Web Application Firewall

API Reference

Issue	01
Date	2024-04-15

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

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 calling WAF APIs, get yourself familiar with the WAF service.

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. Obtain the regions and endpoints from the enterprise administrator.

1.4 Concepts

- Account

  An account is created upon successful registration with the cloud platform. 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 under the account and grant them permissions for routine management.

- User

  An Identity and Access Management (IAM) user is created using an account 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.

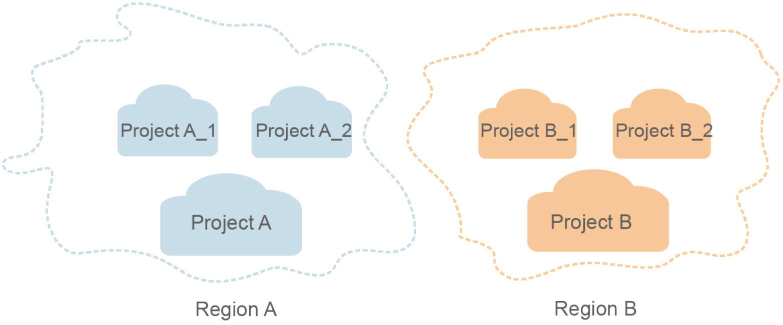
- Availability Zone (AZ)

  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
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 protection policies and modifying the domain names that a protection policy applies to
Event API	API for querying details of an event
Address group management APIs	APIs for managing address groups, such as creating, modifying, querying, and deleting address groups.
Security overview APIs	APIs for querying the number of requests and attacks, bandwidth data, and top statistics data by category.

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 the administrator.

- **resource-path**:

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

- **query-string**:

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

NOTE

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

Request Methods

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

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

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

```
POST https://{{endpoint}}/v3/auth/tokens
```

Request Header

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

Common request header fields are as follows:

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

  NOTE

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

  For more information, see **AK/SK-based Authentication**.

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

```
POST https://{{endpoint}}/v3/auth/tokens
Content-Type: application/json
```

Request Body

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

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

In the case of the API used to obtain a user token, the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Set ***username*** to the name of a user, ***domainname*** to the name of the account that the user belongs to, ************** to the user's login password, and ***xxxxxxxxxxxxxxxxxx*** to the project name. You can learn more information about projects from the administrator.

NOTE

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

```
POST https://{{endpoint}}/v3/auth/tokens
Content-Type: application/json
{
    "auth": {
        "identity": {
            "methods": [
                "password"
            ],
            "password": {
                "user": {
                    "name": "username",
                    "password": "********",
                    "domain": {
                        "name": "domainname"
                    }
                }
            }
        },
        "scope": {
            "project": {
                "name": "xxxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```

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

3.2 Authentication

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

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

Token-based Authentication

NOTE

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

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

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

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

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

```

POST https://{{endpoint}}/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

AK/SK-based Authentication

An AK/SK is used to verify the identity of a request sender. In AK/SK-based authentication, a signature needs to be obtained and then added to requests.

NOTE

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.

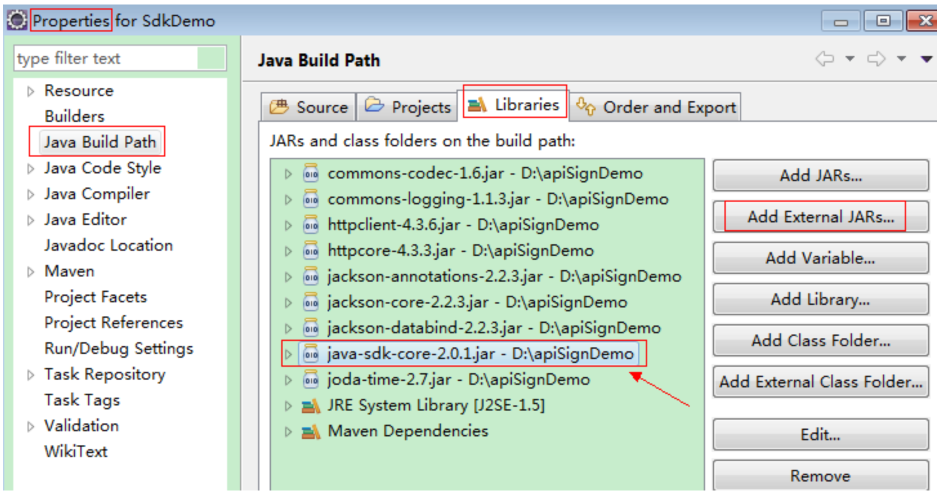
The following uses a demo project to show how to sign a request and use an HTTP client to send an HTTPS request.

Download the demo project at **https://github.com/api-gate-way/SdkDemo**.

If you do not need the demo project, obtain the API Gateway signing SDK from the enterprise administrator.

Decompress the downloaded package and reference the obtained JAR files as dependencies.

Figure 3-1 Importing a JAR file


Properties for SdkDemo
type filter text
Resource
Builders
Java Build Path
Java Code Style
Java Compiler
Java Editor
Javadoc Location
Maven
Project Facets
Project References
Run/Debug Settings
Task Repository
Task Tags
Validation
WikiText
Java Build Path
Source
Projects
Libraries
Order and Export
JARs and class folders on the build path:
commons-codec-1.6.jar - D:\apiSignDemo
commons-logging-1.1.3.jar - D:\apiSignDemo
httpclient-4.3.6.jar - D:\apiSignDemo
httpcore-4.3.3.jar - D:\apiSignDemo
jackson-annotations-2.2.3.jar - D:\apiSignDemo
jackson-core-2.2.3.jar - D:\apiSignDemo
jackson-databind-2.2.3.jar - D:\apiSignDemo
java-sdk-core-2.0.1.jar - D:\apiSignDemo
joda-time-2.7.jar - D:\apiSignDemo
JRE System Library [J2SE-1.5]
Maven Dependencies
Add JARs...
Add External JARs...
Add Variable...
Add Library...
Add Class Folder...
Add External Class Folder...
Edit...
Remove

Step 1 Generate an AK/SK. If an AK/SK pair is already available, skip this step and go to **Step 2**. Find the downloaded AK/SK file, which is usually named **credentials.csv**.

1. Register an account and log in to the management console.
2. Click the username and choose **My Credential** from the drop-down list.
3. On the **My Credentials** page, choose **Access Keys** in the navigation pane.
4. Click **Add Access Key**.

   NOTE

   For users created in IAM that have not bound any email address or mobile number, only the login password needs to be entered.

5. Click **OK**. Download the access key after it is created.

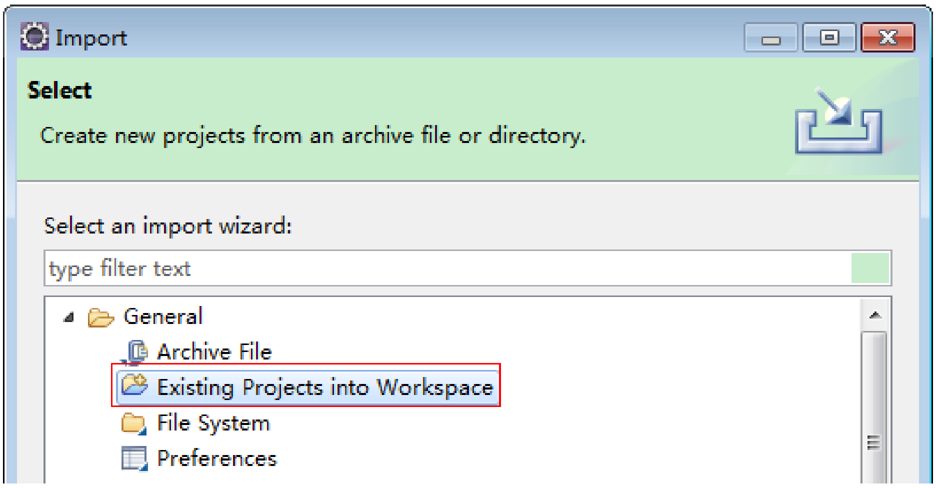
   NOTE

   Keep the access key secure.

Step 2 Download and decompress the demo project.

Step 3 Import the demo project to Eclipse.

Figure 3-2 Selecting Existing Projects into Workspace



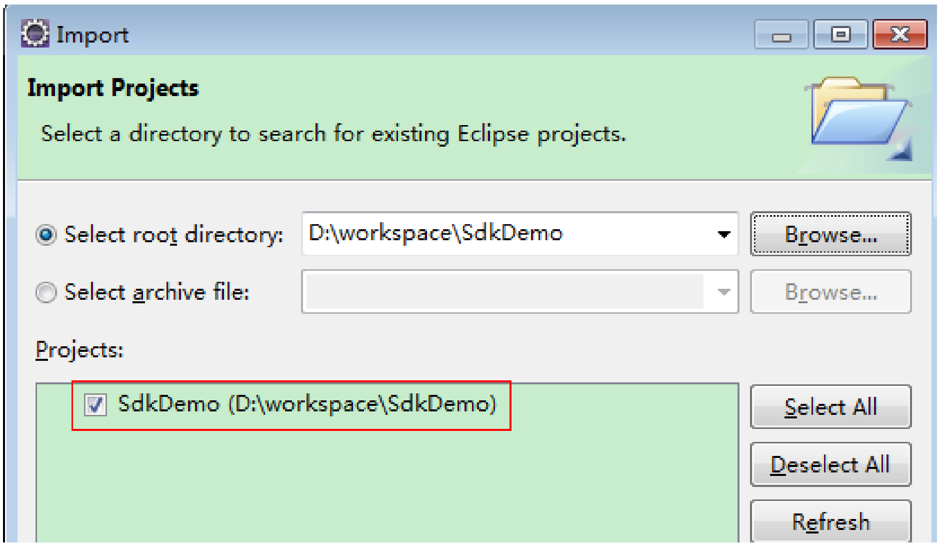
Select

Create new projects from an archive file or directory.

Select an import wizard:

type filter text

Figure 3-3 Selecting the demo project



Import Projects

Select a directory to search for existing Eclipse projects.

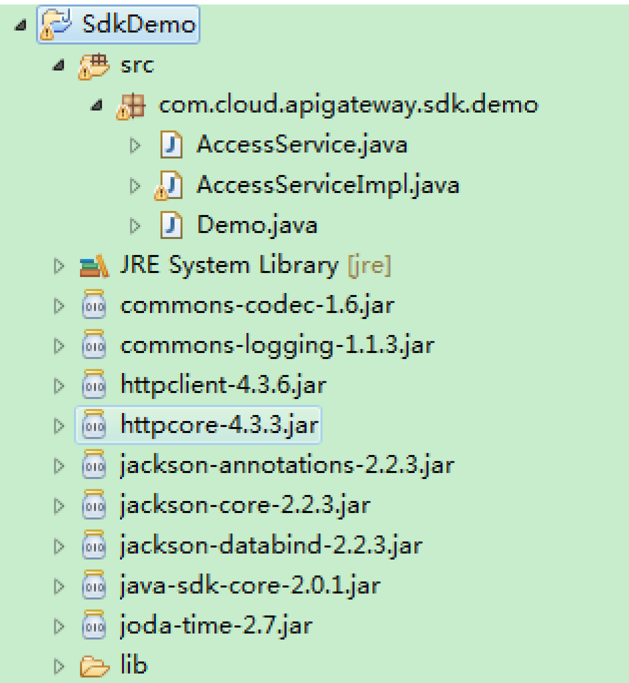
● Select root directory: D:\workspace\SdkDemo

○ Select archive file:

Projects:

☑ SdkDemo (D:\workspace\SdkDemo)

Figure 3-4 Structure of the demo project



```
SdkDemo
  src
    com.cloud.apigateway.sdk.demo
      AccessService.java
      AccessServiceImpl.java
      Demo.java
  JRE System Library [jre]
  commons-codec-1.6.jar
  commons-logging-1.1.3.jar
  httpclient-4.3.6.jar
  httpcore-4.3.3.jar
  jackson-annotations-2.2.3.jar
  jackson-core-2.2.3.jar
  jackson-databind-2.2.3.jar
  java-sdk-core-2.0.1.jar
  joda-time-2.7.jar
  lib
```

Step 4 Sign the request.

The request signing method is integrated in the JAR files imported in **Step 3**. The request needs to be signed before it is sent. The signature will then be added as part of the HTTP header to the request.

The demo code is classified into the following classes to demonstrate signing and sending the HTTP request:

- **AccessService**: An abstract class that merges the GET, POST, PUT, and DELETE methods into the access method.
- **Demo**: Execution entry used to simulate the sending of GET, POST, PUT, and DELETE requests.
- **AccessServiceImpl**: Implements the access method, which contains the code required for communication with API Gateway.

1. Edit the main( ) method in the **Demo.java** file, and replace the bold text with actual values.

   As shown in the following code, if you use other methods such as POST, PUT, and DELETE, see the corresponding comment.

   Specify **region**, **serviceName**, **ak/sk**, and **url** as the actual values. In this demo, the URLs for accessing VPC resources are used.

   To obtain the project ID in the URLs, see **Obtaining a Project ID**. To obtain the endpoint, contact the enterprise administrator.

```
//TODO: Replace region with the name of the region in which the service to be accessed is located.
private static final String region = "";

//TODO: Replace vpc with the name of the service you want to access. For example, ecs, vpc, iam, and elb.
private static final String serviceName = "";

public static void main(String[] args) throws UnsupportedEncodingException
{
```

```
//TODO: Replace the AK and SK with those obtained on the My Credential page.
String ak = System.getenv("CLOUD_SDK_AK")
String sk = System.getenv("CLOUD_SDK_SK")

//TODO: To specify a project ID (multi-project scenarios), add the X-Project-Id header.
//TODO: To access a global service, such as IAM, DNS, CDN, and TMS, add the X-Domain-Id header to
specify an account ID.
//TODO: To add a header, find "Add special headers" in the AccessServiceImple.java file.

//TODO: Test the API
String url = "https://{Endpoint}/v1/{project_id}/vpcs";
get(ak, sk, url);

//TODO: When creating a VPC, replace {project_id} in postUrl with the actual value.
//String postUrl = "https://serviceEndpoint/v1/{project_id}/cloudservers";
//String postbody ="{\"vpc\": {\"name\": \"vpc\",\"cidr\": \"192.168.0.0/16\"}}";
//post(ak, sk, postUrl, postbody);

//TODO: When querying a VPC, replace {project_id} in url with the actual value.
//String url = "https://serviceEndpoint/v1/{project_id}/vpcs/{vpc_id}";
//get(ak, sk, url);

//TODO: When updating a VPC, replace {project_id} and {vpc_id} in putUrl with the actual values.
//String putUrl = "https://serviceEndpoint/v1/{project_id}/vpcs/{vpc_id}";
//String putbody ="{\"vpc\":{\"name\": \"vpc1\",\"cidr\": \"192.168.0.0/16\"}}";
//put(ak, sk, putUrl, putbody);

//TODO: When deleting a VPC, replace {project_id} and {vpc_id} in deleteUrl with the actual values.
//String deleteUrl = "https://serviceEndpoint/v1/{project_id}/vpcs/{vpc_id}";
//delete(ak, sk, deleteUrl);
}
```

2. Compile the code and call the API.

   In the **Package Explorer** area on the left, right-click **Demo.java**, choose **Run AS** > **Java Application** from the shortcut menu to run the demo code.

   You can view the API call logs on the console.

----End

3.3 Response

Status Code

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

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

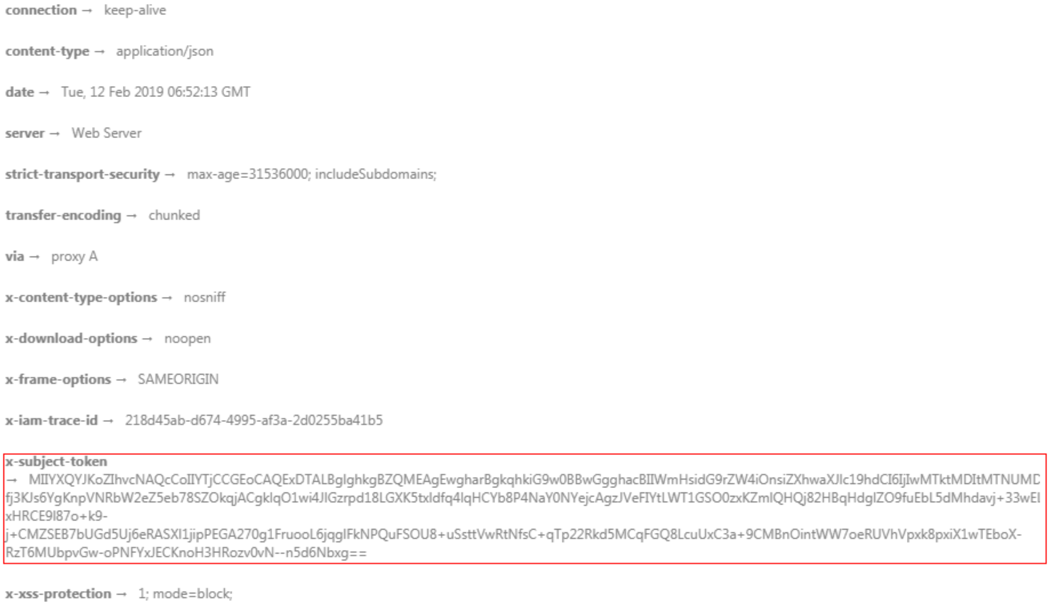
For example, if status code **201** is returned for calling the API used to obtain a user token, the request is successful.

Response Header

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

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

Figure 3-5 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
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkqjACgklqO1wi4JIGzrpd18LGXK5txldfq4lqHCYb8P4NaY0NYejcAgzJVeFIYtLWT1GSO0zxKZmIQHQj82HBqHdglZO9fuEbL5dMhdavj+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 obtain a user token. For the sake of space, only part of the content is displayed here.

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

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

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

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

4 APIs

4.1 Managing Websites Protected by Dedicated WAF Engines

4.1.1 Querying Domain Names Protected by Dedicated WAF Engines

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 4-1 Path Parameters

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

Table 4-2 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the **ListEnterpriseProject** API of EPS.
page	No	String	Page number of the data to be returned during pagination query. Value range: **0** to **100,000**. The default value is **1**, indicating that the data on the first page is returned. Default: **1**
pagesize	No	String	Number of results on each page during pagination query. Value range: **1** to **100**. The default value is **10**, indicating that each page contains 10 results. Default: **10**
hostname	No	String	Domain name
policyname	No	String	Policy name
protect_status	No	Integer	WAF status of the protected domain name. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.

Request Parameters

Table 4-3 Request header parameters

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

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 4-4 Response body parameters

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

Table 4-5 SimplePremiumWafHost

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

Parameter	Type	Description
protect_status	Integer	WAF status of the protected domain name. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be **0** or **1**. **0**: The website traffic has not been routed to WAF. **1**: The website traffic has been routed to WAF.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
hostid	String	Domain name ID, which is the same as the value of id and is a redundant field.

Table 4-6 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. ● **true**: The website passed the PCI 3DS certification check. ● **false**: The website failed the PCI 3DS certification check. Enumeration values: ● **true** ● **false**
pci_dss	String	Whether the website passed the PCI DSS certification check. ● **true**: The website passed the PCI DSS certification check. ● **false**: The website failed the PCI DSS certification check. Enumeration values: ● **true** ● **false**

Parameter	Type	Description
cname	String	The CNAME record being used. - **old**: The old CNAME record is used. - **new**: The new CNAME record is used. Enumeration values: - **old** - **new**
is_dual_az	String	Whether WAF support Multi-AZ DR - **true**: WAF supports multi-AZ DR. - **false**: WAF does not support multi-AZ DR. Enumeration values: - **true** - **false**
ipv6	String	Whether IPv6 protection is supported. - **true**: IPv6 protection is supported. - **false**: IPv6 protection is not supported. Enumeration values: - **true** - **false**

Status code: 400

Table 4-7 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-8 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-9 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.1.2 Adding a Domain Name to a Dedicated WAF Instance

Function

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

URI

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

Table 4-10 Path Parameters

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

Table 4-11 Query Parameters

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

Request Parameters

Table 4-12 Request header parameters

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

Table 4-13 Request body parameters

Parameter	Mandatory	Type	Description
certificateid	No	String	Certificate ID. It can be obtained by calling the **ListCertificates** API. ● This parameter is not required when the client protocol is HTTP. ● This parameter is mandatory when the client protocol is HTTPS.
certificatename	No	String	Certificate name. ● This parameter is not required when the client protocol is HTTP. ● This parameter is mandatory when the client protocol is HTTPS.
hostname	Yes	String	Protected domain name or IP address (port allowed)
proxy	Yes	Boolean	Whether a proxy is used for the protected domain name. ● **false**: No proxy is used. ● **true**: A proxy is used.
policyid	No	String	ID of the policy initially used to the domain name. You can call the **ListPolicy** API to query the policy list and view the ID of a specific policy.
server	Yes	Array of **PremiumWafServer** objects	Origin server configuration of the protected domain name
block_page	No	**BlockPage** object	Alarm page configuration. This parameter is optional. When a user-defined page needs to be configured, all subfields of this parameter are mandatory.
description	No	String	Remarks of the protected domain name

Table 4-14 PremiumWafServer

Parameter	Mandatory	Type	Description
front_protocol	Yes	String	Protocol used by the client to request access to the origin server. Enumeration values: ● **HTTP** ● **HTTPS**
back_protocol	Yes	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: ● **HTTP** ● **HTTPS**
weight	No	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is **1**. This field is not included by cloud WAF.
address	Yes	String	IP address of your origin server requested by the client
port	Yes	Integer	Port used by WAF to forward client requests to the origin server
type	Yes	String	The origin server address is an IPv4 or IPv6 address. Enumeration values: ● **ipv4** ● **ipv6**

Parameter	Mandatory	Type	Description
vpc_id	Yes	String	VPC ID. To obtain the VPC ID, perform the following steps: Use either of the following methods to obtain the VPC ID. ● Log in to the WAF console and choose **Instance Management** > **Dedicated Engine** > **VPC\Subnet**. The VPC ID is in the **VPC \Subnet** column. ● Log in to the VPC console and click the VPC name. On the page displayed, copy the ID in the **VPC Information** area.

Table 4-15 BlockPage

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

Table 4-16 CustomPage

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

Response Parameters

Status code: 200

Table 4-17 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Protected domain names
protocol	String	Client protocol. the protocol used by a client (for example, a browser) to access your website. Enumeration values: - **HTTPS** - **HTTP** - **HTTP&HTTPS**
server	Array of **PremiumWaf Server** objects	Origin server configuration of the protected domain name
proxy	Boolean	Whether to use a proxy - **true**: A proxy is used. - **false**: No proxy is used.
locked	Integer	Domain name status. The value can be **0** or **1**.**0**: The domain name is not frozen. **1**: The domain name is frozen. This parameter is redundant in this version.
timestamp	Long	Time the domain name was added to WAF. The value is a 13-digit timestamp in ms.
tls	String	TLS version. You can use TLS v1.0, TLS v1.1, or TLS v1.2. TLS v1.0 is used by default. Parameter **tls** is available only when the client protocol is HTTPS. Enumeration values: - **TLS v1.0** - **TLS v1.1** - **TLS v1.2** - **TLS v1.3**

Parameter	Type	Description
cipher	String	Parameter **cipher** is required only when the client protocol is HTTPS. The value can be **cipher_1**, **cipher_2**, **cipher_3**, **cipher_4**, or **cipher_default**. ● **cipher_1**: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH ● **cipher_2**: EECDH+AESGCM:EDH+AESGCM ● **cipher_3**: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH ● **cipher_4**: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH ● **cipher_default**: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. Enumeration values: ● **cipher_1** ● **cipher_2** ● **cipher_3** ● **cipher_4** ● **cipher_default**
extend	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.
flag	**Flag** object	Special identifier, which is used on the console.
description	String	Domain name description
policyid	String	ID of the policy initially used to the domain name. You can call the **ListPolicy** API to query the policy list and view the ID of a specific policy.
domainid	String	Account ID, which is the same as the account ID on the **My Credentials** page. To go to this page, log in to Cloud management console, hover the cursor over your username, and click **My Credentials** in the displayed window.

Parameter	Type	Description
projectid	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose **My Credentials**.Then, in the **Projects** area, view **Project ID** of the corresponding project.
enterprise_project_id	String	Enterprise project ID. To obtain the ID, log in to the Cloud management console first. On the menu bar at the top of the page, choose **Enterprise** > **Project Management**. Then, click the project name and view the ID.
protect_status	Integer	WAF status of the protected domain name. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be **0** or **1**. **0**: The website traffic has not been routed to WAF. **1**: The website traffic has been routed to WAF.
block_page	**BlockPage** object	Alarm page configuration

Table 4-18 PremiumWafServer

Parameter	Type	Description
front_protocol	String	Protocol used by the client to request access to the origin server. Enumeration values: ● **HTTP** ● **HTTPS**
back_protocol	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: ● **HTTP** ● **HTTPS**

Parameter	Type	Description
weight	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is **1**. This field is not included by cloud WAF.
address	String	IP address of your origin server requested by the client
port	Integer	Port used by WAF to forward client requests to the origin server
type	String	The origin server address is an IPv4 or IPv6 address. Enumeration values: ● **ipv4** ● **ipv6**
vpc_id	String	VPC ID. To obtain the VPC ID, perform the following steps: Use either of the following methods to obtain the VPC ID. ● Log in to the WAF console and choose **Instance Management** > **Dedicated Engine** > **VPC\Subnet**. The VPC ID is in the **VPC\Subnet** column. ● Log in to the VPC console and click the VPC name. On the page displayed, copy the ID in the **VPC Information** area.

Table 4-19 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. ● **true**: The website passed the PCI 3DS certification check. ● **false**: The website failed the PCI 3DS certification check. Enumeration values: ● **true** ● **false**

Parameter	Type	Description
pci_dss	String	Whether the website passed the PCI DSS certification check. ● **true**: The website passed the PCI DSS certification check. ● **false**: The website failed the PCI DSS certification check. Enumeration values: ● **true** ● **false**
cname	String	The CNAME record being used. ● **old**: The old CNAME record is used. ● **new**: The new CNAME record is used. Enumeration values: ● **old** ● **new**
is_dual_az	String	Whether WAF support Multi-AZ DR ● **true**: WAF supports multi-AZ DR. ● **false**: WAF does not support multi-AZ DR. Enumeration values: ● **true** ● **false**
ipv6	String	Whether IPv6 protection is supported. ● **true**: IPv6 protection is supported. ● **false**: IPv6 protection is not supported. Enumeration values: ● **true** ● **false**

Table 4-20 BlockPage

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

Table 4-21 CustomPage

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

Status code: 400

Table 4-22 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-23 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-24 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "hostname" : "www.demo.com",
  "server" : [ {
    "front_protocol" : "HTTP",
    "back_protocol" : "HTTP",
    "vpc_id" : "cf6dbace-b36a-4d51-ae04-52a3319ae247",
    "type" : "ipv4",
    "address" : "x.x.x.x",
    "port" : 80
  } ],
  "proxy" : false,
  "description" : ""
}
```

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.1.3 Modifying a Domain Name Protected by a Dedicated WAF Instance

Function

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

URI

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

Table 4-25 Path Parameters

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

Table 4-26 Query Parameters

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

Request Parameters

Table 4-27 Request header parameters

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

Table 4-28 Request body parameters

Parameter	Mandatory	Type	Description
proxy	No	Boolean	Whether a proxy is used for the protected domain name. ● **false**: No proxy is used. ● **true**: A proxy is used.
certificateid	No	String	Certificate ID. It can be obtained by calling the **ListCertificates** API. ● This parameter is not required when the client protocol is HTTP. ● This parameter is mandatory when the client protocol is HTTPS.
certificatename	No	String	Certificate name. ● This parameter is not required when the client protocol is HTTP. ● This parameter is mandatory when the client protocol is HTTPS.

Parameter	Mandatory	Type	Description
tls	No	String	TLS version. TLS v1.0 is supported by default. Enumeration values: ● **TLS v1.0** ● **TLS v1.1** ● **TLS v1.2** ● **TLS v1.3**

Parameter	Mandatory	Type	Description
cipher	No	String	Cipher suite. The value can be **cipher_1**, **cipher_2**, **cipher_3**, **cipher_4**, or **cipher_default**: **cipher_1**: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH ● **cipher_2**: EECDH+AESGCM:EDH+AESGCM ● **cipher_3**: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH ● **cipher_4**: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH ● **cipher_default**: The cryptographic algorithms are ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. Enumeration values: ● **cipher_1** ● **cipher_2** ● **cipher_3** ● **cipher_4** ● **cipher_default**
mode	No	String	Special domain name node in dedicated mode. This parameter is required only for special WAF modes, such as ELB.

Parameter	Mandatory	Type	Description
locked	No	Integer	This parameter is reserved, which will be used to freeze a domain name.
protect_status	No	Integer	WAF status of the protected domain name. ● **-1**: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	No	Integer	Domain name access status. The value can be **0** or **1**. **0**: The website traffic has not been routed to WAF. **1**: The website traffic has been routed to WAF.
timestamp	No	Integer	Timestamp.
pool_ids	No	Array of strings	Dedicated engine group the domain name was added to. This parameter is required only in special WAF mode, such as ELB mode.
block_page	No	**BlockPage** object	Alarm page configuration
traffic_mark	No	**TrafficMark** object	Traffic identifier
circuit_breaker	No	**CircuitBreaker** object	Circuit breaker configuration
timeout_config	No	**TimeoutConfig** object	Timeout settings

Table 4-29 BlockPage

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

Table 4-30 CustomPage

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

Table 4-31 TrafficMark

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

Table 4-32 CircuitBreaker

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

Parameter	Mandatory	Type	Description
suspend_num	No	Integer	Threshold of the number of pending URL requests. Connection protection is triggered when the threshold has been reached.
sus_block_time	No	Integer	Downtime duration after the connection protection is triggered. During this period, WAF stops forwarding website requests.

Table 4-33 TimeoutConfig

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

Response Parameters

Status code: 200

Table 4-34 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name added to the dedicated WAF instance
protocol	String	Client protocol. the protocol used by a client (for example, a browser) to access your website.
server	Array of **PremiumWaf Server** objects	Origin server configuration of the protected domain name

Parameter	Type	Description
proxy	Boolean	Whether a proxy is used for the protected domain name. ● **false**: No proxy is used. ● **true**: A proxy is used.
locked	Integer	This parameter is reserved, which will be used to freeze a domain name. Default: **0**
timestamp	Long	Time the domain name was added to WAF.
tls	String	Minimum TLS version. The value can be **TLS v1.0**, **TLS v1.1**, or **TLS v1.2**. TLS v1.0 is used by default. Enumeration values: ● **TLS v1.0** ● **TLS v1.1** ● **TLS v1.2** ● **TLS v1.3**
cipher	String	Cipher suite. The value can be **cipher_1**, **cipher_2**, **cipher_3**, **cipher_4**, or **cipher_default**: **cipher_1**: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH ● **cipher_2**: EECDH+AESGCM:EDH+AESGCM ● **cipher_3**: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH ● **cipher_4**: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH ● **cipher_default**: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. Enumeration values: ● **cipher_1** ● **cipher_2** ● **cipher_3** ● **cipher_4** ● **cipher_default**

Parameter	Type	Description
extend	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.
flag	**Flag** object	Special identifier, which is used on the console.
description	String	Domain name description
policyid	String	ID of the policy initially used to the domain name. You can call the **ListPolicy** API to query the policy list and view the ID of the specific policy.
domainid	String	Account ID, which is the same as the account ID on the **My Credentials** page. To go to this page, log in to Cloud management console, hover the cursor over your username, and click **My Credentials** in the displayed window.
projectid	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose **My Credentials**.Then, in the **Projects** area, view **Project ID** of the corresponding project.
enterprise_project_id	String	Enterprise project ID. To obtain the ID, log in to the Cloud management console first. On the menu bar at the top of the page, choose **Enterprise** > **Project Management**. Then, click the project name and view the ID.
certificateid	String	HTTPS certificate ID.
certificatename	String	Certificate name
protect_status	Integer	WAF status of the protected domain name. ● **-1**: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be **0** or **1**. **0**: The website traffic has not been routed to WAF. **1**: The website traffic has been routed to WAF.

Parameter	Type	Description
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
lb_algorithm	String	Load balancing algorithm. Weighted round robin is used by default and cannot be changed.
block_page	**BlockPage** object	Alarm page configuration
traffic_mark	**TrafficMark** object	Traffic identifier
timeout_config	**TimeoutConfig** object	Timeout settings

Table 4-35 PremiumWafServer

Parameter	Type	Description
front_protocol	String	Protocol used by the client to request access to the origin server. Enumeration values: ● **HTTP** ● **HTTPS**
back_protocol	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: ● **HTTP** ● **HTTPS**
weight	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is **1**. This field is not included by cloud WAF.
address	String	IP address of your origin server requested by the client
port	Integer	Port used by WAF to forward client requests to the origin server
type	String	The origin server address is an IPv4 or IPv6 address. Enumeration values: ● **ipv4** ● **ipv6**

Parameter	Type	Description
vpc_id	String	VPC ID. To obtain the VPC ID, perform the following steps: Use either of the following methods to obtain the VPC ID. ● Log in to the WAF console and choose **Instance Management** > **Dedicated Engine** > **VPC\Subnet**. The VPC ID is in the **VPC\Subnet** column. ● Log in to the VPC console and click the VPC name. On the page displayed, copy the ID in the **VPC Information** area.

Table 4-36 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. ● **true**: The website passed the PCI 3DS certification check. ● **false**: The website failed the PCI 3DS certification check. Enumeration values: ● **true** ● **false**
pci_dss	String	Whether the website passed the PCI DSS certification check. ● **true**: The website passed the PCI DSS certification check. ● **false**: The website failed the PCI DSS certification check. Enumeration values: ● **true** ● **false**
cname	String	The CNAME record being used. ● **old**: The old CNAME record is used. ● **new**: The new CNAME record is used. Enumeration values: ● **old** ● **new**

Parameter	Type	Description
is_dual_az	String	Whether WAF support Multi-AZ DR ● **true**: WAF supports multi-AZ DR. ● **false**: WAF does not support multi-AZ DR. Enumeration values: ● **true** ● **false**
ipv6	String	Whether IPv6 protection is supported. ● **true**: IPv6 protection is supported. ● **false**: IPv6 protection is not supported. Enumeration values: ● **true** ● **false**

Table 4-37 BlockPage

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

Table 4-38 CustomPage

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

Table 4-39 TrafficMark

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

Table 4-40 TimeoutConfig

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

Status code: 400

Table 4-41 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-42 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Status code: 500

Table 4-43 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
{
  "proxy" : false
}
```

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.1.4 Querying Domain Name Settings in Dedicated Mode

Function

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

URI

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

Table 4-44 Path Parameters

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

Table 4-45 Query Parameters

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

Request Parameters

Table 4-46 Request header parameters

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

Response Parameters

Status code: 200

Table 4-47 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name added to the dedicated WAF instance
protocol	String	Client protocol. the protocol used by a client (for example, a browser) to access your website.
server	Array of **PremiumWafServer** objects	Origin server configuration of the protected domain name
proxy	Boolean	Whether a proxy is used for the protected domain name. ● **false**: No proxy is used. ● **true**: A proxy is used.

Parameter	Type	Description
locked	Integer	This parameter is reserved, which will be used to freeze a domain name. Default: **0**
timestamp	Long	Time the domain name was added to WAF.
tls	String	Minimum TLS version. You can use TLS v1.0, TLS v1.1, or TLS v1.2. TLS v1.0 is used by default. Parameter **tls** is required only when the client protocol is HTTPS. Enumeration values: - **TLS v1.0** - **TLS v1.1** - **TLS v1.2** - **TLS v1.3**
cipher	String	Parameter **cipher** is required only when the client protocol is HTTPS. The value can be **cipher_1**, **cipher_2**, **cipher_3**, **cipher_4**, or **cipher_default**. - **cipher_1**: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH - **cipher_2**: EECDH+AESGCM:EDH+AESGCM - **cipher_3**: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH - **cipher_4**: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH - **cipher_default**: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. Enumeration values: - **cipher_1** - **cipher_2** - **cipher_3** - **cipher_4** - **cipher_default**

Parameter	Type	Description
extend	Map<String,String>	Extended field, which is used to save some configuration information about the protected domain name.
flag	**Flag** object	Special identifier, which is used on the console.
description	String	Domain name description
policyid	String	ID of the policy initially used to the domain name. You can call the **ListPolicy** API to query the policy list and view the ID of the specific policy.
domainid	String	Account ID, which is the same as the account ID on the **My Credentials** page. To go to this page, log in to Cloud management console, hover the cursor over your username, and click **My Credentials** in the displayed window.
projectid	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose **My Credentials**.Then, in the **Projects** area, view **Project ID** of the corresponding project.
enterprise_project_id	String	Enterprise project ID. To obtain the ID, log in to the Cloud management console first. On the menu bar at the top of the page, choose **Enterprise** > **Project Management**. Then, click the project name and view the ID.
certificateid	String	HTTPS certificate ID.
certificatename	String	Certificate name
protect_status	Integer	WAF status of the protected domain name. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be **0** or **1**. **0**: The website traffic has not been routed to WAF. **1**: The website traffic has been routed to WAF.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.

Parameter	Type	Description
block_page	**BlockPage** object	Alarm page configuration
traffic_mark	**TrafficMark** object	Traffic identifier
timeout_config	**TimeoutConfig** object	Timeout settings

Table 4-48 PremiumWafServer

Parameter	Type	Description
front_protocol	String	Protocol used by the client to request access to the origin server. Enumeration values: ● **HTTP** ● **HTTPS**
back_protocol	String	Protocol used by WAF to forward client requests it received to origin servers Enumeration values: ● **HTTP** ● **HTTPS**
weight	Integer	Weight of the origin server. The load balancing algorithm forwards requests to the origin server based on the weight. The default value is **1**. This field is not included by cloud WAF.
address	String	IP address of your origin server requested by the client
port	Integer	Port used by WAF to forward client requests to the origin server
type	String	The origin server address is an IPv4 or IPv6 address. Enumeration values: ● **ipv4** ● **ipv6**

Parameter	Type	Description
vpc_id	String	VPC ID. To obtain the VPC ID, perform the following steps: Use either of the following methods to obtain the VPC ID. ● Log in to the WAF console and choose **Instance Management** > **Dedicated Engine** > **VPC\Subnet**. The VPC ID is in the **VPC\Subnet** column. ● Log in to the VPC console and click the VPC name. On the page displayed, copy the ID in the **VPC Information** area.

Table 4-49 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. ● **true**: The website passed the PCI 3DS certification check. ● **false**: The website failed the PCI 3DS certification check. Enumeration values: ● **true** ● **false**
pci_dss	String	Whether the website passed the PCI DSS certification check. ● **true**: The website passed the PCI DSS certification check. ● **false**: The website failed the PCI DSS certification check. Enumeration values: ● **true** ● **false**
cname	String	The CNAME record being used. ● **old**: The old CNAME record is used. ● **new**: The new CNAME record is used. Enumeration values: ● **old** ● **new**

Parameter	Type	Description
is_dual_az	String	Whether WAF support Multi-AZ DR ● **true**: WAF supports multi-AZ DR. ● **false**: WAF does not support multi-AZ DR. Enumeration values: ● **true** ● **false**
ipv6	String	Whether IPv6 protection is supported. ● **true**: IPv6 protection is supported. ● **false**: IPv6 protection is not supported. Enumeration values: ● **true** ● **false**

Table 4-50 BlockPage

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

Table 4-51 CustomPage

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

Table 4-52 TrafficMark

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

Table 4-53 TimeoutConfig

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

Status code: 400

Table 4-54 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-55 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Status code: 500

Table 4-56 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.1.5 Deleting a Domain Name from a Dedicated WAF Instance

Function

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

URI

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

Table 4-57 Path Parameters

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

Table 4-58 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the **ListEnterpriseProject** API of EPS.
keepPolicy	No	Boolean	Whether to retain the rule. **false**: The policy for the domain name will not be retained. **true**: The policy for the domain name will be retained. If the policy used for the domain name you want to delete is also used for other domain names, this parameter must be left blank. Default: **1**

Request Parameters

Table 4-59 Request header parameters

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

Response Parameters

Status code: 200

Table 4-60 Response body parameters

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

Parameter	Type	Description
region	String	Region ID. This parameter is included when the domain name was added to WAF through the console. This parameter is left blank when the domain name was added to WAF by calling an API. You can query the region ID on the Regions and Endpoints page on the Cloud website.
flag	**Flag** object	Special identifier, which is used on the console.
description	String	Domain name description
policyid	String	ID of the policy initially used to the domain name. You can call the **ListPolicy** API to query the policy list and view the ID of a specific policy.
protect_status	Integer	WAF status of the protected domain name. ● **-1**: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be **0** or **1**. **0**: The website traffic has not been routed to WAF. **1**: The website traffic has been routed to WAF.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
host_id	String	Domain name ID, which is the same as the value of **id*. This field is redundant.

Table 4-61 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. - **true**: The website passed the PCI 3DS certification check. - **false**: The website failed the PCI 3DS certification check. Enumeration values: - **true** - **false**
pci_dss	String	Whether the website passed the PCI DSS certification check. - **true**: The website passed the PCI DSS certification check. - **false**: The website failed the PCI DSS certification check. Enumeration values: - **true** - **false**
cname	String	The CNAME record being used. - **old**: The old CNAME record is used. - **new**: The new CNAME record is used. Enumeration values: - **old** - **new**
is_dual_az	String	Whether WAF support Multi-AZ DR - **true**: WAF supports multi-AZ DR. - **false**: WAF does not support multi-AZ DR. Enumeration values: - **true** - **false**
ipv6	String	Whether IPv6 protection is supported. - **true**: IPv6 protection is supported. - **false**: IPv6 protection is not supported. Enumeration values: - **true** - **false**

Status code: 400

Table 4-62 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-63 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-64 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

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

Function

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

URI

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

Table 4-65 Path Parameters

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

Table 4-66 Query Parameters

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

Request Parameters

Table 4-67 Request header parameters

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

Table 4-68 Request body parameters

Parameter	Mandatory	Type	Description
protect_status	Yes	Integer	WAF status of the protected domain name. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.

Response Parameters

Status code: 200

Table 4-69 Response body parameters

Parameter	Type	Description
protect_status	Integer	WAF status of the protected domain name. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.

Status code: 400

Table 4-70 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-71 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-72 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "protect_status" : 1
}
```

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.2 Policy Management

4.2.1 Querying the Protection Policy List

Function

This API is used to query the protection policy list.

URI

GET /v1/{project_id}/waf/policy

Table 4-73 Path Parameters

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

Table 4-74 Query Parameters

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

Request Parameters

Table 4-75 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 4-76 Response body parameters

Parameter	Type	Description
total	Integer	Total number of policies
items	Array of **PolicyResponse** objects	Array of protection policy information

Table 4-77 PolicyResponse

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies
level	Integer	Protection level of basic web protection ● **1**: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, **Low** is recommended. ● **2**: Medium. This protection level meets web protection requirements in most scenarios. ● **3**: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. Default: **2** Enumeration values: ● **1** ● **2** ● **3**

Parameter	Type	Description
full_detection	Boolean	The detection mode in Precise Protection. ● **false**: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. ● **true**: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	**Action** object	Protective actions for each rule in anti-crawler protection.
action	**PolicyAction** object	Protective action
options	**PolicyOption** object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String,Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	Array of strings	Array of domain name IDs protected by the policy.
bind_host	Array of **BindHost** objects	Array of domain names protected with the protection policy. Compared with the **hosts** field, this field contains more details.
extend	Map<String,String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-78 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: ● **log**: WAF only logs discovered attacks. ● **block**: WAF blocks discovered attacks.

Table 4-79 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be **log** or **block**. **log**: WAF only logs discovered attacks. **block**: WAF blocks discovered attacks. Enumeration values: ● **block** ● **log**

Table 4-80 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: ● **true** ● **false**
common	Boolean	Whether general check is enabled Enumeration values: ● **true** ● **false**
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at **true**. You can ignore this parameter. Enumeration values: ● **true** ● **false**
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: ● **true** ● **false**
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: ● **true** ● **false**
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: ● **true** ● **false**

Parameter	Type	Description
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: - **true** - **false**
webshell	Boolean	Whether webshell detection is enabled Enumeration values: - **true** - **false**
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: - **true** - **false**
custom	Boolean	Whether precise protection is enabled Enumeration values: - **true** - **false**
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: - **true** - **false**
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: - **true** - **false**
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: - **true** - **false**
privacy	Boolean	Whether data masking is enabled Enumeration values: - **true** - **false**

Parameter	Type	Description
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: ● **true** ● **false**
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: ● **true** ● **false**
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: ● **true** ● **false**
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: ● **true** ● **false**

Table 4-81 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-82 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-83 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-84 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 1,
  "items" : [ {
    "id" : "41cba8aee2e94bcdbf57460874205494",
    "name" : "policy_2FHwFOKz",
    "level" : 2,
    "action" : {
      "category" : "log"
    },
    "options" : {
      "webattack" : true,
      "common" : true,
      "crawler" : true,
      "crawler_engine" : false,
      "crawler_scanner" : true,
      "crawler_script" : false,
      "crawler_other" : false,
      "webshell" : false,
      "cc" : true,
      "custom" : true,
      "whiteblackip" : true,
      "geoip" : true,
      "ignore" : true,
      "privacy" : true,
      "antitamper" : true,
      "antileakage" : false,
      "bot_enable" : true,
      "modulex_enabled" : false
    },
    "hosts" : [ ],
    "extend" : { },
    "timestamp" : 1650527546218,
    "full_detection" : false,
    "bind_host" : [ ]
  } ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.2.2 Creating a Protection Policy

Function

This API is used to create a protection policy. The system configures some default configuration items when generating the policy. To modify the default configuration items, call the API for updating the protection policy.

URI

POST /v1/{project_id}/waf/policy

Table 4-85 Path Parameters

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

Table 4-86 Query Parameters

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

Request Parameters

Table 4-87 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 4-88 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Array of details of policies

Response Parameters

Status code: 200

Table 4-89 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies
level	Integer	Protection level of basic web protection - **1**: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, **Low** is recommended. - **2**: Medium. This protection level meets web protection requirements in most scenarios. - **3**: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. Default: **2** Enumeration values: - **1** - **2** - **3**
full_detection	Boolean	The detection mode in Precise Protection. - **false**: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. - **true**: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	**Action** object	Protective actions for each rule in anti-crawler protection.
action	**PolicyAction** object	Protective action
options	**PolicyOption** object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String,Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.

Parameter	Type	Description
hosts	Array of strings	Array of domain name IDs protected by the policy.
bind_host	Array of **BindHost** objects	Array of domain names protected with the protection policy. Compared with the **hosts** field, this field contains more details.
extend	Map<String,String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-90 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: ● **log**: WAF only logs discovered attacks. ● **block**: WAF blocks discovered attacks.

Table 4-91 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be **log** or **block**. **log**: WAF only logs discovered attacks. **block**: WAF blocks discovered attacks. Enumeration values: ● **block** ● **log**

Table 4-92 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: ● **true** ● **false**

Parameter	Type	Description
common	Boolean	Whether general check is enabled Enumeration values: - **true** - **false**
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at **true**. You can ignore this parameter. Enumeration values: - **true** - **false**
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: - **true** - **false**
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: - **true** - **false**
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: - **true** - **false**
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: - **true** - **false**
webshell	Boolean	Whether webshell detection is enabled Enumeration values: - **true** - **false**
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: - **true** - **false**

Parameter	Type	Description
custom	Boolean	Whether precise protection is enabled Enumeration values: ● **true** ● **false**
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: ● **true** ● **false**
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: ● **true** ● **false**
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: ● **true** ● **false**
privacy	Boolean	Whether data masking is enabled Enumeration values: ● **true** ● **false**
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: ● **true** ● **false**
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: ● **true** ● **false**
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: ● **true** ● **false**

Parameter	Type	Description
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: ● **true** ● **false**

Table 4-93 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-94 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-95 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 403

Table 4-96 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-97 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "name" : "demo"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true,
    "modulex_enabled" : false
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.2.3 Querying a Policy by ID

Function

This API is used to query a policy by ID.

URI

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

Table 4-98 Path Parameters

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

Table 4-99 Query Parameters

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

Request Parameters

Table 4-100 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 4-101 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies

Parameter	Type	Description
level	Integer	Protection level of basic web protection - **1**: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, **Low** is recommended. - **2**: Medium. This protection level meets web protection requirements in most scenarios. - **3**: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. Default: **2** Enumeration values: - **1** - **2** - **3**
full_detection	Boolean	The detection mode in Precise Protection. - **false**: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. - **true**: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	**Action** object	Protective actions for each rule in anti-crawler protection.
action	**PolicyAction** object	Protective action
options	**PolicyOption** object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String,Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	Array of strings	Array of domain name IDs protected by the policy.

Parameter	Type	Description
bind_host	Array of **BindHost** objects	Array of domain names protected with the protection policy. Compared with the **hosts** field, this field contains more details.
extend	Map<String,String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-102 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: ● **log**: WAF only logs discovered attacks. ● **block**: WAF blocks discovered attacks.

Table 4-103 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be **log** or **block**. **log**: WAF only logs discovered attacks. **block**: WAF blocks discovered attacks. Enumeration values: ● **block** ● **log**

Table 4-104 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: ● **true** ● **false**
common	Boolean	Whether general check is enabled Enumeration values: ● **true** ● **false**

Parameter	Type	Description
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at **true**. You can ignore this parameter. Enumeration values: ● **true** ● **false**
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: ● **true** ● **false**
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: ● **true** ● **false**
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: ● **true** ● **false**
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: ● **true** ● **false**
webshell	Boolean	Whether webshell detection is enabled Enumeration values: ● **true** ● **false**
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: ● **true** ● **false**
custom	Boolean	Whether precise protection is enabled Enumeration values: ● **true** ● **false**

Parameter	Type	Description
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: - **true** - **false**
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: - **true** - **false**
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: - **true** - **false**
privacy	Boolean	Whether data masking is enabled Enumeration values: - **true** - **false**
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: - **true** - **false**
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: - **true** - **false**
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: - **true** - **false**
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: - **true** - **false**

Table 4-105 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-106 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-107 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-108 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "antileakage" : false,
    "bot_enable" : true,
    "modulex_enabled" : false
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.2.4 Updating a Protection Policy

Function

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

URI

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

Table 4-109 Path Parameters

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

Table 4-110 Query Parameters

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

Request Parameters

Table 4-111 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
name	No	String	Array of details of policies
level	No	Integer	Protection level of basic web protection - **1**: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, **Low** is recommended. - **2**: Medium. This protection level meets web protection requirements in most scenarios. - **3**: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. Default: **2** Enumeration values: - **1** - **2** - **3**

Parameter	Mandatory	Type	Description
full_detection	No	Boolean	The detection mode in Precise Protection. - **false**: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. - **true**: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	No	**Action** object	Protective actions for each rule in anti-crawler protection.
action	No	**PolicyAction** object	Protective action
options	No	**PolicyOption** object	Whether a protection type is enabled in protection policy.
modulex_options	No	Map<String,Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	No	Array of strings	Array of domain name IDs protected by the policy.
bind_host	No	Array of **BindHost** objects	Array of domain names protected with the protection policy. Compared with the **hosts** field, this field contains more details.
extend	No	Map<String,String>	Extended field, which is used to store the rule configuration of basic web protection.

Table 4-113 Action

Parameter	Mandatory	Type	Description
category	No	String	Protective action for feature-based anti-crawler rules: ● **log**: WAF only logs discovered attacks. ● **block**: WAF blocks discovered attacks.

Table 4-114 PolicyAction

Parameter	Mandatory	Type	Description
category	No	String	Basic web protection action. The value can be **log** or **block**. **log**: WAF only logs discovered attacks. **block**: WAF blocks discovered attacks. Enumeration values: ● **block** ● **log**

Table 4-115 PolicyOption

Parameter	Mandatory	Type	Description
webattack	No	Boolean	Whether basic web protection is enabled Enumeration values: ● **true** ● **false**
common	No	Boolean	Whether general check is enabled Enumeration values: ● **true** ● **false**

Parameter	Mandatory	Type	Description
crawler	No	Boolean	This parameter is reserved. The value of this parameter is fixed at **true**. You can ignore this parameter. Enumeration values: - **true** - **false**
crawler_engine	No	Boolean	Whether the search engine is enabled Enumeration values: - **true** - **false**
crawler_scanner	No	Boolean	Whether the anti-crawler detection is enabled Enumeration values: - **true** - **false**
crawler_script	No	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: - **true** - **false**
crawler_other	No	Boolean	Whether other crawler check is enabled Enumeration values: - **true** - **false**
webshell	No	Boolean	Whether webshell detection is enabled Enumeration values: - **true** - **false**
cc	No	Boolean	Whether the CC attack protection rules are enabled Enumeration values: - **true** - **false**

Parameter	Mandatory	Type	Description
custom	No	Boolean	Whether precise protection is enabled Enumeration values: - **true** - **false**
whiteblackip	No	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: - **true** - **false**
geoip	No	Boolean	Whether geolocation access control is enabled Enumeration values: - **true** - **false**
ignore	No	Boolean	Whether false alarm masking is enabled Enumeration values: - **true** - **false**
privacy	No	Boolean	Whether data masking is enabled Enumeration values: - **true** - **false**
antitamper	No	Boolean	Whether the web tamper protection is enabled Enumeration values: - **true** - **false**
antileakage	No	Boolean	Whether the information leakage prevention is enabled Enumeration values: - **true** - **false**

Parameter	Mandatory	Type	Description
bot_enable	No	Boolean	Whether the anti-crawler protection is enabled Enumeration values: ● **true** ● **false**
modulex_enabled	No	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: ● **true** ● **false**

Table 4-116 BindHost

Parameter	Mandatory	Type	Description
id	No	String	Domain name ID
hostname	No	String	Domain name
waf_type	No	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	No	String	This parameter is required only by the dedicated mode.

Response Parameters

Status code: 200

Table 4-117 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies

Parameter	Type	Description
level	Integer	Protection level of basic web protection - **1**: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, **Low** is recommended. - **2**: Medium. This protection level meets web protection requirements in most scenarios. - **3**: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. Default: **2** Enumeration values: - **1** - **2** - **3**
full_detection	Boolean	The detection mode in Precise Protection. - **false**: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. - **true**: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	**Action** object	Protective actions for each rule in anti-crawler protection.
action	**PolicyAction** object	Protective action
options	**PolicyOption** object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String,Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	Array of strings	Array of domain name IDs protected by the policy.

Parameter	Type	Description
bind_host	Array of **BindHost** objects	Array of domain names protected with the protection policy. Compared with the **hosts** field, this field contains more details.
extend	Map<String,String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-118 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: ● **log**: WAF only logs discovered attacks. ● **block**: WAF blocks discovered attacks.

Table 4-119 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be **log** or **block**. **log**: WAF only logs discovered attacks. **block**: WAF blocks discovered attacks. Enumeration values: ● **block** ● **log**

Table 4-120 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: ● **true** ● **false**
common	Boolean	Whether general check is enabled Enumeration values: ● **true** ● **false**

Parameter	Type	Description
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at **true**. You can ignore this parameter. Enumeration values: - **true** - **false**
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: - **true** - **false**
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: - **true** - **false**
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: - **true** - **false**
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: - **true** - **false**
webshell	Boolean	Whether webshell detection is enabled Enumeration values: - **true** - **false**
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: - **true** - **false**
custom	Boolean	Whether precise protection is enabled Enumeration values: - **true** - **false**

Parameter	Type	Description
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: - **true** - **false**
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: - **true** - **false**
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: - **true** - **false**
privacy	Boolean	Whether data masking is enabled Enumeration values: - **true** - **false**
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: - **true** - **false**
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: - **true** - **false**
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: - **true** - **false**
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: - **true** - **false**

Table 4-121 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-122 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-123 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-124 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

```
{
  "options" : {
    "whiteblackip" : false
  }
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : false,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true
  },
  "hosts" : [ "c0268b883a854adc8a2cd352193b0e13" ],
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ {
    "id" : "c0268b883a854adc8a2cd352193b0e13",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud"
  } ],
  "share_info" : {
    "is_receiver" : false,
    "provider_display" : {
      "share_count" : 0,
      "accept_count" : 0,
      "process_status" : 0
    }
  }
}
```

Status Codes

Status Code	Description
200	OK

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

Error Codes

See **Error Codes**.

4.2.5 Deleting a Protection Policy

Function

This API is used to delete a protection policy. If the policy is in use, unbind the domain name from the policy before deleting the policy.

URI

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

Table 4-125 Path Parameters

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

Table 4-126 Query Parameters

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

Request Parameters

Table 4-127 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 4-128 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies
level	Integer	Protection level of basic web protection ● **1**: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, **Low** is recommended. ● **2**: Medium. This protection level meets web protection requirements in most scenarios. ● **3**: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. Default: **2** Enumeration values: ● **1** ● **2** ● **3**

Parameter	Type	Description
full_detection	Boolean	The detection mode in Precise Protection. - **false**: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. - **true**: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	**Action** object	Protective actions for each rule in anti-crawler protection.
action	**PolicyAction** object	Protective action
options	**PolicyOption** object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String,Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.
hosts	Array of strings	Array of domain name IDs protected by the policy.
bind_host	Array of **BindHost** objects	Array of domain names protected with the protection policy. Compared with the **hosts** field, this field contains more details.
extend	Map<String,String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-129 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: - **log**: WAF only logs discovered attacks. - **block**: WAF blocks discovered attacks.

Table 4-130 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be **log** or **block**. **log**: WAF only logs discovered attacks. **block**: WAF blocks discovered attacks. Enumeration values: ● **block** ● **log**

Table 4-131 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: ● **true** ● **false**
common	Boolean	Whether general check is enabled Enumeration values: ● **true** ● **false**
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at **true**. You can ignore this parameter. Enumeration values: ● **true** ● **false**
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: ● **true** ● **false**
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: ● **true** ● **false**
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: ● **true** ● **false**

Parameter	Type	Description
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: - **true** - **false**
webshell	Boolean	Whether webshell detection is enabled Enumeration values: - **true** - **false**
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: - **true** - **false**
custom	Boolean	Whether precise protection is enabled Enumeration values: - **true** - **false**
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: - **true** - **false**
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: - **true** - **false**
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: - **true** - **false**
privacy	Boolean	Whether data masking is enabled Enumeration values: - **true** - **false**

Parameter	Type	Description
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: ● **true** ● **false**
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: ● **true** ● **false**
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: ● **true** ● **false**
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: ● **true** ● **false**

Table 4-132 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-133 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-134 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-135 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "62169e2fc4e64148b775ec01b24a1947",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log",
    "modulex_category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true,
    "modulex_enabled" : false
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1649316510603,
  "full_detection" : false,
  "bind_host" : [ ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.2.6 Updating the Domain Name Protection Policy

Function

This API is used to update protection policy applied to a domain name.

URI

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

Table 4-136 Path Parameters

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

Table 4-137 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID.
hosts	Yes	String	Domain name ID. It can be obtained by calling the **ListHost** API.

Request Parameters

Table 4-138 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**

Response Parameters

Status code: 200

Table 4-139 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Array of details of policies
level	Integer	Protection level of basic web protection ● **1**: Low. At this protection level, WAF blocks only requests with obvious attack features. If a large number of false alarms have been reported, **Low** is recommended. ● **2**: Medium. This protection level meets web protection requirements in most scenarios. ● **3**: High. At this protection level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. Default: **2** Enumeration values: ● **1** ● **2** ● **3**
full_detection	Boolean	The detection mode in Precise Protection. ● **false**: Instant detection. When a request hits the blocking conditions in Precise Protection, WAF terminates checks and blocks the request immediately. ● **true**: Full detection. If a request hits the blocking conditions in Precise Protection, WAF does not block the request immediately. Instead, it blocks the requests until other checks are finished.
robot_action	**Action** object	Protective actions for each rule in anti-crawler protection.
action	**PolicyAction** object	Protective action
options	**PolicyOption** object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String,Object>	Configurations about intelligent access control. Currently, this feature is still in the open beta test (OBT) phase and available at some sites.

Parameter	Type	Description
hosts	Array of strings	Array of domain name IDs protected by the policy.
bind_host	Array of **BindHost** objects	Array of domain names protected with the protection policy. Compared with the **hosts** field, this field contains more details.
extend	Map<String,String>	Extended field, which is used to store the rule configuration of basic web protection.
timestamp	Long	Time a policy is created

Table 4-140 Action

Parameter	Type	Description
category	String	Protective action for feature-based anti-crawler rules: ● **log**: WAF only logs discovered attacks. ● **block**: WAF blocks discovered attacks.

Table 4-141 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action. The value can be **log** or **block**. **log**: WAF only logs discovered attacks. **block**: WAF blocks discovered attacks. Enumeration values: ● **block** ● **log**

Table 4-142 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled Enumeration values: ● **true** ● **false**

Parameter	Type	Description
common	Boolean	Whether general check is enabled Enumeration values: - **true** - **false**
crawler	Boolean	This parameter is reserved. The value of this parameter is fixed at **true**. You can ignore this parameter. Enumeration values: - **true** - **false**
crawler_engine	Boolean	Whether the search engine is enabled Enumeration values: - **true** - **false**
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled Enumeration values: - **true** - **false**
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled Enumeration values: - **true** - **false**
crawler_other	Boolean	Whether other crawler check is enabled Enumeration values: - **true** - **false**
webshell	Boolean	Whether webshell detection is enabled Enumeration values: - **true** - **false**
cc	Boolean	Whether the CC attack protection rules are enabled Enumeration values: - **true** - **false**

Parameter	Type	Description
custom	Boolean	Whether precise protection is enabled Enumeration values: ● **true** ● **false**
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled Enumeration values: ● **true** ● **false**
geoip	Boolean	Whether geolocation access control is enabled Enumeration values: ● **true** ● **false**
ignore	Boolean	Whether false alarm masking is enabled Enumeration values: ● **true** ● **false**
privacy	Boolean	Whether data masking is enabled Enumeration values: ● **true** ● **false**
antitamper	Boolean	Whether the web tamper protection is enabled Enumeration values: ● **true** ● **false**
antileakage	Boolean	Whether the information leakage prevention is enabled Enumeration values: ● **true** ● **false**
bot_enable	Boolean	Whether the anti-crawler protection is enabled Enumeration values: ● **true** ● **false**

Parameter	Type	Description
modulex_enabled	Boolean	Whether CC attack protection for moduleX is enabled. This feature is in the open beta test (OBT). During the OBT, only the log only mode is supported. Enumeration values: ● **true** ● **false**

Table 4-143 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-144 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-145 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-146 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
PUT https://{Endpoint}/v1/{project_id}/waf/policy/{policy_id}?
enterprise_project_id=0&hosts=c0268b883a854adc8a2cd352193b0e13
```

Example Responses

Status code: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log",
    "modulex_category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "precise" : false,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "anticrawler" : false,
    "antileakage" : false,
    "followed_action" : false,
    "bot_enable" : true,
    "modulex_enabled" : false
  },
  "hosts" : [ "c0268b883a854adc8a2cd352193b0e13" ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ {
    "id" : "c0268b883a854adc8a2cd352193b0e13",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud"
  } ],
  "share_info" : {
    "is_receiver" : false,
    "provider_display" : {
      "share_count" : 0,
      "accept_count" : 0,
      "process_status" : 0
  }
 }
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3 Rule Management

4.3.1 Changing the Status of a Rule

Function

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

URI

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

Table 4-147 Path Parameters

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

Parameter	Mandatory	Type	Description
ruletype	Yes	String	Policy Type Enumeration values: - **whiteblackip** - **geoip** - **privacy** - **antitamper** - **custom** - **ignore**
rule_id	Yes	String	Rule ID. It can be obtained by calling the specific API that is used to obtain the rule list of a certain type. For example, you can call the **ListWhiteblackipRule** API to obtain the ID of a blacklist or whitelist rule.

Table 4-148 Query Parameters

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

Request Parameters

Table 4-149 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 4-150 Request body parameters

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

Response Parameters

Status code: 200

Table 4-151 Response body parameters

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

Status code: 400

Table 4-152 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-153 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-154 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "status" : 0
}
```

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

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

Function

Querying Global Protection Whitelist (Formerly False Alarm Masking) Rules

URI

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

Table 4-155 Path Parameters

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

Table 4-156 Query Parameters

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

Request Parameters

Table 4-157 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 4-158 Response body parameters

Parameter	Type	Description
total	Integer	The number of global protection whitelist (formerly false alarm masking) rules in the protection policy.
items	Array of **IgnoreRuleBody** objects	Domain names the global protection whitelist (formerly false alarm masking) rule is used for.

Table 4-159 IgnoreRuleBody

Parameter	Type	Description
id	String	Rule ID
policyid	String	ID of the protection policy that includes the rule
timestamp	Long	Timestamp the rule was created.
description	String	Rule description
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.

Parameter	Type	Description
url	String	The path for false masking alarms. This parameter is available only when **mode** is set to **0**.
rule	String	Rules to be masked ● If you want to block a specific built-in rule, the value of this parameter is the rule ID. To query the rule ID, go to the WAF console, choose **Policies** and click the target policy name. On the displayed page, in the **Basic Web Protection** area, select the **Protection Rules** tab, and view the ID of the specific rule. You can also query the rule ID in the event details. ● If you want to mask a type of basic web protection rules, set this parameter to the name of the type of basic web protection rules. **xss**: XSS attacks **webshell**: Web shells **vuln**: Other types of attacks **sqli**: SQL injection attack **robot**: Malicious crawlers **rfi**: Remote file inclusion **lfi**: Local file inclusion **cmdi**: Command injection attack ● To bypass the basic web protection, set this parameter to **all**. ● To bypass all WAF protection, set this parameter to **bypass**.
mode	Integer	Version number. The value 0 indicates the old version V1, and the value 1 indicates the new version V2. If the value of mode is 0, the conditions field does not exist, and the url and url_logic fields exist. When the value of mode is 1, the url and url_logic fields do not exist, and the conditions field exists.
url_logic	String	Matching logic. The value can be **equal**, **not_equal**, **contain**, **not_contain**, **prefix**, **not_prefix**, **suffix**, **not_suffix**.
conditions	Array of **Condition** objects	Condition list
domain	Array of strings	Protecting Domain Names or Protecting Websites
advanced	**Advanced** object	Advanced settings

Table 4-160 Condition

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

Table 4-161 Advanced

Parameter	Type	Description
index	String	Field type. The following field types are supported: params, cookie, header, body, and multipart. ● When you select **params**, **cookie**, or **header**, you can set this parameter to **all** or configure subfields as required. ● When you select **body** or **multipart**, set this parameter to **all**.
contensts	Array of strings	Subfield of the specified field type. The default value is **all**.

Status code: 400

Table 4-162 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 403

Table 4-163 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-164 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-165 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "40484384970948d79fffe4e4ae1fc54d",
    "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",
    "timestamp" : 1650512535222,
    "description" : "demo",
    "status" : 1,
    "rule" : "091004",
    "mode" : 1,
    "conditions" : [ {
      "category" : "ip",
      "contents" : [ "x.x.x.x" ],
      "logic_operation" : "equal"
    } ],
    "domain" : [ "we.test.418lab.cn" ]
  } ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

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

Function

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

URI

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

Table 4-166 Path Parameters

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

Table 4-167 Query Parameters

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

Request Parameters

Table 4-168 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 4-169 Request body parameters

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

Parameter	Mandatory	Type	Description
conditions	Yes	Array of **CreateCondition** objects	Condition list
mode	Yes	Integer	The value is fixed at **1**, indicating v2 false alarm masking rules. v1 is used only for compatibility with earlier versions, and false alarm rules cannot be created in v1.
rule	Yes	String	Items to be masked. You can provide multiple items and separate them with semicolons (;). ● If you want to block a specific built-in rule, the value of this parameter is the rule ID. To query the rule ID, go to the WAF console, choose **Policies** and click the target policy name. On the displayed page, in the **Basic Web Protection** area, select the **Protection Rules** tab, and view the ID of the specific rule. You can also query the rule ID in the event details. ● If you want to mask a type of basic web protection rules, set this parameter to the name of the type of basic web protection rules. **xss**: XSS attacks **webshell**: Web shells **vuln**: Other types of attacks **sqli**: SQL injection attack **robot**: Malicious crawlers **rfi**: Remote file inclusion **lfi**: Local file inclusion **cmdi**: Command injection attack ● To bypass the basic web protection, set this parameter to **all**. ● To bypass all WAF protection, set this parameter to **bypass**.

Parameter	Mandatory	Type	Description
advanced	No	**Advanced** object	Advanced settings
description	No	String	Description of a masking rule

Table 4-170 CreateCondition

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

Parameter	Mandatory	Type	Description
index	No	String	If the field type is **ip** and the subfield is the client IP address, the **index** parameter is not required. If the subfield type is **X-Forwarded-For**, the value is **x-forwarded-for**. If the field type is **params**, **header**, or **cookie**, and the subfield is user-defined, the value of **index** is the user-defined subfield.

Table 4-171 Advanced

Parameter	Mandatory	Type	Description
index	No	String	Field type. The following field types are supported: params, cookie, header, body, and multipart. ● When you select **params**, **cookie**, or **header**, you can set this parameter to **all** or configure subfields as required. ● When you select **body** or **multipart**, set this parameter to **all**.
contensts	No	Array of strings	Subfield of the specified field type. The default value is **all**.

Response Parameters

Status code: 200

Table 4-172 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
timestamp	Long	Timestamp the rule was created.
description	String	Rule Description

Parameter	Type	Description
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.
rule	String	ID of the built-in rule to be masked. You can query the rule ID by choosing **Policies** > **Policy Name** > **Basic Web Protection** > **Protection Rules** on the WAF console or on the event details page.
mode	Integer	The value is fixed at **1**, indicating v2 false alarm masking rules are used. v1 is used only for compatibility with earlier versions, and false alarm rules cannot be created in v1.
conditions	Array of **Condition** objects	Condition list
advanced	**Advanced** object	Advanced settings
domain	Array of strings	Protected domain name or website

Table 4-173 Condition

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

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

Table 4-174 Advanced

Parameter	Type	Description
index	String	Field type. The following field types are supported: params, cookie, header, body, and multipart. ● When you select **params**, **cookie**, or **header**, you can set this parameter to **all** or configure subfields as required. ● When you select **body** or **multipart**, set this parameter to **all**.
contensts	Array of strings	Subfield of the specified field type. The default value is **all**.

Status code: 400

Table 4-175 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-176 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-177 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "domain" : [ "we.test.418lab.cn" ],
  "conditions" : [ {
    "category" : "url",
    "logic_operation" : "contain",
    "contents" : [ "x.x.x.x" ],
    "index" : null
  } ],
  "mode" : 1,
  "description" : "demo",
  "rule" : "091004"
}
```

Example Responses

Status code: 200

OK

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

Status Codes

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

Status Code	Description
500	Internal server error.

Error Codes

See **Error Codes**.

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

Function

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

URI

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

Table 4-178 Path Parameters

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

Table 4-179 Query Parameters

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

Request Parameters

Table 4-180 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 4-181 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
timestamp	Long	Timestamp the rule was created.
description	String	Rule Description
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.
url	String	The path for false masking alarms. This parameter is available only when **mode** is set to **0**.

Parameter	Type	Description
rule	String	ID of the built-in rule to be masked. You can query the rule ID by choosing **Policies** > **Policy Name** > **Basic Web Protection** > **Protection Rules** on the WAF console or on the event details page.
mode	Integer	Version number. The value can be **0** or **1**. **0**: indicates the old version V1. **1** indicates the new version V2. When the value of **mode** is **0**, the **conditions** field does not exist, but the **url** and **url_logic** fields exist. When the value of **mode** is **1**, the **url** and **url_logic** fields do not exist, but the **conditions** field exists.
url_logic	String	URL match logic
conditions	Array of **Condition** objects	Filter
advanced	**Advanced** object	Advanced settings
domains	Array of strings	Protected domain name or website

Table 4-182 Condition

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

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

Table 4-183 Advanced

Parameter	Type	Description
index	String	Field type. The following field types are supported: params, cookie, header, body, and multipart. ● When you select **params**, **cookie**, or **header**, you can set this parameter to **all** or configure subfields as required. ● When you select **body** or **multipart**, set this parameter to **all**.
contensts	Array of strings	Subfield of the specified field type. The default value is **all**.

Status code: 400

Table 4-184 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-185 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-186 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "40484384970948d79fffe4e4ae1fc54d",
  "policyid" : "f385eceedf7c4c34a4d1def19eafbe85",
  "timestamp" : 1650512535222,
  "description" : "demo",
  "status" : 1,
  "rule" : "091004",
  "mode" : 1,
  "conditions" : [ {
    "category" : "ip",
    "contents" : [ "x.x.x.x" ],
    "logic_operation" : "equal"
  } ],
  "domain" : [ "we.test.418lab.cn" ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3.5 Querying the Blacklist and Whitelist Rule List

Function

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

URI

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

Table 4-187 Path Parameters

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

Table 4-188 Query Parameters

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

Request Parameters

Table 4-189 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 4-190 Response body parameters

Parameter	Type	Description
total	Integer	Number of the whitelist and blacklist rules
items	Array of **WhiteBlackIpResponseBody** objects	Details of blacklist or whitelist rules

Table 4-191 WhiteBlackIpResponseBody

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the whitelist or blacklist rule
policyid	String	Policy ID
timestamp	Long	Timestamp (ms) when the rule was created
description	String	Rule Description
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.
addr	String	IP address/IP address group

Parameter	Type	Description
white	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.
ip_group	**Ip_group** object	IP address group

Table 4-192 Ip_group

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

Status code: 400

Table 4-193 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-194 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-195 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.6 Creating a Blacklist/Whitelist Rule

Function

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

URI

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

Table 4-196 Path Parameters

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

Table 4-197 Query Parameters

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

Request Parameters

Table 4-198 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 4-199 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Rue name. The value can contain a maximum of 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.
addr	No	String	IP address or IP address ranges in the blacklist or whitelist rule, for example, 42.123.120.66 or 42.123.120.0/16.
description	No	String	Rule description
white	Yes	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.
ip_group_id	No	String	ID of the created IP address group. Use either this parameter or **addr**. To add an IP address group, go to the WAF console, choose **Objects** > **Address Groups**, and click **Add Address Group**.

Response Parameters

Status code: 200

Table 4-200 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the whitelist or blacklist rule
policyid	String	Policy ID
addr	String	IP address or IP address ranges in the blacklist or whitelist rule, for example, 42.123.120.66 or 42.123.120.0/16.

Parameter	Type	Description
white	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.
ip_group	**Ip_group** object	IP address group
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.
description	String	Rule Description
timestamp	Long	Time a rule is created. The value is a 13-digit timestamp in millisecond.

Table 4-201 Ip_group

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

Status code: 400

Table 4-202 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-203 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Status code: 500

Table 4-204 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.7 Updating a Blacklist or Whitelist Protection Rule

Function

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

URI

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

Table 4-205 Path Parameters

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

Table 4-206 Query Parameters

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

Request Parameters

Table 4-207 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 4-208 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the whitelist or blacklist rule
addr	No	String	IP address or IP address ranges in the blacklist or whitelist rule, for example, 42.123.120.66 or 42.123.120.0/16.
description	No	String	Rule description
white	Yes	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.
ip_group_id	No	String	ID of the created IP address group. Use either this parameter or **addr**. To add an IP address group, go to the WAF console, choose **Objects** > **Address Groups**, and click **Add Address Group**.

Response Parameters

Status code: 200

Table 4-209 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the whitelist or blacklist rule
policyid	String	Policy ID
addr	String	IP address or IP address ranges included in the whitelist or blacklist rule.
description	String	Description of the blacklist or whitelist rule
white	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.
ip_group	**Ip_group** object	IP address group

Table 4-210 Ip_group

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

Status code: 400

Table 4-211 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-212 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-213 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "name" : "demo",
  "white" : 0,
  "description" : "demo",
  "addr" : "1.1.1.2"
}
```

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Status Code	Description
500	Internal server error.

Error Codes

See **Error Codes**.

4.3.8 Deleting a Blacklist or Whitelist Rule

Function

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

URI

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

Table 4-214 Path Parameters

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

Table 4-215 Query Parameters

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

Request Parameters

Table 4-216 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 4-217 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
name	String	Name of the whitelist or blacklist rule
timestamp	Long	Time a rule is deleted. The value must be a 13-digit timestamp in millisecond.
description	String	Description
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.
addr	String	IP address or IP address ranges in the blacklist or whitelist rule, for example, 42.123.120.66 or 42.123.120.0/16.
white	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.
ip_group	**Ip_group** object	IP address group

Table 4-218 Ip_group

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

Status code: 400

Table 4-219 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-220 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-221 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.9 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 4-222 Path Parameters

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

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID. It can be obtained by calling the **ListPolicy** API.

Table 4-223 Query Parameters

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

Request Parameters

Table 4-224 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 4-225 Response body parameters

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

Table 4-226 PrivacyResponseBody

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
timestamp	Long	Time the rule was created. The value is a 13-digit timestamp in ms.
status	Integer	Rule status. The value can be **0** or **1**. - **0**: The rule is disabled. - **1**: The rule is enabled.
url	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/. *The asterisk ()* indicates the path prefix.
category	String	Masked field. - **Params**: The **params** field in requests - **Cookie**: Web visitors distinguished by cookie - **Header**: Custom HTTP header - **Form**: Forms Enumeration values: - **params** - **cookie** - **header** - **form**
index	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs.
description	String	(Optional) A description of the rule.

Status code: 400

Table 4-227 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-228 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-229 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.10 Creating a Data Masking Rule

Function

This API is used to create a data masking rule.

URI

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

Table 4-230 Path Parameters

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

Table 4-231 Query Parameters

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

Request Parameters

Table 4-232 Request header parameters

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

Table 4-233 Request body parameters

Parameter	Mandatory	Type	Description
url	Yes	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/_. The asterisk (_) indicates the path prefix.
category	Yes	String	Masked field. ● **Params**: The **params** field in requests ● **Cookie**: Web visitors distinguished by cookie ● **Header**: Custom HTTP header ● **Form**: Forms Enumeration values: ● **params** ● **cookie** ● **header** ● **form**

Parameter	Mandatory	Type	Description
index	Yes	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs. The masked field name cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.
description	No	String	(Optional) A description of the rule.

Response Parameters

Status code: 200

Table 4-234 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
timestamp	Long	Time the rule was created. The value is a 13-digit timestamp in ms.
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.
url	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/*. The asterisk ()* indicates the path prefix.
category	String	Masked field. ● **Params**: The **params** field in requests ● **Cookie**: Web visitors distinguished by cookie ● **Header**: Custom HTTP header ● **Form**: Forms Enumeration values: ● **params** ● **cookie** ● **header** ● **form**

Parameter	Type	Description
index	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs.
description	String	(Optional) A description of the rule.

Status code: 400

Table 4-235 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-236 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-237 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo",
  "description" : "demo"
}
```

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.11 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 4-238 Path Parameters

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

Table 4-239 Query Parameters

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

Request Parameters

Table 4-240 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 4-241 Request body parameters

Parameter	Mandatory	Type	Description
url	Yes	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/*. The asterisk ()* indicates the path prefix.
category	Yes	String	Masked field. - **Params**: The **params** field in requests - **Cookie**: Web visitors distinguished by cookie - **Header**: Custom HTTP header - **Form**: Forms Enumeration values: - **params** - **cookie** - **header** - **form**
index	Yes	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs. The masked field name cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.
description	No	String	(Optional) A description of the rule.

Response Parameters

Status code: 200

Table 4-242 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID

Parameter	Type	Description
timestamp	Long	Time the rule was created. The value is a 13-digit timestamp in ms.
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.
url	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/*. The asterisk (*) indicates the path prefix.
category	String	Masked field. ● **Params**: The **params** field in requests ● **Cookie**: Web visitors distinguished by cookie ● **Header**: Custom HTTP header ● **Form**: Forms Enumeration values: ● **params** ● **cookie** ● **header** ● **form**
index	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs.
description	String	(Optional) A description of the rule.

Status code: 400

Table 4-243 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-244 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-245 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "url" : "/demo",
  "category" : "cookie",
  "index" : "demo1",
  "description" : "demo"
}
```

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.12 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 4-246 Path Parameters

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

Table 4-247 Query Parameters

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

Request Parameters

Table 4-248 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 4-249 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
timestamp	Long	Time the rule was created. The value is a 13-digit timestamp in ms.
description	String	(Optional) A description of the rule.
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.
url	String	URL protected by the data masking rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/*. The asterisk ()* indicates the path prefix.
category	String	Masked field. ● **Params**: The **params** field in requests ● **Cookie**: Web visitors distinguished by cookie ● **Header**: Custom HTTP header ● **Form**: Forms
index	String	Masked field name. Set the field name based on the masked field. The masked field will not be displayed in logs.

Status code: 400

Table 4-250 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-251 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-252 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.13 Querying the List of Geolocation Access Control Rules

Function

Querying the List of Geolocation Access Control Rules

URI

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

Table 4-253 Path Parameters

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

Table 4-254 Query Parameters

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

Parameter	Mandatory	Type	Description
page	No	Integer	Page number of the data to be returned during pagination query. The default value is **1**, indicating that the data on the first page is returned. Default: **1**
pagesize	No	Integer	Number of results on each page during pagination query. Value range: **1** to **100**. The default value is **10**, indicating that each page contains 10 results. Default: **10**

Request Parameters

Table 4-255 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 4-256 Response body parameters

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

Table 4-257 GeOIpItem

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
name	String	Name of the geolocation access control rue
geoip	String	Locations that can be configured in the geolocation access control rule: (**CN**: China, **CA**: Canada, **US**: The United States, **AU**: Australia, **IN**: India, **JP**: Japan, **UK**: United Kingdom, **FR**: France, **DE**: Germany, **BR**: Brazil, **Thailand**: Thailand, **Singapore**: Singapore,**South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia, **GD** Guangdong, **FJ**: Fujian, **JL**: Jilin, **LN**: Liaoning, **TW**: Taiwan (China), **GZ**: Guizhou, **AH**: Anhui, **HL**: Heilongjiang, **HA**: Henan, **SC**: Sichuan, **HE**: Hebei, **YN**: Yunnan, **HB**: Hubei, **HI**: Hainan, **QH**: Qinghai, **HN**: Hunan, **JX**: Jiangxi, **SX**: Shanxi, **SN**: Shaanxi, **ZJ**: Zhejiang, **GS**: Gansu, **JS**: Jiangsu, **SD**: Shandong, **BJ**: Beijing, **SH**: Shanghai, **TJ**: Tianjin, **CQ**: Chongqing, **MO**: Macao (China), **HK**: Hong Kong (China), **NX**: Ningxia, **GX**: Guangxi, **XJ**: Xinjiang, **XZ**: Tibet, **NM**: Inner Mongolia
white	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.
status	Integer	Rule status. ● **true**: enabled. ● **false**: disabled.
timestamp	Long	Time the rule is created.

Status code: 400

Table 4-258 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-259 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-260 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "06f07f6c229141b9a4a78614751bb687",
    "policyid" : "2abeeecefb9840e6bf05efbd80d0fcd7",
    "timestamp" : 1636340038062,
    "status" : 1,
    "geoip" : "US",
    "white" : 1,
    "name" : "demo"
  } ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3.14 Creating a Geolocation Access Control Rule

Function

Creating a Geolocation Access Control Rule

URI

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

Table 4-261 Path Parameters

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

Table 4-262 Query Parameters

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

Request Parameters

Table 4-263 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 4-264 Request body parameters

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

Parameter	Mandatory	Type	Description
geoip	Yes	String	Locations that can be configured in the geolocation access control rule: (**CN**: China, **CA**: Canada, **US**: The United States, **AU**: Australia, **IN**: India, **JP**: Japan, **UK**: United Kingdom, **FR**: France, **DE**: Germany, **BR**: Brazil, **Thailand**: Thailand, **Singapore**: Singapore,**South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia, **GD** Guangdong, **FJ**: Fujian, **JL**: Jilin, **LN**: Liaoning, **TW**: Taiwan (China), **GZ**: Guizhou, **AH**: Anhui, **HL**: Heilongjiang, **HA**: Henan, **SC**: Sichuan, **HE**: Hebei, **YN**: Yunnan, **HB**: Hubei, **HI**: Hainan, **QH**: Qinghai, **HN**: Hunan, **JX**: Jiangxi, **SX**: Shanxi, **SN**: Shaanxi, **ZJ**: Zhejiang, **GS**: Gansu, **JS**: Jiangsu, **SD**: Shandong, **BJ**: Beijing, **SH**: Shanghai, **TJ**: Tianjin, **CQ**: Chongqing, **MO**: Macao (China), **HK**: Hong Kong (China), **NX**: Ningxia, **GX**: Guangxi, **XJ**: Xinjiang, **XZ**: Tibet, **NM**: Inner Mongolia
white	Yes	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.
status	No	Integer	Rule status. ● **true**: enabled. ● **false**: disabled.
description	No	String	Rule Description

Response Parameters

Status code: 200

Table 4-265 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the geolocation access control rue
policyid	String	Policy ID
geoip	String	Locations that can be configured in the geolocation access control rule: **CN**: China, **CA**: Canada, **US**: The United States, **AU**: Australia, **IN**: India, **JP**: Japan, **UK**: United Kingdom, **FR**: France, **DE**: Germany, **BR**: Brazil, **Thailand**: Thailand, **Singapore**: Singapore,**South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia
white	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.
status	Integer	Rule status. ● **true**: enabled. ● **false**: disabled.
timestamp	Long	Time the rule is created.

Status code: 400

Table 4-266 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-267 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-268 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "white" : 0,
  "description" : "demo",
  "name" : "demo",
  "geoip" : "SH|Afghanistan"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "02dafa406c4941368a1037b020f15a53",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650534513775,
  "description" : "demo",
  "status" : 1,
  "geoip" : "US",
  "white" : 0,
  "geoTagList" : [ "US" ]
}
```

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**.

4.3.15 Updating a Geolocation Access Control Rule

Function

Updating a Geolocation Access Control Rule

URI

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

Table 4-269 Path Parameters

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

Table 4-270 Query Parameters

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

Request Parameters

Table 4-271 Request header parameters

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

Table 4-272 Request body parameters

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

Parameter	Mandatory	Type	Description
geoip	Yes	String	Locations that can be configured in the geolocation access control rule: (**CN**: China, **CA**: Canada, **US**: The United States, **AU**: Australia, **IN**: India, **JP**: Japan, **UK**: United Kingdom, **FR**: France, **DE**: Germany, **BR**: Brazil, **Thailand**: Thailand, **Singapore**: Singapore,**South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia, **GD** Guangdong, **FJ**: Fujian, **JL**: Jilin, **LN**: Liaoning, **TW**: Taiwan (China), **GZ**: Guizhou, **AH**: Anhui, **HL**: Heilongjiang, **HA**: Henan, **SC**: Sichuan, **HE**: Hebei, **YN**: Yunnan, **HB**: Hubei, **HI**: Hainan, **QH**: Qinghai, **HN**: Hunan, **JX**: Jiangxi, **SX**: Shanxi, **SN**: Shaanxi, **ZJ**: Zhejiang, **GS**: Gansu, **JS**: Jiangsu, **SD**: Shandong, **BJ**: Beijing, **SH**: Shanghai, **TJ**: Tianjin, **CQ**: Chongqing, **MO**: Macao (China), **HK**: Hong Kong (China), **NX**: Ningxia, **GX**: Guangxi, **XJ**: Xinjiang, **XZ**: Tibet, **NM**: Inner Mongolia
white	Yes	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.

Response Parameters

Status code: 200

Table 4-273 Response body parameters

Parameter	Type	Description
id	String	Rule ID

Parameter	Type	Description
name	String	Name of the geolocation access control rue
description	String	Description
policyid	String	Policy ID
geoip	String	Locations that can be configured in the geolocation access control rule: **CN**: China, **CA**: Canada, **US**: The United States, **AU**: Australia, **IN**: India, **JP**: Japan, **UK**: United Kingdom, **FR**: France, **DE**: Germany, **BR**: Brazil, **Thailand**: Thailand, **Singapore**: Singapore,**South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia
white	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.

Status code: 400

Table 4-274 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-275 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-276 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "white" : 0,
  "name" : "demo",
  "geoip" : "BJ|Afghanistan"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "02dafa406c4941368a1037b020f15a53",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "description" : "demo",
  "geoip" : "US",
  "white" : 0,
  "geoTagList" : [ "US" ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3.16 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 4-277 Path Parameters

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

Table 4-278 Query Parameters

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

Request Parameters

Table 4-279 Request header parameters

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

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

Response Parameters

Status code: 200

Table 4-280 Response body parameters

Parameter	Type	Description
id	String	Rule ID
name	String	Name of the geolocation access control rue
policyid	String	Policy ID
geoip	String	Locations that can be configured in the geolocation access control rule: **CN**: China, **CA**: Canada, **US**: The United States, **AU**: Australia, **IN**: India, **JP**: Japan, **UK**: United Kingdom, **FR**: France, **DE**: Germany, **BR**: Brazil, **Thailand**: Thailand, **Singapore**: Singapore,**South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia
white	Integer	Protective action ● **0**: WAF blocks requests that hit the rule. ● **1**: WAF allows requests that hit the rule. ● **2**: WAF only record requests that hit the rule.
status	Integer	Rule status. ● **true**: enabled. ● **false**: disabled.
description	String	Description
timestamp	Long	Time the rule is created.

Status code: 400

Table 4-281 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-282 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-283 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "02dafa406c4941368a1037b020f15a53",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "timestamp" : 1650534513775,
  "description" : "demo",
  "status" : 1,
  "geoip" : "US",
  "white" : 0,
  "geoTagList" : [ "US" ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3.17 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 4-284 Path Parameters

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

Table 4-285 Query Parameters

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

Parameter	Mandatory	Type	Description
page	No	Integer	Page number of the data to be returned during pagination query. The default value is **1**, indicating that the data on the first page is returned.
pagesize	No	Integer	Number of results on each page during pagination query. Value range: **1** to **100**. The default value is **10**, indicating that each page contains 10 results.

Request Parameters

Table 4-286 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).
Content-Type	Yes	String	Content type. Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-287 Response body parameters

Parameter	Type	Description
total	Integer	Total number of web tamper protection rules
items	Array of **AntiTamperRuleResponseBody** objects	Number of web tamper protection rules.

Table 4-288 AntiTamperRuleResponseBody

Parameter	Type	Description
id	String	Rule ID
policyid	String	ID of the protection policy that includes the rule
timestamp	Long	Timestamp the rule was created.
description	String	Rule remarks
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.
hostname	String	Domain name protected by the web tamper protection rule
url	String	URL protected by the web tamper protection rule

Status code: 400

Table 4-289 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-290 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-291 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "b77c3182957b46ed8f808a1998245cc4",
    "policyid" : "bdba8e224cbd4d11915f244c991d1720",
    "timestamp" : 1647499571037,
    "description" : "",
    "status" : 0,
    "hostname" : "www.demo.com",
    "url" : "/sdf"
  } ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3.18 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 4-292 Path Parameters

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

Table 4-293 Query Parameters

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

Request Parameters

Table 4-294 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 4-295 Request body parameters

Parameter	Mandatory	Type	Description
hostname	Yes	String	Protected websites. The list can be obtained by calling the **ListHost** API in cloud mode (the value of the **hostname** field in the response body).
url	Yes	String	URL protected by the web tamper protection rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/*. The asterisk ()* indicates the path prefix.
description	No	String	Rule Description

Response Parameters

Status code: 200

Table 4-296 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
hostname	String	Domain name protected by the web tamper protection rule
url	String	URL protected by the web tamper protection rule
description	String	Timestamp the rule was created.
status	Integer	Rule status. The value can be **0** or **1**. ● **0**: The rule is disabled. ● **1**: The rule is enabled.

Status code: 400

Table 4-297 Response body parameters

Parameter	Type	Description
error_code	String	Error code

Parameter	Type	Description
error_msg	String	Error message

Status code: 401

Table 4-298 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-299 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

{
  "hostname" : "www.demo.com",
  "url" : "/test",
  "description" : "demo"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "eed1c1e9c1b04b4bad4ba1186387a5d8",
  "policyid" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "timestamp" : 1650594937397,
  "description" : "demo",
  "status" : 1,
  "hostname" : "www.demo.com",
  "url" : "/test"
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3.19 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 4-300 Path Parameters

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

Table 4-301 Query Parameters

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

Request Parameters

Table 4-302 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 4-303 Response body parameters

Parameter	Type	Description
id	String	Rule ID
policyid	String	Policy ID
url	String	URL protected by the web tamper protection rule
timestamp	Long	Timestamp the rule was created.

Status code: 400

Table 4-304 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-305 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-306 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 1,
  "items" : [ {
    "id" : "b77c3182957b46ed8f808a1998245cc4",
    "policyid" : "bdba8e224cbd4d11915f244c991d1720",
    "policyname" : "demo",
    "timestamp" : 1647499571037,
    "description" : "",
    "status" : 0,
    "hostname" : "www.demo.com",
    "url" : "/sdf"
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.

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

Error Codes

See **Error Codes**.

4.3.20 Querying the Reference Table List

Function

This API is used to query the reference table list.

URI

GET /v1/{project_id}/waf/valuelist

Table 4-307 Path Parameters

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

Table 4-308 Query Parameters

Parameter	Mandatory	Type	Description
page	No	Integer	Page number of the data to be returned during pagination query. The default value is **1**, indicating that the data on the first page is returned.

Parameter	Mandatory	Type	Description
pagesize	No	Integer	Number of results on each page during pagination query. Value range: **1** to **100**. The default value is **10**, indicating that each page contains 10 results.
name	No	String	Reference table name

Request Parameters

Table 4-309 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 4-310 Response body parameters

Parameter	Type	Description
total	Integer	Number of reference tables Minimum: **0** Maximum: **500**
items	Array of **ValueListResponseBody** objects	Reference table list Array Length: **0 - 10**

Table 4-311 ValueListResponseBody

Parameter	Type	Description
id	String	ID of the reference table
name	String	Reference table name.
type	String	Reference table type Enumeration values: ● **url** ● **params** ● **ip** ● **cookie** ● **referer** ● **user-agent** ● **header** ● **response_code** ● **response_header** ● **response_body**
timestamp	Long	Reference table timestamp
values	Array of strings	Value of the reference table
producer	Integer	Reference table source. The value can be **1** or others. **1**: The table is created by you. Other values indicate that the table is automatically generated by moduleX.
description	String	Reference table description

Status code: 400

Table 4-312 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-313 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-314 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
GET https://{Endpoint}/v1/{project_id}/waf/valuelist?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 1,
  "items" : [ {
    "id" : "3b03be27a40b45d3b21fe28a351e2021",
    "name" : "ip_list848",
    "type" : "ip",
    "values" : [ "100.100.100.125" ],
    "timestamp" : 1650421866870,
    "producer" : 1,
    "description" : "demo"
  } ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3.21 Creating a Reference Table

Function

This API is used to add a reference table. A reference table can be used by CC attack protection rules and precise protection rules.

URI

POST /v1/{project_id}/waf/valuelist

Table 4-315 Path Parameters

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

Table 4-316 Query Parameters

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

Request Parameters

Table 4-317 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 4-318 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Reference table name. The value can contain a maximum of 64 characters. Only digits, letters, hyphens (-), underscores (_), and periods (.) are allowed. Minimum: **2** Maximum: **64**
type	Yes	String	Reference table type. For details, see the enumeration list. Minimum: **2** Maximum: **32** Enumeration values: ● **url** ● **params** ● **ip** ● **cookie** ● **referer** ● **user-agent** ● **header** ● **response_code** ● **response_header** ● **response_body**
values	Yes	Array of strings	Value of the reference table
description	No	String	Reference table description. The value contains a maximum of 128 characters. Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 4-319 Response body parameters

Parameter	Type	Description
id	String	ID of the reference table
name	String	Reference table name.
type	String	Reference table type
description	String	Reference table description
timestamp	Long	Reference table timestamp
values	Array of strings	Value of the reference table
producer	Integer	Source of the reference table. ● **1**: The reference table was created by you. ● **2**: The reference table was created by the intelligent access control protection.

Status code: 400

Table 4-320 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-321 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-322 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
POST https://{Endpoint}/v1/{project_id}/waf/valuelist?enterprise_project_id=0

{
  "name" : "demo",
  "type" : "url",
  "values" : [ "/124" ],
  "description" : "demo"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "e5d9032d8da64d169269175c3e4c2849",
  "name" : "demo",
  "type" : "url",
  "values" : [ "/124" ],
  "timestamp" : 1650524684892,
  "description" : "demo",
  "producer" : 1
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3.22 Modifying a Reference Table

Function

This API is used to modify a reference table.

URI

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

Table 4-323 Path Parameters

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

Table 4-324 Query Parameters

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

Request Parameters

Table 4-325 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 4-326 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Reference table name, which is a string of 2 to 32 characters. Minimum: **2** Maximum: **32**
type	Yes	String	Reference table type. For details, see the enumeration list. Minimum: **2** Maximum: **32** Enumeration values: ● **url** ● **params** ● **ip** ● **cookie** ● **referer** ● **user-agent** ● **header** ● **response_code** ● **response_header** ● **resopnse_body**
values	No	Array of strings	Value of the reference table
description	No	String	Reference table description. The value contains a maximum of 128 characters. Minimum: **0** Maximum: **128**

Response Parameters

Status code: 200

Table 4-327 Response body parameters

Parameter	Type	Description
id	String	ID of the reference table
name	String	Reference table name.
type	String	Reference table type
description	String	Reference table description
values	Array of strings	Value of the reference table
producer	Integer	Source of the reference table. ● **1**: The reference table was created by you. ● **2**: The reference table was created by the intelligent access control protection.

Status code: 400

Table 4-328 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-329 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-330 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
PUT https://{Endpoint}/v1/{project_id}/waf/valuelist/{valuelistid}?enterprise_project_id=0

{
  "name" : "RPmvp0m4",
  "type" : "response_code",
  "values" : [ "500" ],
  "description" : "demo"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "63b1d9edf2594743bc7c6ee98527306c",
  "name" : "RPmvp0m4",
  "type" : "response_code",
  "values" : [ "500" ],
  "description" : "demo",
  "producer" : 1
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3.23 Deleting a Reference Table

Function

This API is used to delete a reference table.

URI

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

Table 4-331 Path Parameters

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

Table 4-332 Query Parameters

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

Request Parameters

Table 4-333 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 4-334 Response body parameters

Parameter	Type	Description
id	String	ID of a reference table
name	String	Reference table name.
type	String	Reference table type
timestamp	Long	Time the reference table is deleted. The value is a 13-digit timestamp in millisecond.

Status code: 400

Table 4-335 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-336 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-337 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
DELETE https://{Endpoint}/v1/{project_id}/waf/valuelist/{valuelistid}?enterprise_project_id=0
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "63b1d9edf2594743bc7c6ee98527306c",
  "name" : "RPmvp0m4",
  "type" : "response_code",
  "timestamp" : 1640938602391
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.4 Certificate Management

4.4.1 Querying the List of Certificates

Function

This API is used to query the list of certificates.

URI

GET /v1/{project_id}/waf/certificate

Table 4-338 Path Parameters

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

Table 4-339 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the **ListEnterpriseProject** API of EPS.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is **1**, indicating that the data on the first page is returned. Default: **1**
pagesize	No	Integer	Number of results on each page during pagination query. Value range: **1** to **100**. The default value is **10**, indicating that each page contains 10 results. Default: **10**
name	No	String	Certificate name
host	No	Boolean	Whether to obtain the domain name for which the certificate is used. The default value is **false**. ● **true**: Obtain the certificates that have been used for domain names. ● **false**: Obtain the certificates that have not been used for any domain name. Default: **false**

Parameter	Mandatory	Type	Description
exp_status	No	Integer	Certificate status. The options are as follows: 0: not expired; 1: expired; 2: about to expire (The certificate will expire within one month.)

Request Parameters

Table 4-340 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 4-341 Response body parameters

Parameter	Type	Description
items	Array of **CertificateBody** objects	Certificates
total	Integer	Total number of certificates

Table 4-342 CertificateBody

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

Parameter	Type	Description
exp_status	Integer	Certificate status. The value can be: **0**: The certificate is valid. **1**: The certificate has expired. **2**: The certificate will expire within one month.
timestamp	Long	Certificate upload timestamp.
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-343 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-344 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-345 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-346 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
GET https://{Endpoint}/v1/{project_id}/waf/certificate?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "dc443ca4f29c4f7e8d4adaf485be317b",
    "name" : "demo",
    "timestamp" : 1643181401751,
    "expire_time" : 1650794100000,
    "bind_host" : [ ],
    "exp_status" : 2
  } ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.4.2 Uploading a Certificate

Function

This API is used to upload a certificate.

URI

POST /v1/{project_id}/waf/certificate

Table 4-347 Path Parameters

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

Table 4-348 Query Parameters

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

Request Parameters

Table 4-349 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 4-350 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Certificate name. The value can contain a maximum of 64 characters. Only digits, letters, hyphens (-), underscores (_), and periods (.) are allowed.
content	Yes	String	Certificate file. Only certificates and private key files in PEM format are supported, and the newline characters in the file must be replaced with \n.
key	Yes	String	Certificate private key. Only certificates and private key files in PEM format are supported, and the newline characters in the files must be replaced with \n.

Response Parameters

Status code: 200

Table 4-351 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
content	String	Certificate file, PEM encoding
key	String	Private key of the certificate, which is in PEM format.
expire_time	Long	Certificate expiration timestamp
exp_status	Integer	Certificate status. The options can be: **0**: The certificate has not expired. **1**: The certificate expired. **2**: The certificate is about to expire.
timestamp	Long	Certificate upload timestamp
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-352 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-353 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-354 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-355 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
POST https://{Endpoint}/v1/{project_id}/waf/certificate?enterprise_project_id=0
```

```
{
  "name" : "demo",
  "content" : "-----BEGIN CERTIFICATE----- \
\nMIIDyzCCArOgAwIBAgIJAN5U0Z4Bh5ccMA0GCSqGSIb3DQEBCwUAMHwxCzAJBgNV
BAYTAlpIMRIwEAYDVQQIDAlHVUFOR0RPTkcxETAPBgNVBAcMCERPTkdHVUFOMQ0w
CwYDVQQKDARERUtFMQswCQYDVQQLDAJESzELMAkGA1UEAwwCT0QxHTAbBgkqhkiG
9w0BCQEWDk8IZC5odWF3ZWkuY29tMB4XDTIxMTExNTA4MTk0MVoXDTIyMTExNTA4
MTk0MVowfDELMAkGA1UEBhMCWkgxEjAQBgNVBAgMCUdVQU5HRE9ORzERMA8GA1UE
BwwIRE9OR0dVQU4xDTALBgNVBAoMBERFS0UxCzAJBgNVBAsMAkRLMQswCQYDVQQD
DAJPRDEdMBsGCSqGSIb3DQEJARYOTwhkLmh1YXdlaS5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDcoLFK62//r0RHFyweYBj97S4NsJ8Qj0RG+Y02
OgwhQmRiNNjubJwP8Nqqyd86zr+fsSQxKBaBCosn1PcN2Pj2vPJD6NEk4I6VdOWr /
kFYMlOcimhSfW4wt6VakniOKIYGrCxxvQe1X2OyBxT+ocTLRgEIB8ZbvJyPNseg
feLEUuPYRpQ5kXLgJH2/3NwZFOgBHVv/b07l4fR+sWJMnIA2yIjSBQ0DEAOSusXo FQ/
WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi8L+mKeRL+lcMMbXC/3k6OfMB
tVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9sE+tmJZTPH6lYtAgMBAAGjUDBOMB0G
A1UdDgQWBBQprUUFXW+gIkpzXdrYlsWjfSahWjAfBgNVHSMEGDAWgBQprUUFXW+g
IkpzXdrYlsWjfSahWjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQA2
603KozsQoIKeLvqDJlcAXwWRfNW8SvlaSJAulhHgneMt9bQgIL+3PJWA/iMniOhU o/
kVwkiUIcxw4t7RwP0hVms0OZw59MuqKd3oCSWkYO4vEHs3t40JDWnGDnmQ4sol
RkOWJwL4w8tnPe3qY9JSupjlsu6Y1hlvKtEfN2vEKFnsuMhidkUpUAJWodHhWBQH
wgIDo4/6yTnWZNGK8JDal86Dm5IchXea1EoYBJsHxiJb7HeWQlkre+MCYi1RHOin 4mIXTr0oT4/jWlgklSz6/
ZhGRq+7W7tIl7cvzCe+4XsVZIenAcYoNd/WLfo91PD4 yAsRXrOjW1so1Bj0BkDz\\n -----END CERTIFICATE-----",
  "key" : "-----BEGIN PRIVATE KEY----- \
\nMIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDcoLFK62//r0RH FyweYBj97S4NsJ8Qj0RG
+Y02OgwhQmRiNNjubJwP8Nqqyd86zr+fsSQxKBaBCosn 1PcN2Pj2vPJD6NEk4I6VdOWr/
kFYMlOcimhSfW4wt6VakniOKIYGrCxxvQe1X2Oy BxT
+ocTLRgEIB8ZbvJyPNsegfeLEUuPYRpQ5kXLgJH2/3NwZFOgBHVv/b07l4fR+ sWJMnIA2yIjSBQ0DEAOSusXoFQ/
WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi 8L+mKeRL+lcMMbXC/
3k6OfMBtVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9sE+tmJ ZTPH6lYtAgMBAAECggEBAL+xZxm/QoqXT
+2stoqV2GEYaMFASpRqxlocjZMmEE/9 jZa+cBWIjHhVPsjRqYFBDcHEebu0JwlrjcjIAvgnIvnO5XgXm1A9Q
+WbscokmcX1 xCvpHgc+MDVn+uWdCd4KW5kEk4EnSsFN5iNSf+1VxNURN+gwSSp/0E+muwA5IISO G6HQ
+p6qs52JAitX5t/7ruKoHYXJxBnf7TUs7768qrh++KPKpPlq044qoYlcGO1n 4urPBHuNLy04GgGw
+vkaqjqOvZrNLVOMMaFWBxsDWBehgSSBQTj+f3NCxneGYtt8 3SCTZQI5nIkb+r/
M455EwKTSXuEsNHoIwx7L6GEPbQECgYEA8IxgK2fYykloICoh
TFJaRAvyjyKa2+Aza4qT9SGY9Y30VPClPjBB1vUu5M9KrFufzlv06nGEcHmpEwOe
8vbRu7nLAQTGYFi8VK63q8w6FlFdAyCG6Sx+BWCfWxJzXsZLAJTfklwi8HsOSlqh
6QNv0xbE2fLjXKf8MHvtrufip40CgYEA6sy87eDrkVgtq4ythAik3i1C5Z3v0fvx mTblG52Z21OyocNq3Tf/
b1ZwoIc1ik6cyBzY6z1bIrbSzArCqm0sb2iD+kJL81O0 /qqdXjBxZUkKiVAMNNp7xJGZHHFKWUxT2+UX/
tlyx4tT4dzrFIkdDXkcMmqfsRxd 1NEVaAaT8SECgYAoU7BPtpIun43YTpfUfr3pSIN6oZeKoxSbw9i4MNC
+4fSDRPC+ 80ImcmZRL7taF+Y7p0jxAOTuIkdJC8NbAiv5J9WzrwQ+5MF2BPB/2bYnRa6tNofH kZDy/
9bXYsl6qw2p5Ety8wVcgZTMvFMGiG/32IpZ65FYWEU8L5qSRwfFhQKBgQC9 ihjZTj/bTHtRiHZppzCvyYm/Igd
+Uwtsy0uXR1n0G1SQENgrTBD/J6AzdfJae6tE P0U8YIM5Oqxf2i/as9ay+IPRecMl4eSxz7jJWAGx6Yx/3AZ
+hAB1ZbNbqniCLYNk d0MvjwmA25ATO+ro4OZ7AdEpQbk3l9aG/WFyYBz9AQKBgQCucFPA1l5eslL8196V
WMr2Qo0tqzl7CGSoWQk2Sa2HZtZdfofXAaaqo+zvJ6RPHtJh0jgJtx536DVV3egI
37YrdQyJbCPZXQ3SPgqWCorUnXBwq/nxS06uwu6JBxUFc57ijmMU4fWYNrvkkmWb 7keAg/
r5Uy1joMAvBN1I6lB8pg==\\n -----END PRIVATE KEY-----"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "64af92e2087d49cbabc233e9bdc761b7",
  "name" : "testly",
  "timestamp" : 1658994431596,
  "expire_time" : 1682394560000
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.4.3 Querying a Certificate

Function

This API is used to query a certificate.

URI

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

Table 4-356 Path Parameters

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

Table 4-357 Query Parameters

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

Request Parameters

Table 4-358 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).
Content-Type	Yes	String	Content type. Default: **application/json;charset=utf8**

Response Parameters

Status code: 200

Table 4-359 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
content	String	Certificate file, PEM encoding
key	String	Private key of the certificate, which is in PEM format.
expire_time	Long	Certificate expiration timestamp.
exp_status	Integer	Certificate status. The options can be: **0**: The certificate has not expired. **1**: The certificate expired. **2**: The certificate is about to expire.
timestamp	Long	Certificate upload timestamp
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-360 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-361 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-362 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-363 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
GET https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "id" : "6e2be127b79f4a418414952ad5d8c59f",
  "name" : "certificatename94319",
  "content" : "-----BEGIN CERTIFICATE-----\nMIIB
+TCCAaOgAwIBAgIUJP9I8OupQ77w0bGL2yWOQXreM4kwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMC
QVUxEzARBgNVBAgMClNvbWUtU3RhdGUxDzANBgNVBAoMBkh1YXdlaTEcMBoGA1UEAwwTd2FmLmh1YXdl
aWNsb3VkLmNvbTAeFw0yMDA3MDkwNTQ2MDRaFw0yMDA4MDgwNTQ2MDRaMFExCzAJBgNVBAYTAkFV
MRMwEQYDVQQIDApTb21lLVN0YXRlMQ8wDQYDVQQKDAZIdWF3ZWkxHDAaBgNVBAMME3dhZi5odWF3Z
WljbG91ZC5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIAkEA0UEbMzbvgOJTKrKcDUw9xjFqxM7BaQFM3SLs
QlmD5hkzygyL1ra
+cWajPJlTCxz9Ph6qldna2+OrIuTdvCcpjwIDAQABo1MwUTAdBgNVHQ4EFgQUE7ZQNcgl3lmryx1s5gy9mnC1rs
YwHwYDVR0jBBgwFoAUE7ZQNcgl3lmryx1s5gy9mnC1rsYwDwYDVR0TAQH/BAUwAwEB/
zANBgkqhkiG9w0BAQsFAANBAM5wGi88jYWLgOnGbae5hH3I9lMBKxGqv17Cbm1tjWuUogVINz86lqvCpuhzLv
D/vzJAqPIuDwqM8uvzjgRfZs8=\n-----END CERTIFICATE-----",
  "key" : "-----BEGIN RSA PRIVATE KEY-----
\nMIIBOQIBAAJBANFBGzM274DiUyqynA1MPcYxasTOwWkBTN0i7EJZg+YZM8oMi9a2vnFmozyZUwsc/
T4eqpXZ2tvjqyLk3bwnKY8CAwEAAQJBAI7LMPaH/HQk/b/bVmY0qsr
+me9nb9BqFLuqwzKbx0hSmWPOWFsd3rOFlSopyHqgYtAsPfvPumEdGbdnCyU8zAECIQD71768K1ejb
+ei2lqZqHaczqdUNQxMh54yot9F2yVWjwIhANS1Y1Jv89WEU/ZvvMS9a4638Msv2c4GGp08RtXNYn0BAiA0H4b
+cwoEbZjHf+HYg6Fo+uxu5TvSaw8287a6Qo0LyQIfVZSlYYWplT6oiX5rdLzBiap4N0gJWdsa2ihmV59LAQIgK8N
+j1daq63b0bJ9k4HruhQtpgxI6U9nFBemH4zTRYM=\n-----END RSA PRIVATE KEY-----",
  "timestamp" : 1650595334578,
  "expire_time" : 1596865564000,
  "bind_host" : [ {
    "id" : "978b411657624c2db069cd5484195d1c",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud"
  } ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.4.4 Modifying a Certificate

Function

This API is used to modify a certificate.

URI

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

Table 4-364 Path Parameters

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

Table 4-365 Query Parameters

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

Request Parameters

Table 4-366 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 4-367 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Certificate name. The value can contain a maximum of 64 characters. Only digits, letters, hyphens (-), underscores (_), and periods (.) are allowed.
content	No	String	Certificate file. Only certificates and private key files in PEM format are supported, and the newline characters in the file must be replaced with \n.
key	No	String	Certificate private key. Only certificates and private key files in PEM format are supported, and the newline characters in the files must be replaced with \n.

Response Parameters

Status code: 200

Table 4-368 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
expire_time	Long	Timestamp when the certificate expires
timestamp	Long	Timestamp.

Status code: 400

Table 4-369 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-370 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-371 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
PUT https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?enterprise_project_id=0

{
  "name" : "demo"
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "360f992501a64de0a65c50a64d1ca7b3",
  "name" : "demo",
  "timestamp" : 1650593797892,
  "expire_time" : 1596865564000
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.4.5 Deleting a Certificate

Function

This API is used to delete a certificate.

URI

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

Table 4-372 Path Parameters

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

Table 4-373 Query Parameters

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

Request Parameters

Table 4-374 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 4-375 Response body parameters

Parameter	Type	Description
id	String	Certificate ID
name	String	Certificate name
content	String	Certificate file, PEM encoding
key	String	Private key of the certificate in PEM format
expire_time	Long	Certificate expiration timestamp
exp_status	Integer	Certificate status. The options can be: **0**: The certificate has not expired. **1**: The certificate expired. **2**: The certificate is about to expire.
timestamp	Long	Certificate upload timestamp
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-376 BindHost

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	Deployment mode of WAF instance that is used for the domain name. The value can be **cloud** for cloud WAF or **premium** for dedicated WAF instances.
mode	String	This parameter is required only by the dedicated mode.

Status code: 400

Table 4-377 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-378 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-379 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
DELETE https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

OK

```
{
  "id" : "e1d87ba2d88d4ee4a3b0c829e935e5e0",
  "name" : "certificatename29556",
  "timestamp" : 1650594410630,
  "expire_time" : 1596865564000
}
```

Status Codes

Status Code	Description
200	OK

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

Error Codes

See **Error Codes**.

4.4.6 Applying a Certificate to a Domain Name

Function

This API is used to apply a certificate to a domain name.

URI

POST /v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts

Table 4-380 Path Parameters

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

Table 4-381 Query Parameters

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

Request Parameters

Table 4-382 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 4-383 Request body parameters

Parameter	Mandatory	Type	Description
cloud_host_ids	No	Array of strings	ID of HTTPS domain name in cloud mode. You can obtain it by calling the **ListHost** API.
premium_host_ids	No	Array of strings	ID of the HTTPS domain name in dedicated mode. You can obtain it by calling the **ListPremiumHost** API.

Response Parameters

Status code: 200

Table 4-384 Response body parameters

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name
timestamp	Long	Timestamp.
expire_time	Long	Expiration date
bind_host	Array of **CertificateBundingHostBody** objects	Domain name list

Table 4-385 CertificateBundingHostBody

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name
waf_type	String	WAF mode (Cloud: cloud; Dedicated: premium) Enumeration values: ● **cloud** ● **premium**

Status code: 400

Table 4-386 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-387 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-388 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
POST https://{Endpoint}/v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts?
enterprise_project_id=0
```

```
{
  "cloud_host_ids" : [ "85e554189d494c0f97789e93531c9f90" ],
  "premium_host_ids" : [ "4e9e97c425fc463c8f374b90124e8392" ]
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "3ac1402300374a63a05be68c641e92c8",
  "name" : "www.abc.com",
  "timestamp" : 1636343349139,
  "expire_time" : 1650794100000,
  "bind_host" : [ {
    "id" : "e350cf556da34adab1f017523d1c05ed",
    "hostname" : "www.demo.com",
    "waf_type" : "cloud",
    "bandwidth" : 0,
    "qps" : 0
  } ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.5 Event Management

4.5.1 Querying the List of Attack Events

Function

This API is used to query the attack event list. Currently, this API does not support query of all protection events. The **pagesize** parameter cannot be set to **-1**. The larger the data volume, the larger the memory consumption. A maximum of 10,000 data records can be queried. For example, if the number of data records in a user-defined period exceeds 10,000, the data whose page is 101 (or **pagesize** is greater than 100) cannot be queried. You need to adjust the time range to a longer period and then query the data.

URI

GET /v1/{project_id}/waf/event

Table 4-389 Path Parameters

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

Table 4-390 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the **ListEnterpriseProject** API of EPS.
recent	No	String	Time range for querying logs. This parameter cannot be used together with **from** or **to** at the same time. Parameter **recent** must be used with either **from** or **to**. Enumeration values: ● **yesterday** ● **today** ● **3days** ● **1week** ● **1month**
from	No	Long	Start time (13-digit timestamp). This parameter must be used together with to, but cannot be used together with recent.
to	No	Long	End time (13-digit timestamp). This parameter must be used together with from but cannot be used together with recent.

Parameter	Mandatory	Type	Description
attacks	No	Array	Attack type ● **vuln**: other attack types ● **sqli**: SQL injection attacks ● **lfi**: local file inclusion ● **cmdi**: command injection attacks ● **xss**: XSS attacks ● **robot**: malicious crawler ● **rfi**: remote file inclusion ● **custom_custom**: attack hit the precision protection rule ● **cc**: CC attacks ● **webshell**: website Trojan ● **custom_whiteblackip**: attacks that hit the blocklist and trustlist rule ● **custom_geoip**: attacks that hit the geolocation access control rule ● **antitamper**: attacks that hit the web tamper prevention rule ● **anticrawler**: attacks that hit the anti-crawler rules ● **leakage**: attacks that hit the information leakage prevention rule ● **illegal**: illegal requests
hosts	No	Array	Domain name ID. It can be obtained by calling the **ListHost API.
page	No	Integer	Page number of the data to be returned during pagination query. The default value is **1**, indicating that the data on the first page is returned.
pagesize	No	Integer	Number of results on each page during pagination query. Value range: **1** to **100**. The default value is **10**, indicating that each page contains 10 results.

Request Parameters

Table 4-391 Request header parameters

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

Response Parameters

Status code: 200

Table 4-392 Response body parameters

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

Table 4-393 ListEventItems

Parameter	Type	Description
id	String	Event ID
time	Long	Count
policyid	String	Policy ID
sip	String	Source IP address, which is the IP address of the web visitor (attacker's IP address).
host	String	Attacked domain name
url	String	Attacked URL

Parameter	Type	Description
attack	String	Attack type - **vuln**: other attack types - **sqli**: SQL injection attack - **lfi**: local file inclusion - **cmdi**: command injection attacks - **XSS**: XSS attacks - **robot**: malicious crawler - **rfi**: remote file inclusion - **custom_custom**: attacks hit a precise protection rule - **webshell**: Trojan - **custom_whiteblackip**: attacks hit a blacklist or whitelist rule - **custom_geoip**: attacks hit a geolocation access control rule - **antitamper**: attacks hit a web tamper prevention rule - anticrawler: attacks hit an anti-crawler rule - **leakage**: attacks hit an information leakage prevention rule - **illegal**: invalid requests
rule	String	ID of the matched rule
payload	String	Hit payload
payload_location	String	Hit Load Position
action	String	Protective action
request_line	String	Request method and path
headers	Object	HTTP request header
cookie	String	Request cookie
status	String	Response code status
process_time	Integer	Processing time
region	String	Geographical location
host_id	String	Domain name ID
response_time	Long	Time to response
response_size	Integer	Response body size

Parameter	Type	Description
response_body	String	Response body
request_body	String	Request body

Status code: 400

Table 4-394 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-395 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-396 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
GET https://{Endpoint}/v1/{project_id}/waf/event?
enterprise_project_id=0&page=1&pagesize=10&recent=today
```

Example Responses

Status code: 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "04-0000-0000-0000-21120220421152601-2f7a5ceb",
    "time" : 1650525961000,
    "policyid" : "25f1d179896e4e3d87ceac0598f48d00",
    "host" : "x.x.x.x:xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "url" : "/osclass/oc-admin/index.php",
    "attack" : "lfi",
    "rule" : "040002",
    "payload" : " file=../../../../../../../../../../etc/passwd",
    "payload_location" : "params",
    "sip" : "x.x.x.x",
    "action" : "block",
    "request_line" : "GET /osclass/oc-admin/index.php?
page=appearance&action=render&file=../../../../../../../../../../etc/passwd",
    "headers" : {
      "accept-language" : "en",
      "ls-id" : "xxxxx-xxxxx-xxxx-xxxx-9c302cb7c54a",
      "host" : "x.x.x.x",
      "lb-id" : "2f5f15ce-08f4-4df0-9899-ec0cc1fcdc52",
      "accept-encoding" : "gzip",
      "accept" : "*/*",
      "user-agent" : "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
35.0.2309.372 Safari/537.36"
    },
    "cookie" : "HWWAFSESID=2a1d773f9199d40a53; HWWAFSESTIME=1650525961805",
    "status" : "418",
    "host_id" : "6fbe595e7b874dbbb1505da3e8579b54",
    "response_time" : 0,
    "response_size" : 3318,
    "response_body" : "",
    "process_time" : 2,
    "request_body" : "{}"
  } ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.5.2 This API is used to query details about an event of a specified ID.

Function

Querying Details About an Event of a Specified ID

URI

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

Table 4-397 Path Parameters

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

Table 4-398 Query Parameters

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

Request Parameters

Table 4-399 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 4-400 Response body parameters

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

Table 4-401 ShowEventItems

Parameter	Type	Description
time	Long	Timestamp when the attack occurs, in milliseconds.
policyid	String	ID of the policy
sip	String	Source IP address
host	String	Domain name
url	String	Attacked URL
attack	String	Attack type
rule	String	ID of the hit rule
action	String	Protective action
cookie	String	Cookie of the attack request
headers	Object	Header of the attack request
host_id	String	ID of the attacked domain name
id	String	Event ID
payload	String	Malicious load
payload_location	String	Malicious load location
region	String	Geographical location of the source IP address
process_time	Integer	Processing time
request_line	String	Body of the attack request
response_size	Integer	Response body size (byte)
response_time	Long	Response time (ms)
status	String	Response code
request_body	String	Request body

Status code: 400

Table 4-402 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-403 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-404 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

```
GET https://{Endpoint}/v1/{project_id}/waf/event{event_id}?enterprise_project_id=0
```

Example Responses

Status code: 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "09-0000-0000-0000-12120220421093806-a60a6166",
    "time" : 1650505086000,
    "policyid" : "173ed802272a4b0798049d7edffeff03",
    "host" : "x.x.x.x:xxxxxx-xxx-xxx-xxx-xxxxxxxxx",
    "url" : "/mobile/DBconfigReader.jsp",
    "attack" : "vuln",
    "rule" : "091004",
    "payload" : " /mobile/dbconfigreader.jsp",
    "payload_location" : "uri",
    "sip" : "x.x.x.x",
    "action" : "block",
    "request_line" : "GET /mobile/DBconfigReader.jsp",
    "headers" : {
      "ls-id" : "c0d957e6-26a8-4f2e-8216-7fc9332a250f",
      "host" : "x.x.x.x:81",
      "lb-id" : "68d3c435-2607-45e0-a5e2-38980544dd45",
      "accept-encoding" : "gzip",
      "user-agent" : "Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 CSIRTx/2022"
    },
    "cookie" : "HWWAFSESID=2a0bf76a111c93926d; HWWAFSESTIME=1650505086260",
    "status" : "418",
    "region" : "Reserved IP",
    "host_id" : "e093a352fd3a4ddd994c585e2e1dda59",
    "response_time" : 0,
    "response_size" : 3318,
    "process_time" : 0,
    "request_body" : "{}"
  } ]
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.6 Querying the Domain Name of a Tenant

4.6.1 Querying Domain Names Protected with All WAF Instances

Function

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

URI

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

Table 4-405 Path Parameters

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

Table 4-406 Query Parameters

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

Parameter	Mandatory	Type	Description
protect_status	No	Integer	WAF status of the protected domain name. ● **-1**: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
waf_type	No	String	WAF mode of the domain name
is_https	No	Boolean	Whether HTTPS is used for the domain name

Request Parameters

Table 4-407 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 4-408 Response body parameters

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

Table 4-409 CompositeHostResponse

Parameter	Type	Description
id	String	- **false**: The exclusive IP address is not practical.
hostid	String	Domain name ID
hostname	String	Domain name added to cloud WAF.
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	WAF status of the protected domain name. - **-1**: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. - **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. - **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be **0** or **1**. **0**: The website traffic has not been routed to WAF. **1**: The website traffic has been routed to WAF.
proxy	Boolean	Whether a proxy is used for the protected domain name. - **false**: No proxy is used. - **true**: A proxy is used.

Parameter	Type	Description
timestamp	Long	Time the domain name was added to WAF.
paid_type	String	Package-based payment mode. Currently, only the prepaid mode is supported.
flag	**Flag** object	Special identifier, which is used on the console.
waf_type	String	Mode of WAF that is used to protection the domain name. The value can be **cloud** or **premium**. **cloud**: The cloud WAF is used to protect the domain. **premium**: A dedicated WAF instance is used to protect the domain name.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
premium_waf_instances	Array of **Premium_waf_instances** objects	List of dedicated WAF instances
description	String	Domain name description
exclusive_ip	Boolean	Whether to use a dedicated IP address.This parameter is reserved and can be ignored. ● **true**: Use a dedicated IP address. ● **false**: Do not use a dedicated IP address.
region	String	Region ID. This parameter is included when the domain name was added to WAF through the console. This parameter is left blank when the domain name was added to WAF by calling an API. You can query the region ID on the Regions and Endpoints page on the Cloud website.

Table 4-410 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. - **true**: The website passed the PCI 3DS certification check. - **false**: The website failed the PCI 3DS certification check. Enumeration values: - **true** - **false**
pci_dss	String	Whether the website passed the PCI DSS certification check. - **true**: The website passed the PCI DSS certification check. - **false**: The website failed the PCI DSS certification check. Enumeration values: - **true** - **false**
cname	String	The CNAME record being used. - **old**: The old CNAME record is used. - **new**: The new CNAME record is used. Enumeration values: - **old** - **new**
is_dual_az	String	Whether WAF support Multi-AZ DR - **true**: WAF supports multi-AZ DR. - **false**: WAF does not support multi-AZ DR. Enumeration values: - **true** - **false**
ipv6	String	Whether IPv6 protection is supported. - **true**: IPv6 protection is supported. - **false**: IPv6 protection is not supported. Enumeration values: - **true** - **false**

Table 4-411 Premium_waf_instances

Parameter	Type	Description
id	String	ID of the dedicated WAF instance
name	String	Name of the dedicated WAF instance
accessed	Boolean	Whether the domain name is added to the dedicated WAF instance. The options are **true** and **false**. ● **true**: The domain name has been added to WAF. ● **false**: The domain name has not been added to WAF.

Status code: 400

Table 4-412 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-413 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-414 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

OK

```
{
  "items" : [ {
    "id" : "31af669f567246c289771694f2112289",
    "hostid" : "31af669f567246c289771694f2112289",
    "description" : "",
    "proxy" : false,
    "flag" : {
      "pci_3ds" : "false",
      "pci_dss" : "false",
      "ipv6" : "false",
      "cname" : "new",
      "is_dual_az" : "true"
    },
    "region" : "xxxxxx-xx",
    "hostname" : "www.demo.com",
    "access_code" : "1b18879b9d064f8bbcbf8abce7294cac",
    "policyid" : "41cba8aee2e94bcdbf57460874205494",
    "timestamp" : 1650527546454,
    "protect_status" : 0,
    "access_status" : 0,
    "exclusive_ip" : false,
    "web_tag" : "",
    "paid_type" : "prePaid",
    "waf_type" : "cloud"
  } ],
  "total" : 1,
  "cloud_total" : 1,
  "premium_total" : 0
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.6.2 Querying a Domain Name by ID

Function

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

URI

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

Table 4-415 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Cloud management console and hover the cursor over your username. On the displayed window, choose **My Credentials**.Then, in the **Projects** area, view **Project ID** of the corresponding project.
host_id	Yes	String	Domain name ID. In the cloud mode, it can be obtained by calling the ListHost API. In the dedicated mode, it can be obtained by calling the **ListPremiumHost** API.

Table 4-416 Query Parameters

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

Request Parameters

Table 4-417 Request header parameters

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

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

Response Parameters

Status code: 200

Table 4-418 Response body parameters

Parameter	Type	Description
id	String	● **false**: The exclusive IP address is not practical.
hostid	String	Domain name ID
hostname	String	Domain name added to cloud WAF.
policyid	String	Policy ID
access_code	String	CNAME prefix
protect_status	Integer	WAF status of the protected domain name. ● **-1**: The WAF protection is bypassed. Requests of the domain name are directly sent to the backend server and do not pass through WAF. ● **0**: The WAF protection is suspended. WAF only forwards requests destined for the domain name and does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the policy you configure.
access_status	Integer	Domain name access status. The value can be **0** or **1**. **0**: The website traffic has not been routed to WAF. **1**: The website traffic has been routed to WAF.
proxy	Boolean	Whether a proxy is used for the protected domain name. ● **false**: No proxy is used. ● **true**: A proxy is used.
timestamp	Long	Time the domain name was added to WAF.
paid_type	String	Package-based payment mode. Currently, only the prepaid mode is supported.

Parameter	Type	Description
flag	**Flag** object	Special identifier, which is used on the console.
waf_type	String	Mode of WAF that is used to protection the domain name. The value can be **cloud** or **premium**. **cloud**: The cloud WAF is used to protect the domain. **premium**: A dedicated WAF instance is used to protect the domain name.
web_tag	String	Website name, which is the same as the website name in the domain name details on the WAF console.
premium_waf_instances	Array of **Premium_waf_instances** objects	List of dedicated WAF instances
description	String	Domain name description
exclusive_ip	Boolean	Whether to use a dedicated IP address.This parameter is reserved and can be ignored. ● **true**: Use a dedicated IP address. ● **false**: Do not use a dedicated IP address.
region	String	Region ID. This parameter is included when the domain name was added to WAF through the console. This parameter is left blank when the domain name was added to WAF by calling an API. You can query the region ID on the Regions and Endpoints page on the Cloud website.

Table 4-419 Flag

Parameter	Type	Description
pci_3ds	String	Whether the website passes the PCI 3DS certification check. ● **true**: The website passed the PCI 3DS certification check. ● **false**: The website failed the PCI 3DS certification check. Enumeration values: ● **true** ● **false**

Parameter	Type	Description
pci_dss	String	Whether the website passed the PCI DSS certification check. - **true**: The website passed the PCI DSS certification check. - **false**: The website failed the PCI DSS certification check. Enumeration values: - **true** - **false**
cname	String	The CNAME record being used. - **old**: The old CNAME record is used. - **new**: The new CNAME record is used. Enumeration values: - **old** - **new**
is_dual_az	String	Whether WAF support Multi-AZ DR - **true**: WAF supports multi-AZ DR. - **false**: WAF does not support multi-AZ DR. Enumeration values: - **true** - **false**
ipv6	String	Whether IPv6 protection is supported. - **true**: IPv6 protection is supported. - **false**: IPv6 protection is not supported. Enumeration values: - **true** - **false**

Table 4-420 Premium_waf_instances

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

Parameter	Type	Description
accessed	Boolean	Whether the domain name is added to the dedicated WAF instance. The options are **true** and **false**. ● **true**: The domain name has been added to WAF. ● **false**: The domain name has not been added to WAF.

Status code: 400

Table 4-421 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 401

Table 4-422 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Status code: 500

Table 4-423 Response body parameters

Parameter	Type	Description
error_code	String	Error code
error_msg	String	Error message

Example Requests

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

Example Responses

Status code: 200

OK

```
{
  "id" : "31af669f567246c289771694f2112289",
  "hostid" : "31af669f567246c289771694f2112289",
  "description" : "",
  "proxy" : false,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false",
    "ipv6" : "false",
    "cname" : "new",
    "is_dual_az" : "true"
  },
  "region" : "xx-xxxx-x",
  "hostname" : "www.demo.com",
  "access_code" : "1b18879b9d064f8bbcbf8abce7294cac",
  "policyid" : "41cba8aee2e94bcdbf57460874205494",
  "timestamp" : 1650527546454,
  "protect_status" : 0,
  "access_status" : 0,
  "exclusive_ip" : false,
  "web_tag" : "",
  "paid_type" : "prePaid",
  "waf_type" : "cloud"
}
```

Status Codes

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

Error Codes

See **Error Codes**.

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.00011016	name.duplicate	Duplicated name.	Change the name.

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00012001	invalid.token	Illegal token	Check whether the token is correct
400	WAF.00012002	invalid.project	Inconsistency between project_id and token	Check consistency of project_id and token
400	WAF.00012003	permission.denied	No permission	Assign WAF required permissions to account
400	WAF.00012004	account.frozen	Account freezing	Account unfreezing
400	WAF.00012005	not.subscribe	Unsubscribed	Subscribe to WAF service first
400	WAF.00012006	pdp.permission.denied	No permission	Check the PDP authority of the account
400	WAF.00012007	jwt.authentication.disabled	JWT certification off	Open JWT certification
400	WAF.00012008	jwt.authentication.invalid.token	Illegal JWT token	Check whether the account has JWT permission
400	WAF.00012009	jwt.authentication.failed	JWT authentication failed	Give the account authorization first
400	WAF.00012010	eps.all.not.support	eps.all.not.support	Open the write permission of enterprise project
400	WAF.00013001	insufficient.quota	Insufficient function quota	Purchase function quota upgrade package
400	WAF.00013002	feature.not.support	Function not supported	nothing
400	WAF.00013003	port.not.support	Port not supported	Port conversion via ELB
400	WAF.00013004	protocol.not.support	Protocol not supported	Through ELB conversion protocol

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00013005	wildcard.domain.not.support	Pan domain name not supported	Use specific domain names
400	WAF.00013006	ipv6.not.support	IPv6 is not supported	The current version does not support IPv6
400	WAF.00013007	insufficient.tenant.quota	insufficient.tenant.quota	Purchase quota upgrade package
400	WAF.00014001	resource.not.found	Resource not found	The resource has been deleted or does not exist
400	WAF.00014002	resource.already.exists	Resource already exists	Resource already exists
400	WAF.00014003	open.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 English grammar for description
400	WAF.00021017	incorrect.rule.config	Incorrect rule configuration	It is recommended to configure protection rules according to the documentation in the help center
400	WAF.00021018	incorrect.reference.table.config	Incorrect reference table configuration	It is recommended to configure the reference table according to the documentation in the help center
400	WAF.00021019	incorrect.route.config	Incorrect line configuration	It is recommended to configure the line according to the documentation in the help center

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00021020	offsetOrLimit.illegal	Paging parameter error	It is recommended to fill in pagination parameters according to the documents in the help center
400	WAF.00021021	param.exceed.limit	Parameter exceeds limit	It is recommended to view the parameter limits according to the documentation in the help center
400	WAF.00022002	resource.already.exists	Resource already exists	It is recommended to check whether the created resource already exists in the console
400	WAF.00022003	resource.is.being.used	The resource is in use	Remove the relationship between the resource and the user before deleting the resource
400	WAF.00022004	rule.conflict	Rule conflict	Check whether the target rule conflicts with the existing rule
403	WAF.00013014	insufficient.policy.quota	Insufficient policy quota	Purchase the domain name expansion package or upgrade the specification
403	WAF.00022005	insufficient.quota	Insufficient resources	It is recommended to purchase the upgrade package of corresponding resources

Status Code	Error Codes	Error Message	Description	Solution
404	WAF.00022001	resource.not.found	Resource does not exist	It is recommended to check the resource status on the console or ask for technical support
500	WAF.00010001	internal.error	Internal error	Contact technical support
500	WAF.00010002	system.busy	Internal error	Contact technical support
500	WAF.00010003	cname.failed	Failed to create or modify CNAME	Contact technical support
500	WAF.00010004	cname.failed	Failed to get OBS file download link	Contact technical support
500	WAF.00020001	internal.error	Service internal exception	It is recommended to try again in five minutes
500	WAF.00020002	system.busy	System busy	It is recommended to try again in five minutes

A.3 Obtaining a Project ID

Obtaining a Project ID by Calling an API

You can obtain the project ID by calling the 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 the administrator. 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
2024-04-15	This issue is the first official release.