Detection mode in a precise protection rule
bind_host	Array of **BindHost** objects	Basic information about the protected domain name
timestamp	Long	Time the policy was created

Parameter	Type	Description
extend	Map<String,String>	Extended field

Table 4-6 PolicyAction

Parameter	Type	Description
category	String	Protection level. The options are log and block.

Table 4-7 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled
common	Boolean	Whether general check is enabled
crawler	Boolean	Whether anti-crawler is enabled
crawler_engine	Boolean	Whether the search engine check is enabled
crawler_scanner	Boolean	Whether anti-crawler is enabled
crawler_script	Boolean	Whether JavaScript-based anti-crawler is enabled
crawler_other	Boolean	Whether the other check item of anti-crawler is enabled
webshell	Boolean	Whether web shell check is enabled
cc	Boolean	Whether the CC attack protection is enabled
custom	Boolean	Whether precise protection is enabled
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled
ignore	Boolean	Whether false alarm masking is enabled
privacy	Boolean	Whether data masking is enabled
antitamper	Boolean	Whether web tamper protection is enabled

Table 4-8 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF edition for the domain name. The options are cloud and premium.
mode	String	(Dedicated mode only) Special domain name mode

Status code: 400

Table 4-9 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-10 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-11 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.1.2 Creating a Protection Policy

Function

This API is used to create a protection policy.

URI

POST /v1/{project_id}/waf/policy

Table 4-12 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-13 Request header parameters

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

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

Table 4-14 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Policy name. A policy name can contain only digits, letters, and underscores (_), and contains a maximum of 64 characters.

Response Parameters

Status code: 200

Table 4-15 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Policy name
level	Integer	Protection level
action	**PolicyAction** object	Operation
options	**PolicyOption** object	Option
full_detection	Boolean	Detection mode in a precise protection rule
hosts	Array of strings	ID of the protected website.
bind_host	Array of **BindHost** objects	Information about the protected website
timestamp	Long	Time the policy was created
extend	Object	Extended field

Table 4-16 PolicyAction

Parameter	Type	Description
category	String	Protection level. The options are log and block.

Table 4-17 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled
common	Boolean	Whether general check is enabled
crawler	Boolean	Whether anti-crawler is enabled
crawler_engine	Boolean	Whether the search engine check is enabled
crawler_scanner	Boolean	Whether anti-crawler is enabled
crawler_script	Boolean	Whether JavaScript-based anti-crawler is enabled
crawler_other	Boolean	Whether the other check item of anti-crawler is enabled
webshell	Boolean	Whether web shell check is enabled
cc	Boolean	Whether the CC attack protection is enabled
custom	Boolean	Whether precise protection is enabled
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled
ignore	Boolean	Whether false alarm masking is enabled
privacy	Boolean	Whether data masking is enabled
antitamper	Boolean	Whether web tamper protection is enabled

Table 4-18 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF edition for the domain name. The options are cloud and premium.

Parameter	Type	Description
mode	String	(Dedicated mode only) Special domain name mode

Status code: 400

Table 4-19 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-20 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-21 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.1.3 Querying a Protection Policy by ID

Function

This API is used to query a protection policy by ID.

URI

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

Table 4-22 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Request Parameters

Table 4-23 Request header parameters

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

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

Response Parameters

Status code: 200

Table 4-24 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Policy name
action	**PolicyAction** object	Operation
options	**PolicyOption** object	Option
level	Integer	Protection level
full_detection	Boolean	Detection mode in a precise protection rule
bind_host	Array of **BindHost** objects	Basic information about the protected domain name
timestamp	Long	Time the policy was created
extend	Map<String,String>	Extended field

Table 4-25 PolicyAction

Parameter	Type	Description
category	String	Protection level. The options are log and block.

Table 4-26 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled
common	Boolean	Whether general check is enabled

Parameter	Type	Description
crawler	Boolean	Whether anti-crawler is enabled
crawler_engine	Boolean	Whether the search engine check is enabled
crawler_scanner	Boolean	Whether anti-crawler is enabled
crawler_script	Boolean	Whether JavaScript-based anti-crawler is enabled
crawler_other	Boolean	Whether the other check item of anti-crawler is enabled
webshell	Boolean	Whether web shell check is enabled
cc	Boolean	Whether the CC attack protection is enabled
custom	Boolean	Whether precise protection is enabled
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled
ignore	Boolean	Whether false alarm masking is enabled
privacy	Boolean	Whether data masking is enabled
antitamper	Boolean	Whether web tamper protection is enabled

Table 4-27 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF edition for the domain name. The options are cloud and premium.
mode	String	(Dedicated mode only) Special domain name mode

Status code: 400

Table 4-28 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-29 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-30 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.1.4 Updating the Domain Name of a Protection Policy

Function

This API is used to update domain names a protection policy applies to.

URI

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

Table 4-31 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Table 4-32 Query parameters

Parameter	Mandatory	Type	Description
hosts	Yes	String	Domain name ID. It can be obtained from the protected website list.

Request Parameters

Table 4-33 Request header parameters

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

Response Parameters

Status code: 200

Table 4-34 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Policy name
action	**PolicyAction** object	Operation
options	**PolicyOption** object	Option
level	Integer	Protection level
full_detection	Boolean	Detection mode in a precise protection rule
bind_host	Array of **BindHost** objects	Basic information about the protected domain name
timestamp	Long	Time the policy was created
extend	Map<String,String>	Extended field

Table 4-35 PolicyAction

Parameter	Type	Description
category	String	Protection level. The options are log and block.

Table 4-36 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled
common	Boolean	Whether general check is enabled
crawler	Boolean	Whether anti-crawler is enabled
crawler_engine	Boolean	Whether the search engine check is enabled
crawler_scanner	Boolean	Whether anti-crawler is enabled
crawler_script	Boolean	Whether JavaScript-based anti-crawler is enabled
crawler_other	Boolean	Whether the other check item of anti-crawler is enabled

Parameter	Type	Description
webshell	Boolean	Whether web shell check is enabled
cc	Boolean	Whether the CC attack protection is enabled
custom	Boolean	Whether precise protection is enabled
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled
ignore	Boolean	Whether false alarm masking is enabled
privacy	Boolean	Whether data masking is enabled
antitamper	Boolean	Whether web tamper protection is enabled

Table 4-37 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF edition for the domain name. The options are cloud and premium.
mode	String	(Dedicated mode only) Special domain name mode

Status code: 400

Table 4-38 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-39 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-40 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.1.5 Updating a Protection Policy

Function

This API is used to update a protection policy. The request body can contain only the part that needs to be updated.

URI

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

Table 4-41 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Request Parameters

Table 4-42 Request header parameters

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

Table 4-43 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Policy name
action	No	**PolicyAction** object	Operation
options	No	**PolicyOption** object	Option

Table 4-44 PolicyAction

Parameter	Mandatory	Type	Description
category	No	String	Protection level. The options are log and block.

Table 4-45 PolicyOption

Parameter	Mandatory	Type	Description
webattack	No	Boolean	Whether basic web protection is enabled
common	No	Boolean	Whether general check is enabled
crawler	No	Boolean	Whether anti-crawler is enabled
crawler_engine	No	Boolean	Whether the search engine check is enabled
crawler_scanner	No	Boolean	Whether anti-crawler is enabled
crawler_script	No	Boolean	Whether JavaScript-based anti-crawler is enabled
crawler_other	No	Boolean	Whether the other check item of anti-crawler is enabled
webshell	No	Boolean	Whether web shell check is enabled
cc	No	Boolean	Whether the CC attack protection is enabled
custom	No	Boolean	Whether precise protection is enabled
whiteblackip	No	Boolean	Whether blacklist and whitelist protection is enabled
ignore	No	Boolean	Whether false alarm masking is enabled
privacy	No	Boolean	Whether data masking is enabled
antitamper	No	Boolean	Whether web tamper protection is enabled

Response Parameters

Status code: 200

Table 4-46 Response body parameters

Parameter	Type	Description
id	String	Policy ID

Parameter	Type	Description
name	String	Policy name
action	**PolicyAction** object	Operation
options	**PolicyOption** object	Option
level	Integer	Protection level
full_detection	Boolean	Detection mode in a precise protection rule
bind_host	Array of **BindHost** objects	Basic information about the protected domain name
timestamp	Long	Time the policy was created
extend	Map<String,String>	Extended field

Table 4-47 PolicyAction

Parameter	Type	Description
category	String	Protection level. The options are log and block.

Table 4-48 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled
common	Boolean	Whether general check is enabled
crawler	Boolean	Whether anti-crawler is enabled
crawler_engine	Boolean	Whether the search engine check is enabled
crawler_scanner	Boolean	Whether anti-crawler is enabled
crawler_script	Boolean	Whether JavaScript-based anti-crawler is enabled
crawler_other	Boolean	Whether the other check item of anti-crawler is enabled
webshell	Boolean	Whether web shell check is enabled
cc	Boolean	Whether the CC attack protection is enabled

Parameter	Type	Description
custom	Boolean	Whether precise protection is enabled
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled
ignore	Boolean	Whether false alarm masking is enabled
privacy	Boolean	Whether data masking is enabled
antitamper	Boolean	Whether web tamper protection is enabled

Table 4-49 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF edition for the domain name. The options are cloud and premium.
mode	String	(Dedicated mode only) Special domain name mode

Status code: 400

Table 4-50 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-51 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-52 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.1.6 Deleting a Policy

Function

This API is used to delete a policy.

URI

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

Table 4-53 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Request Parameters

Table 4-54 Request header parameters

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

Response Parameters

Status code: 400

Table 4-55 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-56 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-57 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2 Rule Management

4.2.1 Querying False Alarm Masking Rules

Function

Querying False Alarm Masking Rules

URI

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

Table 4-58 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	policyid

Table 4-59 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number Default: **0**
pagesize	No	Integer	Number of records on each page Default: **10**

Request Parameters

Table 4-60 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token
Content-Type	Yes	String	Content type Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-61 Response body parameters

Parameter	Type	Description
total	Integer	Number of rules in the policy

Table 4-62 IngnoreItem

Parameter	Type	Description
id	String	Rule ID

Parameter	Type	Description
policyid	String	Policy ID
timestamp	Long	Rule creation timestamp
description	String	Rule description
status	Integer	Status. The options can be 0 and 1. 0: Disabled 1: Enabled
url	String	URL of the false alarm
rule	String	Masked rule. The value can be the ID of the matched rule, all rules (all), or enumeration value of the attack type. Enumeration values of attack types: XSS attacks: xss or sqli Command injection: cmdi Malicious crawlers: robot Local file inclusion: lfi Remote file inclusion: rfi Website Trojans: webshell CC attack: cc Precise protection: custom_custom IP address blacklist and whitelist: custom_whiteblackip Geolocation access control: custom_geoip Anti-tamper protection: antitamper Anti-crawler protection: anticrawler Data leakage prevention: leakage Illegal requests: illegal Other attack types: vuln
domain	Array of strings	Protected domain name
url_logic	String	URL match logic (prefix: prefix match; equal: full match)
advanced	**Advance** object	Advanced settings

Table 4-63 Advance

Parameter	Type	Description
index	String	Index (parameter: params; Session cookie: cookie; Header field: header; Body field: body; multiple combinations: multipart)
contents	Array of strings	Specified field (available only for param, cookie, and header)

Status code: 400

Table 4-64 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-65 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-66 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

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**.

4.2.2 Querying the Reference Table List

Function

This API is used to query the reference table list.

URI

GET /v1/{project_id}/waf/valuelist

Table 4-67 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-68 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number
pagesize	No	Integer	Number of records per page

Request Parameters

Table 4-69 Request header parameters

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

Response Parameters

Status code: 200

Table 4-70 Response body parameters

Parameter	Type	Description
total	Integer	Number of reference tables Minimum: **0** Maximum: **500**
items	Array of **ValueListResponseBody** objects	Reference table list

Table 4-71 ValueListResponseBody

Parameter	Type	Description
id	String	Reference table ID
name	String	Reference table name
type	String	Reference table type
description	String	Reference table description
timestamp	Long	Reference table creation timestamp
values	Array of strings	Reference table content

Status code: 400

Table 4-72 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-73 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-74 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.3 Creating a Reference Table

Function

This API is used to create a reference table.

URI

POST /v1/{project_id}/waf/valuelist

Table 4-75 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-76 Request header parameters

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

Table 4-77 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the reference table. The name is a string consisting of 2 to 32 characters. Minimum: **2** Maximum: **32**
type	Yes	String	Reference table type. For details, see the enumerated type list. Minimum: **2** Maximum: **32**
values	No	Array of strings	Reference table content
description	No	String	Description of the reference table, which contains a maximum of 128 characters. Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 4-78 Response body parameters

Parameter	Type	Description
id	String	Reference table ID
name	String	Reference table name
type	String	Reference table type
description	String	Reference table description
timestamp	Long	Reference table creation timestamp
values	Array of strings	Reference table content

Status code: 400

Table 4-79 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-80 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-81 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.4 Modifying a Reference Table

Function

This API is used to modify a reference table.

URI

PUT /v1/{project_id}/waf/valuelist/{valuelistid}

Table 4-82 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
valuelistid	Yes	String	Reference table ID

Request Parameters

Table 4-83 Request header parameters

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

Table 4-84 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the reference table. The name is a string consisting of 2 to 32 characters. Minimum: **2** Maximum: **32**
type	Yes	String	Reference table type. For details, see the enumerated type list. Minimum: **2** Maximum: **32**
values	No	Array of strings	Reference table content
description	No	String	Description of the reference table, which contains a maximum of 128 characters. Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 4-85 Response body parameters

Parameter	Type	Description
id	String	Reference table ID
name	String	Reference table name
type	String	Reference table type
description	String	Reference table description
timestamp	Long	Reference table creation timestamp
values	Array of strings	Reference table content

Status code: 400

Table 4-86 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-87 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-88 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.5 Deleting a Reference Table

Function

This API is used to delete a reference table.

URI

DELETE /v1/{project_id}/waf/valuelist/{valuelistid}

Table 4-89 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
valuelistid	Yes	String	Reference table ID

Request Parameters

Table 4-90 Request header parameters

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

Response Parameters

Status code: 200

Table 4-91 Response body parameters

Parameter	Type	Description
id	String	Reference table ID
name	String	Reference table name
type	String	Reference table type
description	String	Reference table description
timestamp	Long	Reference table creation timestamp
values	Array of strings	Reference table content

Status code: 400

Table 4-92 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-93 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-94 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.6 Querying the List of Blacklist and Whitelist Rules

Function

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

URI

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

Table 4-95 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Table 4-96 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number Default: **1**
pagesize	No	Integer	Number of records on each page. Default: **10**

Request Parameters

Table 4-97 Request header parameters

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

Response Parameters

Status code: 200

Table 4-98 Response body parameters

Parameter	Type	Description
total	Integer	Number of rules
items	Array of **WhiteBlackIpResponseBody** objects	Rule

Table 4-99 WhiteBlackIpResponseBody

Parameter	Type	Description
id	String	Rule ID
ip	String	Blacklist and whitelist
white	Integer	Type. The options are 0 and 1. 0: Block. 1: Allow
timestamp	Long	Time the rule was created

Status code: 400

Table 4-100 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-101 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-102 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.7 Creating a Whitelist or Blacklist Rule

Function

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

URI

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

Table 4-103 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Request Parameters

Table 4-104 Request header parameters

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

Table 4-105 Request body parameters

Parameter	Mandatory	Type	Description
addr	Yes	String	IP addresses in the blacklist or whitelist rule
description	No	String	Description of the blacklist or whitelist rule
white	No	Integer	Protective action for the rule. The options are 0, 1, and 2. 0: Block. 1: Allow. 2: Log only.

Response Parameters

Status code: 200

Table 4-106 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
ip	String	Blacklist and whitelist

Parameter	Type	Description
white	Integer	Type. The options are 0 and 1. 0: Block. 1: Allow
timestamp	Long	Time the rule was created

Status code: 400

Table 4-107 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-108 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-109 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.8 Updating a Whitelist or Blacklist 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 4-110 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.
rule_id	Yes	String	ID of the blacklist or whitelist rule, which can be obtained by querying the list of blacklist and whitelist rules through the ListWhiteblackipRule interface.

Request Parameters

Table 4-111 Request header parameters

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

Table 4-112 Request body parameters

Parameter	Mandatory	Type	Description
addr	Yes	String	IP addresses in the blacklist or whitelist rule
description	No	String	Description of the blacklist or whitelist rule
white	No	Integer	Protective action for the rule. The options are 0, 1, and 2. 0: Block. 1: Allow. 2: Log only.

Response Parameters

Status code: 200

Table 4-113 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	Description of the blacklist or whitelist rule
white	Integer	Protective action for the rule. The options are 0, 1, and 2. 0: Block. 1: Allow. 2: Log only.

Status code: 400

Table 4-114 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-115 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-116 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.9 Deleting a Whitelist or Blacklist 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 4-117 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.
rule_id	Yes	String	whiteblackIpRuleId

Request Parameters

Table 4-118 Request header parameters

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

Response Parameters

Status code: 400

Table 4-119 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-120 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-121 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.10 Adding a Data Masking Rule

Function

Adding a data masking rule

URI

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

Table 4-122 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Request Parameters

Table 4-123 Request header parameters

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

Table 4-124 Request body parameters

Parameter	Mandatory	Type	Description
id	No	String	Rule ID
url	No	String	URL to which the data masking rule applies
category	No	String	Masked field

Parameter	Mandatory	Type	Description
index	No	String	Name of the masked field

Response Parameters

Status code: 200

Table 4-125 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
url	String	URL to which the data masking rule applies
category	String	Masked field
index	String	Name of the masked field

Status code: 400

Table 4-126 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-127 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-128 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.11 Querying a Data Masking Rule

Function

This API is used to query a data masking rule.

URI

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

Table 4-129 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Table 4-130 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number
pagesize	No	Integer	Number of records on each page.

Request Parameters

Table 4-131 Request header parameters

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

Response Parameters

Status code: 200

Table 4-132 Response body parameters

Parameter	Type	Description
total	Integer	Number of rules
items	Array of **PrivacyResponseBody** objects	Rule

Table 4-133 PrivacyResponseBody

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
url	String	URL to which the data masking rule applies
category	String	Masked field
index	String	Name of the masked field

Status code: 400

Table 4-134 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-135 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-136 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.12 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 4-137 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.
rule_id	Yes	String	privacyRuleId

Request Parameters

Table 4-138 Request header parameters

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

Table 4-139 Request body parameters

Parameter	Mandatory	Type	Description
id	No	String	Rule ID
url	No	String	URL to which the data masking rule applies
category	No	String	Masked field
index	No	String	Name of the masked field

Response Parameters

Status code: 200

Table 4-140 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
url	String	URL to which the data masking rule applies
category	String	Masked field
index	String	Name of the masked field

Status code: 400

Table 4-141 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-142 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-143 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.13 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 4-144 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.
rule_id	Yes	String	privacyRuleId

Request Parameters

Table 4-145 Request header parameters

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

Response Parameters

Status code: 400

Table 4-146 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-147 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-148 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.14 Querying the Geolocation Access Control Rule List

Function

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

URI

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

Table 4-149 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Table 4-150 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number Default: **1**
pagesize	No	Integer	Number of records on each page Default: **10**

Request Parameters

Table 4-151 Request header parameters

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

Response Parameters

Status code: 200

Table 4-152 Response body parameters

Parameter	Type	Description
total	Integer	Number of blocked locations in the geolocation access control rules
items	Array of objects	List of the blocked locations in the geolocation access control rules

Table 4-153 items

Parameter	Type	Description
id	String	Rule ID
geoip	String	Blocked locations in the geolocation access control rules
white	Integer	Protective action for the rule. You can configure Allow or Block action.
timestamp	Long	Time the rule was created

Status code: 400

Table 4-154 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-155 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-156 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.15 Creating a Geolocation Access Control Rule

Function

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

URI

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

Table 4-157 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Request Parameters

Table 4-158 Request header parameters

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

Table 4-159 Request body parameters

Parameter	Mandatory	Type	Description
geoip	No	String	Blocked locations in the geolocation access control rules
white	No	Integer	Protective action for the rule. The options are 0 and 1. 0: Block. 1: Allow.
description	No	String	Time the rule was created

Response Parameters

Status code: 200

Table 4-160 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID

Parameter	Type	Description
geoip	String	Blocked locations in the geolocation access control rules
white	Integer	Protective action for the rule. The options are 0 and 1. 0: Block. 1: Allow.
timestamp	Long	Time the rule was created

Status code: 400

Table 4-161 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-162 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-163 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.16 Updating a Geolocation Access Control Rule

Function

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

URI

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

Table 4-164 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.
rule_id	Yes	String	geoipRuleId

Request Parameters

Table 4-165 Request header parameters

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

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

Table 4-166 Request body parameters

Parameter	Mandatory	Type	Description
geoip	Yes	String	Location
white	No	Integer	Protective action for the rule. The options are 0 and 1. 0: Allow. 1: Block.

Response Parameters

Status code: 200

Table 4-167 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
geoip	String	Blocked locations in the geolocation access control rules
white	Integer	Protective action for the rule. The options are 0 and 1. 0: Block. 1: Allow.

Status code: 400

Table 4-168 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-169 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-170 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.17 Deleting a Geolocation Access Control Rule

Function

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

URI

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

Table 4-171 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.
rule_id	Yes	String	geoipRuleId

Request Parameters

Table 4-172 Request header parameters

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

Response Parameters

Status code: 200

Table 4-173 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
geoip	String	Blocked locations in the geolocation access control rules
white	Integer	Protective action for the rule. The options are 0 and 1. 0: Block. 1: Allow.
description	String	Description

Parameter	Type	Description
timestamp	Long	Time stamp when the rule was created

Status code: 400

Table 4-174 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-175 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-176 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.18 Querying the List of Web Tamper Protection Rules

Function

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

URI

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

Table 4-177 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Table 4-178 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number
pagesize	No	Integer	Number of records on each page

Request Parameters

Table 4-179 Request header parameters

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

Response Parameters

Status code: 200

Table 4-180 Response body parameters

Parameter	Type	Description
total	Integer	Number of the web tamper protection rules
items	Array of **AntiTamperRuleResponseBody** objects	Rule

Table 4-181 AntiTamperRuleResponseBody

Parameter	Type	Description
id	String	Rule ID
hostname	String	Protected domain names for the web tamper protection rule
url	String	URLs for the web tamper protection rule
description	String	Time the rule was created

Status code: 400

Table 4-182 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-183 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-184 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.19 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 4-185 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.

Request Parameters

Table 4-186 Request header parameters

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

Table 4-187 Request body parameters

Parameter	Mandatory	Type	Description
hostname	No	String	Protected website. Query the protected domain name list in cloud mode to obtain the protected domain name, which is in the hostname field in the response body.

Parameter	Mandatory	Type	Description
url	No	String	URLs for the web tamper protection rule
description	No	String	Rule description

Response Parameters

Status code: 200

Table 4-188 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
hostname	String	Protected domain names for the web tamper protection rule
url	String	URLs for the web tamper protection rule
description	String	Time the rule was created
status	Integer	Rule status

Status code: 400

Table 4-189 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-190 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-191 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.20 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 4-192 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.
rule_id	Yes	String	antitamperRuleId

Request Parameters

Table 4-193 Request header parameters

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

Response Parameters

Status code: 200

Table 4-194 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
url	String	URLs for the web tamper protection rule
timestamp	Long	Time the rule was created

Status code: 400

Table 4-195 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-196 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-197 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.2.21 Changing the Status of a Rule

Function

This API is used to query details about sensitive information options.

URI

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

Table 4-198 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
policy_id	Yes	String	Policy ID. It can be obtained by calling the API for querying the policy list.
ruletype	Yes	String	Policy type
rule_id	Yes	String	Rule ID. It can be obtained by calling a specific API for querying the lists of the corresponding type of rule.

Request Parameters

Table 4-199 Request header parameters

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

Table 4-200 Request body parameters

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

Response Parameters

Status code: 400

Table 4-201 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-202 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-203 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed

Status Code	Description
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.3 Certificate Management

4.3.1 Querying the List of Certificates

Function

This API is used to query the list of certificates.

URI

GET /v1/{project_id}/waf/certificate

Table 4-204 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-205 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number Default: **1**
pagesize	No	Integer	Number of records on each page. Default: **10**
name	No	String	Certificate name
host	No	Boolean	Whether to obtain the Domain name the certificate is applied to Default: **false**

Parameter	Mandatory	Type	Description
exp_status	No	Integer	Certificate status. The options are 0, 1, and 2. 0: The certificate does not expire. 1: The certificate has expired. 2: The certificate is about to expire.

Request Parameters

Table 4-206 Request header parameters

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

Response Parameters

Status code: 200

Table 4-207 Response body parameters

Parameter	Type	Description
items	Array of **CertificateBody** objects	Certificate list
total	Integer	Number of certificates

Table 4-208 CertificateBody

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
content	String	Certificate file, in PEM format

Parameter	Type	Description
key	String	Certificate private key (in PEM format)
expire_time	Long	Certificate expiration Time stamp
exp_status	Integer	Certificate status. The options are 0, 1, and 2. 0: The certificate does not expire. 1: The certificate has expired. 2: The certificate is about to expire.
timestamp	Long	Time the certificate was uploaded
bind_host	Array of **BindHost** objects	Domain name the certificate is applied to

Table 4-209 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF edition for the domain name. The options are cloud and premium.
mode	String	(Dedicated mode only) Special domain name mode

Status code: 400

Table 4-210 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-211 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-212 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.3.2 Creating a Certificate

Function

This API is used to create a certificate.

URI

POST /v1/{project_id}/waf/certificate

Table 4-213 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-214 Request header parameters

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

Table 4-215 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Certificate name
content	No	String	Certificate file, in PEM format
key	No	String	Certificate private key (in PEM format)

Response Parameters

Status code: 200

Table 4-216 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
content	String	Certificate file, in PEM format
key	String	Certificate private key (in PEM format)
expire_time	Long	Certificate expiration timestamp

Parameter	Type	Description
exp_status	Integer	Certificate status. The options are 0, 1, and 2. 0: The certificate does not expire. 1: The certificate has expired. 2: The certificate is about to expire.
timestamp	Long	Time the certificate was uploaded
bind_host	Array of **BindHost** objects	Domain name the certificate is applied to

Table 4-217 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF edition for the domain name. The options are cloud and premium.
mode	String	(Dedicated mode only) Special domain name mode

Status code: 400

Table 4-218 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-219 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-220 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

```
{
  "name" : "test",
  "content" : "-----BEGIN CERTIFICATE-----
MIIDIjCCAougAwIBAgIJALV96mEtVF4EMA0GCSqGSIb3DQEBBQUAMGoxCzAJBgNVBAYTAnh4MQswCQYDVQ
QIEwJ4eDELMAkGA1UEBxMCeHgxCzAJBgNVBAoTAnh4MQswCQYDVQQLEwJ -----END CERTIFICATE-----",
  "key" : "-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDFPN9ojPndxSC4E1pqWQVKGHCFlXAAGBOxbGfSzXqzsoyacotueqMqXQbxrPSQFATeVmhZ
PNVEMdvcAMjYsV/mymtAwVqVA6q/OFdX/b3UHO+b/VqLo3J5SrM -----END RSA PRIVATE KEY-----"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.3.3 Querying a Certificate

Function

This API is used to query a certificate.

URI

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

Table 4-221 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
certificate_id	Yes	String	Certificate ID

Request Parameters

Table 4-222 Request header parameters

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

Response Parameters

Status code: 200

Table 4-223 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
content	String	Certificate file, in PEM format
key	String	Certificate private key (in PEM format)
expire_time	Long	Certificate expiration timestamp
exp_status	Integer	Certificate status. The options are 0, 1, and 2. 0: The certificate does not expire. 1: The certificate has expired. 2: The certificate is about to expire.
timestamp	Long	Time the certificate was uploaded
bind_host	Array of **BindHost** objects	Domain name the certificate is applied to

Table 4-224 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF edition for the domain name. The options are cloud and premium.
mode	String	(Dedicated mode only) Special domain name mode

Status code: 400

Table 4-225 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-226 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-227 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.3.4 Deleting a Certificate

Function

This API is used to delete a certificate.

URI

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

Table 4-228 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
certificate_id	Yes	String	Certificate ID

Request Parameters

Table 4-229 Request header parameters

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

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

Response Parameters

Status code: 200

Table 4-230 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
content	String	Certificate file, in PEM format
key	String	Certificate private key (in PEM format)
expire_time	Long	Certificate expiration timestamp
exp_status	Integer	Certificate status. The options are 0, 1, and 2. 0: The certificate does not expire. 1: The certificate has expired. 2: The certificate is about to expire.
timestamp	Long	Time the certificate was uploaded
bind_host	Array of **BindHost** objects	Domain name the certificate is applied to

Table 4-231 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF edition for the domain name. The options are cloud and premium.
mode	String	(Dedicated mode only) Special domain name mode

Status code: 400

Table 4-232 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-233 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-234 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.3.5 Modifying a Certificate

Function

This API is used to modify a certificate.

URI

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

Table 4-235 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
certificate_id	Yes	String	Certificate ID

Request Parameters

Table 4-236 Request header parameters

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

Table 4-237 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Certificate name

Response Parameters

Status code: 200

Table 4-238 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
expire_time	Long	Certificate expiration timestamp
timestamp	Long	Time stamp

Status code: 400

Table 4-239 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-240 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-241 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

```
{
  "name" : "test_cert",
  "content" : "-----BEGIN CERTIFICATE-----
\nMIIDIjCCAougAwIBAgIJALV96mEtVF4EMA0GCSqGSIb3DQEBBQUAMGoxCzAJBgNVBAYTAnh4MQswCQYDV
QQIEwJ4eDELMAkGA1UEBxMCeHgxCzAJBgNVBAoTAnh4MQswCQYDVQQLEwJ\n-----END
CERTIFICATE-----",
  "key" : "-----BEGIN RSA PRIVATE KEY-----
\nMIICXQIBAAKBgQDFPN9ojPndxSC4E1pqWQVKGHCFlXAAGBOxbGfSzXqzsoyacotueqMqXQbxrPSQFATeVmh
ZPNVEMdvcAMjYsV/mymtAwVqVA6q/OFdX/b3UHO+b/VqLo3J5SrM\n-----END RSA PRIVATE KEY-----"
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.4 Event Management

4.4.1 This API is used to query the list of events.

Function

Querying the List of Events

URI

GET /v1/{project_id}/waf/event

Table 4-242 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-243 Query parameters

Parameter	Mandatory	Type	Description
recent	Yes	String	Log query time range

Parameter	Mandatory	Type	Description
hosts	No	Array	Domain name ID. It can be obtained from the protected website list.
page	No	Integer	Page number
pagesize	No	Integer	Number of records per page

Request Parameters

Table 4-244 Request header parameters

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

Response Parameters

Status code: 200

Table 4-245 Response body parameters

Parameter	Type	Description
total	Integer	Number of attack events
items	Array of **ListEventItems** objects	Details about an attack event

Table 4-246 ListEventItems

Parameter	Type	Description
id	String	Event ID
time	Long	Count
policyid	String	Policy ID

Parameter	Type	Description
sip	String	Source IP address
host	String	Domain name
url	String	Attacked URL
attack	String	Attack type XSS attacks: xss or sqli Command injection: cmdi Malicious crawlers: robot Local file inclusion: lfi Remote file inclusion: rfi Website Trojans: webshell CC attack: cc Precise protection: custom_custom IP address blacklist and whitelist: custom_whiteblackip Geolocation access control: custom_geoip Anti-tamper protection: antitamper Anti-crawler protection: anticrawler Data leakage prevention: leakage Illegal requests: illegal Other attack types: vuln
rule	String	ID of the matched rule
payload	String	Hit payload
action	String	Protective action
request_line	String	Request method and path
headers	**headers** object	Request header
cookie	String	Request cookie
status	String	Response code status
region	String	Region
host_id	String	Domain name ID
response_time	Long	Time to response
response_size	Integer	Response body size
response_body	String	Response body

Table 4-247 headers

Parameter	Type	Description
content-length	String	Request length
host	String	Domain name
content-type	String	Content type

Parameter	Type	Description
user-agent	String	Proxy
accept	String	Type of the received content

Status code: 400

Table 4-248 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-249 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-250 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	ok
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.4.2 This API is used to query details of an event.

Function

Querying Details of an Event

URI

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

Table 4-251 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
eventid	Yes	String	Event ID

Request Parameters

Table 4-252 Request header parameters

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

Response Parameters

Status code: 200

Table 4-253 Response body parameters

Parameter	Type	Description
total	Integer	Number of attack events
items	Array of **ShowEventItems** objects	Details about an attack event

Table 4-254 ShowEventItems

Parameter	Type	Description
time	Long	Count
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
payload	String	Hit payload
action	String	Protective action
timestamp	Long	Timestamp

Status code: 400

Table 4-255 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-256 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-257 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	ok
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.5 Protected Website Management in Dedicated Mode

4.5.1 Connecting a Domain Name to a Dedicated WAF Instance

Function

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

URI

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

Table 4-258 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-259 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 4-260 Request body parameters

Parameter	Mandatory	Type	Description
certificateid	No	String	Certificate ID
certificatename	No	String	Certificate name
hostname	Yes	String	Domain name or IP address (or IP address with port)
proxy	No	Boolean	Whether a proxy is used
policyid	No	String	ID of the policy initially applied to the protected domain name
server	No	Array of **PremiumWaf Server** objects	Configuration of retrieval server in dedicated mode

Table 4-261 PremiumWafServer

Parameter	Mandatory	Type	Description
front_protocol	Yes	String	Client protocol
back_protocol	Yes	String	Server protocol
address	Yes	String	Server address
port	Yes	Integer	Server port
type	No	String	Origin server IP address format. Default: **ipv4**
vpc_id	No	String	ID of the VPC where the dedicated WAF engine resides. The origin server and the dedicated WAF engine must be in the same subnet.

Response Parameters

Status code: 200

Table 4-262 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
policyid	String	Policy ID
hostname	String	Policy ID
domainid	String	Tenant ID
projectid	String	Project ID
protocol	String	HTTP protocol

Status code: 400

Table 4-263 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-264 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-265 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

```
{
  "hostname" : "www.test.com",
  "server" : [ {
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP",
    "vpc_id" : "34e414f6-2407-456b-b61d-93d64e9e56f0",
    "type" : "ipv4",
    "address" : "1.1.1.1",
    "port" : 80
  } ],
  "proxy" : true
}
```

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Invalid request
401	Unauthorized token
500	Internal server error

Error Codes

See **Error Codes**.

4.5.2 Querying the List of Domain Names Connected to Dedicated WAF Instances

Function

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

URI

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

Table 4-266 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-267 Query parameters

Parameter	Mandatory	Type	Description
page	No	String	Page number Default: **1**
pagesize	No	String	Number of records on each page. Default: **10**
hostname	No	String	Domain name
policyname	No	String	Policy Name
protect_status	No	Integer	Protection status of the domain name

Request Parameters

Table 4-268 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).

Response Parameters

Status code: 200

Table 4-269 Response body parameters

Parameter	Type	Description
total	Integer	Number of all protected domain names
items	Array of **SimplePremiumWafHost** objects	Details about the protected domain name

Table 4-270 SimplePremiumWafHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
policyid	String	Policy ID
protect_status	Integer	Protection status
access_status	Integer	Access status
flag	Map<String,String>	Special identifier
mode	String	Dedicated engine identifier in special mode, for example, the ELB mode.
pool_ids	Array of strings	Dedicated engine group to which the domain name in special mode belongs

Status code: 400

Table 4-271 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-272 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-273 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Invalid request
401	Unauthorized token
500	Internal server error

Error Codes

See **Error Codes**.

4.5.3 Modifying the Configuration of a Domain Name Connected to a Dedicated WAF Instance

Function

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

URI

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

Table 4-274 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
host_id	Yes	String	ID of a domain name connected to a dedicated WAF instance

Request Parameters

Table 4-275 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 4-276 Request body parameters

Parameter	Mandatory	Type	Description
proxy	No	Boolean	Whether a proxy is used
certificateid	No	String	Certificate ID
certificatename	No	String	Certificate name
tls	No	String	Minimum TLS version

Parameter	Mandatory	Type	Description
cipher	No	String	Cipher suite code

Response Parameters

Status code: 200

Table 4-277 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
policyid	String	Policy ID
hostname	String	Domain name connected to a cloud WAF instance
domainid	String	ID of the protected domain name
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	Certificate ID
certificatename	String	Certificate
tls	String	Minimum TLS version
cipher	String	Cipher suite code
proxy	Boolean	Whether the proxy is enabled
locked	Integer	Locked state Default: **0**
protect_status	Integer	Protection status
access_status	Integer	Access status
timestamp	Long	Time the domain name was connected to WAF
block_page	**BlockPage** object	Alarm page
extend	Map<String,String>	Extensible attribute

Parameter	Type	Description
traffic_mark	**TrafficMark** object	Traffic identifier (for known attack source rule only)
flag	Map<String,String>	Special domain name tag
mode	String	Special domain name for the dedicated mode (required in special mode, for example, the ELB mode)
pool_ids	Array of strings	ID of the group associated with the domain name (required only in special mode, for example, the ELB mode)

Table 4-278 PremiumWafServer

Parameter	Type	Description
front_protocol	String	Client protocol
back_protocol	String	Server protocol
address	String	Server address
port	Integer	Server port
type	String	Origin server IP address format. Default: **ipv4**
vpc_id	String	ID of the VPC where the dedicated WAF engine resides. The origin server and the dedicated WAF engine must be in the same subnet.

Table 4-279 BlockPage

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

Table 4-280 CustomPage

Parameter	Type	Description
status_code	String	Returned status code
content_type	String	Page content type
content	String	Page content

Table 4-281 TrafficMark

Parameter	Type	Description
sip	Array of strings	IP address of the known attack source
cookie	String	cookie
params	String	Parameter

Status code: 400

Table 4-282 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-283 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-284 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Invalid request
401	Unauthorized token
500	Internal server error

Error Codes

See **Error Codes**.

4.5.4 Querying the Domain Name Configuration in Dedicated Mode

Function

This API is used to query the domain name configuration in dedicated mode.

URI

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

Table 4-285 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
host_id	Yes	String	ID of a domain name connected to a dedicated WAF instance

Request Parameters

Table 4-286 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).

Response Parameters

Status code: 200

Table 4-287 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
policyid	String	Policy ID
hostname	String	Domain name connected to a cloud WAF instance
domainid	String	ID of the protected domain name
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	Certificate ID
certificatename	String	Certificate
tls	String	Minimum TLS version
cipher	String	Cipher suite code
proxy	Boolean	Whether the proxy is enabled
locked	Integer	Locked state Default: **0**
protect_status	Integer	Protection status
access_status	Integer	Access status

Parameter	Type	Description
timestamp	Long	Time the domain name was connected to WAF
block_page	**BlockPage** object	Alarm page
extend	Map<String,String>	Extensible attribute
traffic_mark	**TrafficMark** object	Traffic identifier (for known attack source rule only)
flag	Map<String,String>	Special domain name tag
mode	String	Special domain name for the dedicated mode (required in special mode, for example, the ELB mode)
pool_ids	Array of strings	ID of the group associated with the domain name (required only in special mode, for example, the ELB mode)

Table 4-288 PremiumWafServer

Parameter	Type	Description
front_protocol	String	Client protocol
back_protocol	String	Server protocol
address	String	Server address
port	Integer	Server port
type	String	Origin server IP address format. Default: **ipv4**
vpc_id	String	ID of the VPC where the dedicated WAF engine resides. The origin server and the dedicated WAF engine must be in the same subnet.

Table 4-289 BlockPage

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

Table 4-290 CustomPage

Parameter	Type	Description
status_code	String	Returned status code
content_type	String	Page content type
content	String	Page content

Table 4-291 TrafficMark

Parameter	Type	Description
sip	Array of strings	IP address of the known attack source
cookie	String	cookie
params	String	Parameter

Status code: 400

Table 4-292 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-293 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-294 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Invalid request
401	Unauthorized token
500	Internal server error

Error Codes

See **Error Codes**.

4.5.5 Deleting a Domain Name from a Dedicated WAF Instance

Function

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

URI

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

Table 4-295 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
host_id	Yes	String	ID of a domain name connected to a dedicated WAF instance

Table 4-296 Query parameters

Parameter	Mandatory	Type	Description
keepPolicy	No	Boolean	Whether to retain the rules Default: **1**

Request Parameters

Table 4-297 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).

Response Parameters

Status code: 200

Table 4-298 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
policyid	String	Policy ID
protect_status	Integer	Protection status
access_status	Integer	Access status
flag	Map<String,String>	Special identifier
mode	String	Dedicated engine identifier in special mode, for example, the ELB mode.
pool_ids	Array of strings	Dedicated engine group to which the domain name in special mode belongs

Status code: 400

Table 4-299 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-300 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-301 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Invalid request
401	Unauthorized token
500	Internal server error

Error Codes

See **Error Codes**.

4.5.6 Modifying the Protection Status of a Domain Name Connected to a Dedicated WAF Instance

Function

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

URI

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

Table 4-302 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
host_id	Yes	String	ID of a domain name connected to a dedicated WAF instance

Request Parameters

Table 4-303 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 4-304 Request body parameters

Parameter	Mandatory	Type	Description
protect_status	No	Integer	Protection status

Response Parameters

Status code: 200

Table 4-305 Response body parameters

Parameter	Type	Description
protect_status	Integer	Protection status

Status code: 400

Table 4-306 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-307 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-308 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Invalid request
401	Unauthorized token
500	Internal server error

Error Codes

See **Error Codes**.

4.6 Dashboard

4.6.1 Querying Statistics on WAF Dashboard

Function

Querying Statistics on WAF Dashboard

URI

GET /v1/{project_id}/waf/overviews/statistics

Table 4-309 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-310 Query parameters

Parameter	Mandatory	Type	Description
from	Yes	Long	Start time
to	Yes	Long	End time
hosts	No	String	List of the domain names to query
instances	No	String	List of instances to query

Request Parameters

Table 4-311 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token
Content-Type	Yes	String	Content type Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-312 Response body parameters

Parameter	Type	Description
[items]	Array of **CountItem** objects	Security statistics

Table 4-313 CountItem

Parameter	Type	Description
key	String	Type
num	Integer	Quantity

Status code: 400

Table 4-314 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-315 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-316 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

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

Error Codes

See **Error Codes**.

4.6.2 Querying the QPS Statistics

Function

Querying the QPS Statistics

URI

GET /v1/{project_id}/waf/overviews/qps/timeline

Table 4-317 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-318 Query parameters

Parameter	Mandatory	Type	Description
from	Yes	Long	Start time, which is a 13-digit timestamp in millisecond
to	Yes	Long	End time, which is a 13-digit timestamp in millisecond
hosts	No	String	Domain name ID, which can be obtained by calling the ListHost API
instances	No	String	ID of the dedicated WAF instance. This parameter is required only in instantiation mode.
group_by	No	String	Display dimension. For example, the value is DAY if data is displayed by the day.

Request Parameters

Table 4-319 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token
Content-Type	Yes	String	Content type Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-320 Response body parameters

Parameter	Type	Description
[items]	Array of **StatisticsTimelineItem** objects	Timeline of security statistics

Table 4-321 StatisticsTimelineItem

Parameter	Type	Description
key	String	Key value
timeline	Array of **TimeLineItem** objects	Timeline corresponding to the key value

Table 4-322 TimeLineItem

Parameter	Type	Description
time	Long	Time
num	Integer	Quantity

Status code: 400

Table 4-323 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-324 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-325 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

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**.

4.7 Querying the Protected Domain Names

4.7.1 Querying the List of Protection Domain Names

Function

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

URI

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

Table 4-326 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-327 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	page Default: **1**
pagesize	No	Integer	Number of records on each page. Default: **10**
hostname	No	String	Domain name
policyname	No	String	Policy name
protect_status	No	Integer	Protection status of the domain name
waf_type	No	String	WAF mode for the domain name
is_https	No	Boolean	Whether HTTPS is used for the domain name

Request Parameters

Table 4-328 Request header parameters

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

Response Parameters

Status code: 200

Table 4-329 Response body parameters

Parameter	Type	Description
total	Integer	Number of all protected domain names
cloud_total	Integer	Number of domain names protected with the cloud WAF instance
premium_total	Integer	Number of domain names protected with the dedicated WAF instances
items	Array of **CompositeHostResponse** objects	Details about the protected domain name

Table 4-330 CompositeHostResponse

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name connected to a cloud WAF instance
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	Protection status
access_status	Integer	Access status
proxy	Boolean	Whether the proxy is enabled
timestamp	Long	Time the domain name was connected to WAF
paid_type	String	Billing mode
flag	**HostFlag** object	Domain name configuration
waf_type	String	WAF mode of the domain name

Table 4-331 HostFlag

Parameter	Type	Description
pci_dss	String	true/false
pci_3ds	String	true/false
cname	String	old/new

Parameter	Type	Description
is_dual_az	String	true/false
ipv6	String	true/false

Status code: 400

Table 4-332 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-333 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-334 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.7.2 Querying a Protected Domain Name by ID

Function

This API is used to query a protected domain name by ID.

URI

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

Table 4-335 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
host_id	Yes	String	Domain name ID

Request Parameters

Table 4-336 Request header parameters

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

Response Parameters

Status code: 200

Table 4-337 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name connected to a cloud WAF instance
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	Protection status
access_status	Integer	Access status
proxy	Boolean	Whether the proxy is enabled
timestamp	Long	Time the domain name was connected to WAF
paid_type	String	Billing mode
flag	**HostFlag** object	Domain name configuration
waf_type	String	WAF mode of the domain name

Table 4-338 HostFlag

Parameter	Type	Description
pci_dss	String	true/false
pci_3ds	String	true/false
cname	String	old/new
is_dual_az	String	true/false
ipv6	String	true/false

Status code: 400

Table 4-339 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error code message

Status code: 401

Table 4-340 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-341 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

Status Code	Description
200	OK
400	Request failed
401	Insufficient token permissions
500	Internal server error

Error Codes

See **Error Codes**.

4.8 Querying Features Available in a Site

4.8.1 Querying Features Available in a Site

Function

This API is used to query features available for a certain site.

URI

GET /v1/{project_id}/waf/config/console

Table 4-342 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-343 Request header parameters

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

Response Parameters

Status code: 200

Table 4-344 Response body parameters

Parameter	Type	Description
eps	Boolean	Support for EPS

Parameter	Type	Description
tls	Boolean	Support for TLS
ipv6	Boolean	Support for IPv6
alert	Boolean	Support for alarms
custom	Boolean	Support for precise protection
elb_mode	Boolean	Support for load-balancing WAF instances
event_lts	Boolean	Support for LTS for WAF logging
multi_dns	Boolean	Support for multi-DNS resolution
search_ip	Boolean	Support for searching for IP addresses
cc_enhance	Boolean	Support for CC attack protection enhancement
cname_switch	Boolean	Support for CNAME record switchover
custom_block	Boolean	Support for precise block
advanced_ignore	Boolean	Support for false alarm masking
js_crawler_enable	Boolean	Support for JavaScript anti-crawler
deep_decode_enable	Boolean	Support for in-depth parsing
overview_bandwidth	Boolean	Support for bandwidth statistics
proxy_use_oldcname	Boolean	Support for DNS resolution with the old CNAME record
check_all_headers_enable	Boolean	Support for inspection of all headers

Status code: 400

Table 4-345 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-346 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-347 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

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**.

4.9 Managing Websites Protected by Cloud WAF

4.9.1 Querying Domain Names Protected by Cloud WAF

Function

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

URI

GET /v1/{project_id}/waf/instance

Table 4-348 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-349 Query parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number Default: **1**
pagesize	No	Integer	Number of records on each page Default: **10**
hostname	No	String	Domain name
policyname	No	String	Policy name

Request Parameters

Table 4-350 Request header parameters

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

Response Parameters

Status code: 200

Table 4-351 Response body parameters

Parameter	Type	Description
total	Integer	Number of domain names protected with the cloud WAF instance
items	Array of **CloudWafHostResponseBody** objects	Details about the protected domain name

Table 4-352 CloudWafHostResponseBody

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name connected to a cloud WAF instance
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	Protection status
access_status	Integer	Access status
protocol	String	Returned client protocol type
certificateid	String	Certificate ID
certificatename	String	Certificate name
server	Array of **CloudWafServer** objects	Origin server details
proxy	Boolean	Whether the proxy is enabled
timestamp	Long	Time the domain name was connected to WAF
exclusive_ip	Boolean	Whether a dedicated IP address is used

Table 4-353 CloudWafServer

Parameter	Type	Description
front_protocol	String	Client protocol
back_protocol	String	Server protocol
address	String	Server address
port	Integer	Server port
type	String	Origin server IP address format. Default: **ipv4**

Status code: 400

Table 4-354 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-355 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-356 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

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**.

4.9.2 Adding a Domain Name to Cloud WAF

Function

This API is used to add a domain name to cloud WAF.

URI

POST /v1/{project_id}/waf/instance

Table 4-357 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-358 Request header parameters

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

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

Table 4-359 Request body parameters

Parameter	Mandatory	Type	Description
hostname	No	String	Domain name
policyid	No	String	ID of the policy initially applied to the protected domain name
server	No	Array of **CloudWafServer** objects	Origin server details
certificateid	No	String	Certificate ID
certificatename	No	String	Certificate name
proxy	No	Boolean	Whether a proxy is used
description	No	String	Domain name description

Table 4-360 CloudWafServer

Parameter	Mandatory	Type	Description
front_protocol	Yes	String	Client protocol
back_protocol	Yes	String	Server protocol
address	Yes	String	Server address
port	Yes	Integer	Server port
type	No	String	Origin server IP address format. Default: **ipv4**

Response Parameters

Status code: 200

Table 4-361 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name connected to a cloud WAF instance
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	Protection status
access_status	Integer	Access status
protocol	String	Returned client protocol type
certificateid	String	Certificate ID
certificatename	String	Certificate name
server	Array of **CloudWafServer** objects	Origin server details
proxy	Boolean	Whether the proxy is enabled
timestamp	Long	Time the domain name was connected to WAF
exclusive_ip	Boolean	Whether a dedicated IP address is used

Table 4-362 CloudWafServer

Parameter	Type	Description
front_protocol	String	Client protocol
back_protocol	String	Server protocol
address	String	Server address
port	Integer	Server port
type	String	Origin server IP address format. Default: **ipv4**

Status code: 400

Table 4-363 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-364 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-365 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

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**.

4.9.3 Modifying the Protection Status for a Domain Name

Function

This API is used to obtain the domain name route information.

URI

PUT /v1/{project_id}/waf/instance/{instance_id}/protect-status

Table 4-366 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
instance_id	Yes	String	Domain name ID, which can be obtained by querying the domain names protected by cloud WAF.

Request Parameters

Table 4-367 Request header parameters

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

Table 4-368 Request body parameters

Parameter	Mandatory	Type	Description
protect_status	No	Integer	Protection status. The options are -1, 0, and 1. -1: Bypassed. 0: Suspended. 1: Enabled.

Response Parameters

Status code: 400

Table 4-369 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-370 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-371 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

```
{
  "protect_status" : 0
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.

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

Error Codes

See **Error Codes**.

4.9.4 Obtaining Domain Name Route Information in Cloud Mode

Function

This API is used to obtain the domain name route information.

URI

GET /v1/{project_id}/waf/instance/{instance_id}/route

Table 4-372 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
instance_id	Yes	String	Domain name ID

Request Parameters

Table 4-373 Request header parameters

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

Response Parameters

Status code: 200

Table 4-374 Response body parameters

Parameter	Type	Description
total	Integer	Quantity
items	Array of **RouteBody** objects	Route information body

Table 4-375 RouteBody

Parameter	Type	Description
name	String	Name
servers	Array of **RouteServerBody** objects	Route information

Table 4-376 RouteServerBody

Parameter	Type	Description
back_protocol	String	Protocol
address	String	IP address
port	Integer	Port

Status code: 400

Table 4-377 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-378 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-379 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

Example Responses

None

Status Codes

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

Error Codes

See **Error Codes**.

4.9.5 Querying a Domain Name Protected by Cloud WAF by ID

Function

This API is used to query a domain name protected by cloud WAF by ID.

URI

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

Table 4-380 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
instance_id	Yes	String	Domain name ID

Request Parameters

Table 4-381 Request header parameters

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

Response Parameters

Status code: 200

Table 4-382 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name connected to a cloud WAF instance
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	Protection status
access_status	Integer	Access status
protocol	String	Returned client protocol type
certificateid	String	Certificate ID

Parameter	Type	Description
certificatename	String	Certificate name
server	Array of **CloudWafServer** objects	Origin server details
proxy	Boolean	Whether the proxy is enabled
timestamp	Long	Time the domain name was connected to WAF
exclusive_ip	Boolean	Whether a dedicated IP address is used

Table 4-383 CloudWafServer

Parameter	Type	Description
front_protocol	String	Client protocol
back_protocol	String	Server protocol
address	String	Server address
port	Integer	Server port
type	String	Origin server IP address format. Default: **ipv4**

Status code: 400

Table 4-384 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-385 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-386 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

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**.

4.9.6 Updating a Domain Name Protected by Cloud WAF

Function

This API is used to update a domain name protected by cloud WAF.

URI

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

Table 4-387 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Parameter	Mandatory	Type	Description
instance_id	Yes	String	Domain name ID

Request Parameters

Table 4-388 Request header parameters

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

Table 4-389 Request body parameters

Parameter	Mandatory	Type	Description
proxy	No	Boolean	Whether a proxy is used
certificateid	No	String	Certificate ID
certificatename	No	String	Certificate name
server	No	Array of **PremiumWafServer** objects	Configuration of retrieval server in dedicated mode
tls	No	String	Minimum TLS version. The options are TLS v1.0, TLS v1.1, and TLS v1.2.
cipher	No	String	Cipher suite code. The options are cipher_default, cipher_1, and cipher_2.

Table 4-390 PremiumWafServer

Parameter	Mandatory	Type	Description
front_protocol	Yes	String	Client protocol
back_protocol	Yes	String	Server protocol

Parameter	Mandatory	Type	Description
address	Yes	String	Server address
port	Yes	Integer	Server port
type	No	String	Origin server IP address format. Default: **ipv4**
vpc_id	No	String	ID of the VPC where the dedicated WAF engine resides. The origin server and the dedicated WAF engine must be in the same subnet.

Response Parameters

Status code: 200

Table 4-391 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name connected to a cloud WAF instance
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	Protection status
access_status	Integer	Access status
protocol	String	Returned client protocol type
certificateid	String	Certificate ID
certificatename	String	Certificate name
server	Array of **CloudWafServer** objects	Origin server details
proxy	Boolean	Whether the proxy is enabled
timestamp	Long	Time the domain name was connected to WAF
exclusive_ip	Boolean	Whether a dedicated IP address is used

Table 4-392 CloudWafServer

Parameter	Type	Description
front_protocol	String	Client protocol
back_protocol	String	Server protocol
address	String	Server address
port	Integer	Server port
type	String	Origin server IP address format. Default: **ipv4**

Status code: 400

Table 4-393 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-394 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-395 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

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**.

4.9.7 Removing a Domain Name from Cloud WAF

Function

This API is used to remove a domain name from cloud WAF.

URI

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

Table 4-396 Path parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
instance_id	Yes	String	Domain name ID

Request Parameters

Table 4-397 Request header parameters

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

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

Response Parameters

Status code: 200

Table 4-398 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name connected to a cloud WAF instance
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	Protection status
access_status	Integer	Access status
protocol	String	Returned client protocol type
certificateid	String	Certificate ID
certificatename	String	Certificate name
server	Array of **CloudWafServer** objects	Origin server details
proxy	Boolean	Whether the proxy is enabled
timestamp	Long	Time the domain name was connected to WAF
exclusive_ip	Boolean	Whether a dedicated IP address is used

Table 4-399 CloudWafServer

Parameter	Type	Description
front_protocol	String	Client protocol
back_protocol	String	Server protocol
address	String	Server address

Parameter	Type	Description
port	Integer	Server port
type	String	Origin server IP address format. Default: **ipv4**

Status code: 400

Table 4-400 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 401

Table 4-401 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Status code: 500

Table 4-402 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error code message

Example Requests

None

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**.

A Appendix

A.1 Status Code

- Normal

Returned Value	Description
200	The request is successfully processed.

- Abnormal

Status Code	Status	Description
400	Bad Request	The server fails to process the request.
401	Unauthorized	The requested page requires a username and a password.
403	Forbidden	Access to the requested page is denied.
404	Not Found	The server fails to find the requested page.
405	Method Not Allowed	Method specified in the request is not allowed.
406	Not Acceptable	Response generated by the server is not acceptable to the client.
407	Proxy Authentication Required	Proxy authentication is required before the request is processed.
408	Request Timeout	A timeout error occurs because the request is not processed within the specified waiting period of the server.

Status Code	Status	Description
409	Conflict	The request cannot be processed due to a conflict.
500	Internal Server Error	The request is not processed due to a server error.
501	Not Implemented	The request is not processed because the server does not support the requested function.
502	Bad Gateway	The request is not processed, and the server receives an invalid response from the upstream server.
503	Service Unavailable	The request is not processed due to a temporary system abnormality.
504	Gateway Timeout	A gateway timeout error occurs.

A.2 Error Codes

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00011001	bad.request	Bad request	Check param
400	WAF.00011002	url.param.illegal	The URL format is incorrect	Check URL format
400	WAF.00011003	request.body.illegal	Request body format error: missing parameter and illegal value in body	Check request body
400	WAF.00011004	id.illegal	Illegal ID	Check ID
400	WAF.00011005	name.illegal	Illegal name	Check name
400	WAF.00011006	host.illegal	Illegal domain name	Check domain name
400	WAF.00011007	port.illegal	Illegal port	Check port

Status Code	Error Codes	Error Message	Description	Solution
400	WAF. 00011007	ip.illegal	Illegal IP	Check IP
400	WAF. 00011008	protect.status. illegal	Illegal protection status	Check whether the protection state is in the range of enumeration value
400	WAF. 00011009	access.status.illegal	Illegal access status	Check whether the access status is in the range of enumeration value
400	WAF. 00011010	offsetOrLimit.illegal	Illegal offset or limit number	Check whether the starting line or limit number is within the range
400	WAF. 00011011	pageOrPageSize.illegal	Illegal page number or number of entries per page	Check if page number or number of items per page are in range
400	WAF. 00011012	standard.violated	Invalid parameter	Check the parameters
400	WAF. 00011013	description.illegal	Illegal description format	Check description format
400	WAF. 00011014	request.header.illegal	Request header format error: missing parameter and illegal value in header	Check header required parameters
400	WAF. 00011014	website.not.register	The website has not been put on record	Filing website
400	WAF. 00012001	invalid.token	Illegal token	Check whether the token is correct

Status Code	Error Codes	Error Message	Description	Solution
400	WAF. 00012002	invalid.project	Inconsistency between project_id and token	Check Consistency of project_id and token
400	WAF. 00012003	permission.denied	No permission	Assign WAF required permissions to account
400	WAF. 00012004	account.frozen	Account freezing	Account unfreezing
400	WAF. 00012005	not.subscribe	Unsubscribed	Subscribe to WAF service first
400	WAF. 00012006	pdp.permission.denied	No permission	Check the PDP authority of the account
400	WAF. 00012007	jwt.authentication.disabled	JWT certification off	Open JWT certification
400	WAF. 00012008	jwt.authentication.invalid.token	Illegal JWT token	Check whether the account has JWT permission
400	WAF. 00012009	jwt.authentication.failed	JWT authentication failed	Give the account authorization first
400	WAF. 00012010	eps.all.not.support	eps.all.not.support	Open the write permission of enterprise project
400	WAF. 00013001	insufficient.quota	Insufficient function quota	Purchase function quota upgrade package
400	WAF. 00013002	feature.not.support	Function not supported	nothing
400	WAF. 00013003	port.not.support	Port not supported	Port conversion via ELB
400	WAF. 00013004	protocol.not.support	Protocol not supported	Through ELB conversion protocol
400	WAF. 00013005	wildcard.domain.not.support	Pan domain name not supported	Use specific domain names

Status Code	Error Codes	Error Message	Description	Solution
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
400	WAF. 00014010	port.protocol.mismatch	Port and protocol mismatch	Select the matching protocol and port

Status Code	Error Codes	Error Message	Description	Solution
400	WAF. 00014011	host.blacklist	It is forbidden to add the protection website, and the domain name is blacklisted	
400	WAF. 00014012	insufficient.tenant.quota	Insufficient tenant quota	Purchase quota upgrade package
400	WAF. 00014013	exclusive.ip.config.error	Exclusive IP configuration error	Check exclusive IP configuration
400	WAF. 00014014	exclusive.ip.config.error	exclusive.ip.config.error	Check exclusive IP configuration
400	WAF. 00021002	url.param.illegal	The URL format is incorrect	It is recommended to modify the URL in the request body parameter to the standard URL and debug again
400	WAF. 00021003	request.body.illegal	The request body parameter is incorrect	It is recommended that you verify the parameters according to the document before initiating debugging
400	WAF. 00021004	id.illegal	The unique identifier ID format is incorrect	It is recommended to follow the correct instructions in the documentation to obtain the ID
400	WAF. 00021005	name.illegal	The name parameter format is incorrect	Check the format of name, which can only be composed of letters, numbers, -_ And. Cannot exceed 64 characters in length

Status Code	Error Codes	Error Message	Description	Solution
400	WAF. 00021006	host.illegal	The domain name format is incorrect	Domain name can only be composed of letters, numbers, -_ And. Cannot exceed 64 characters in length
400	WAF. 00021007	protocol.illegal	The back-end protocol format is incorrect	The back-end protocol can only be configured as HTTP or HTTPS and must be capitalized
400	WAF. 00021008	port.illegal	The source port format is incorrect	Check whether the configured port is empty and whether the target port is in the range of 0-65535
400	WAF. 00021009	ip.illegal	Incorrect IP format	Check whether the IP format meets the standard format of IPv4 or IPv6
400	WAF. 00021010	server.address.illegal	Server configuration exception	Check whether the server configuration is empty and whether the quantity is in the range of 1-80
400	WAF. 00021012	path.illegal	The URL format in the rule configuration is incorrect	It is recommended to modify the URL in the request body parameter to the standard URL and debug again
400	WAF. 00021013	cert.illegal	The HTTPS certificate has expired	It is recommended to upload the unexpired certificate again

Status Code	Error Codes	Error Message	Description	Solution
400	WAF. 00021014	action.illegal	Illegal protective action	It is recommended to configure protection actions according to the enumerated values in the document
400	WAF. 00021015	rule.status.illegal	Illegal rule status	It is recommended to modify the rule status according to the rule status enumeration value in the document
400	WAF. 00021016	description.illegal	Description exception	It is recommended to use standard Chinese and English grammar for description
400	WAF. 00021017	incorrect.rule.config	Incorrect rule configuration	It is recommended to configure protection rules according to the documentation in the help center
400	WAF. 00021018	incorrect.reference.table.config	Incorrect reference table configuration	It is recommended to configure the reference table according to the documentation in the help center
400	WAF. 00021019	incorrect.route.config	Incorrect line configuration	It is recommended to configure the line according to the documentation in the help center

Status Code	Error Codes	Error Message	Description	Solution
400	WAF. 00021020	offsetOrLimit.illegal	Paging parameter error	It is recommended to fill in pagination parameters according to the documents in the help center
400	WAF. 00021021	param.exceed.limit	Parameter exceeds limit	It is recommended to view the parameter limits according to the documentation in the help center
400	WAF. 00022002	resource.already.exists	Resource already exists	It is recommended to check whether the created resource already exists in the console
400	WAF. 00022003	resource.is.being.used	The resource is in use	Remove the relationship between the resource and the user before deleting the resource
400	WAF. 00022004	rule.conflict	Rule conflict	Check whether the target rule conflicts with the existing rule
403	WAF. 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 Huawei technical support

Status Code	Error Codes	Error Message	Description	Solution
500	WAF. 00010001	internal.error	Internal error	Contact Huawei technical support
500	WAF. 00010002	system.busy	Internal error	Contact Huawei technical support
500	WAF. 00010003	cname.failed	Failed to create or modify CNAME	Contact Huawei technical support
500	WAF. 00010004	cname.failed	Failed to get OBS file download link	Contact Huawei technical support
500	WAF. 00020001	internal.error	Service internal exception	It is recommended to try again in five minutes
500	WAF. 00020002	system.busy	System busy	It is recommended to try again in five minutes

A.3 Obtaining a Project ID

Obtaining a Project ID by Calling an API

You can obtain the project ID by calling the IAM API used to query project information based on the specified criteria.

The API used to obtain a project ID is GET https://{Endpoint}/v3/projects. **{Endpoint}** is the IAM endpoint and can be obtained from **Regions and Endpoints**. For details about API authentication, see **Authentication**.

In the following example, **id** indicates the project ID.

```
{
    "projects": [
        {
            "domain_id": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "xxxxxxxx",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
            },
            "id": "a4a5d4098fb4474fa22cd05f897d6b99",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```

Obtaining a Project ID from the Console

A project ID is required for some URLs when an API is called. To obtain a project ID, perform the following operations:

1. Log in to the management console.
2. Click the username and choose **My Credential** from the drop-down list.

   On the **My Credential** page, view project IDs in the project list.

B Change History

Released On	Description
2022-08-05	This is the first official release.