Web Application Firewall (WAF)

API Reference

Issue 01

Date 2025-08-20

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

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

Overview

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.

API Calling

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

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.

Basic 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.

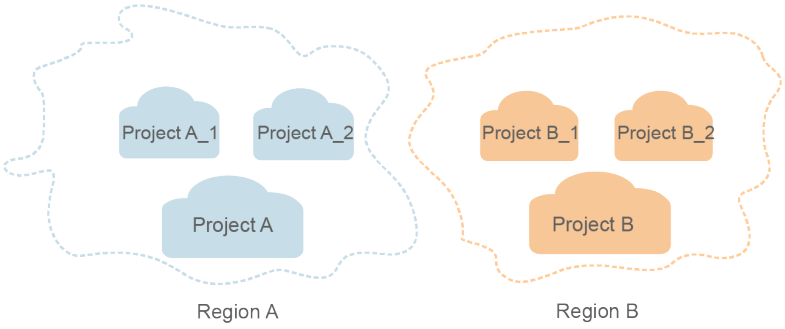
- Availability Zone (AZ)

  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

  A project corresponds to a region. Projects group and isolate resources (including compute, storage, and network resources) across physical regions. Users can be granted permissions in a default project to access all resources in the region associated with the 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 isolating 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 **ABCDEFG....**, add **X-Auth-Token: ABCDEFG....** to a request as follows:

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

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.

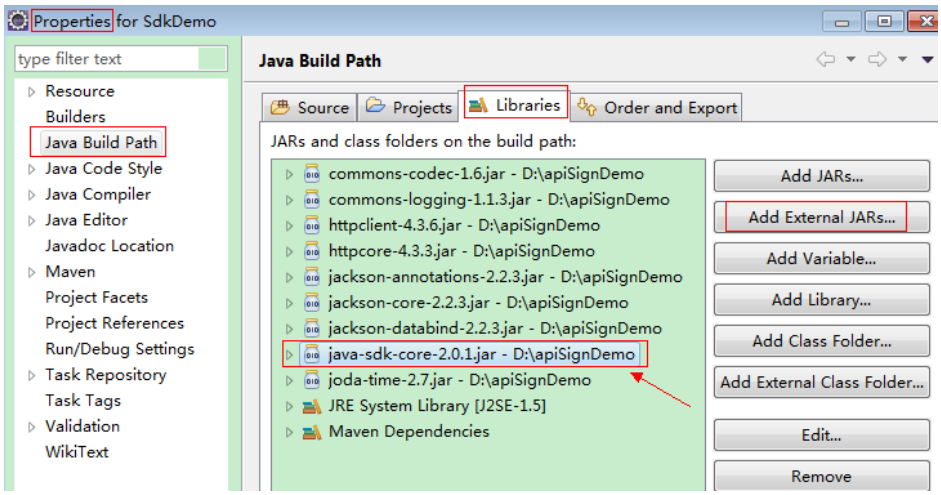
The following uses a demo project to show how to sign a request and use an HTTP client to send an HTTPS request.

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



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

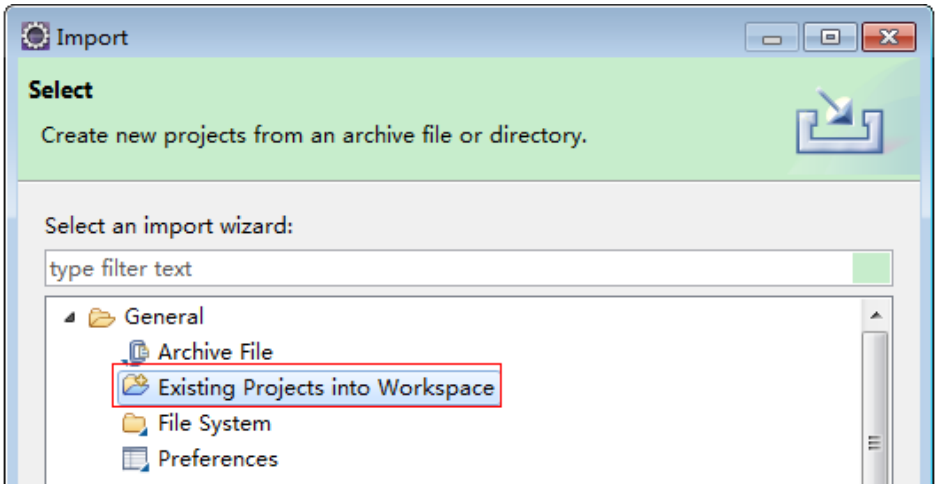


Figure 3-3 Selecting the demo project

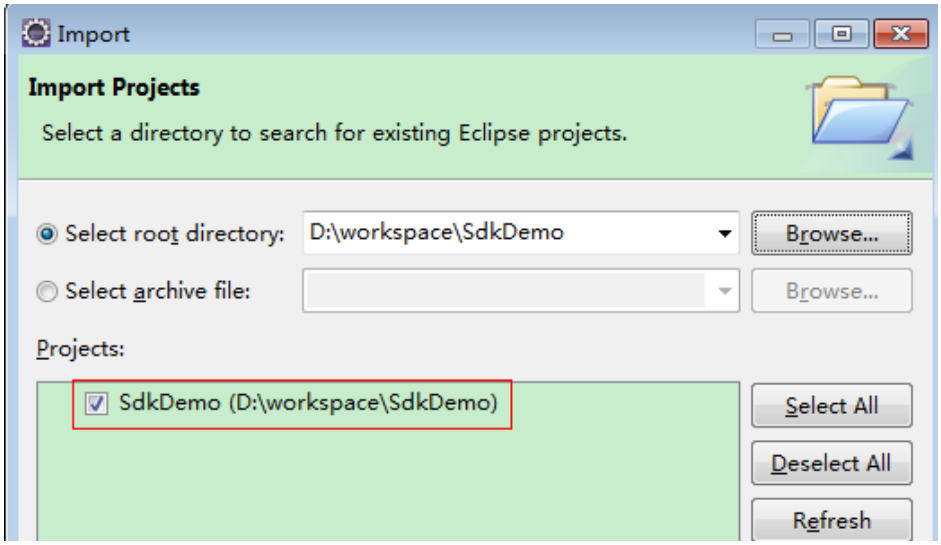
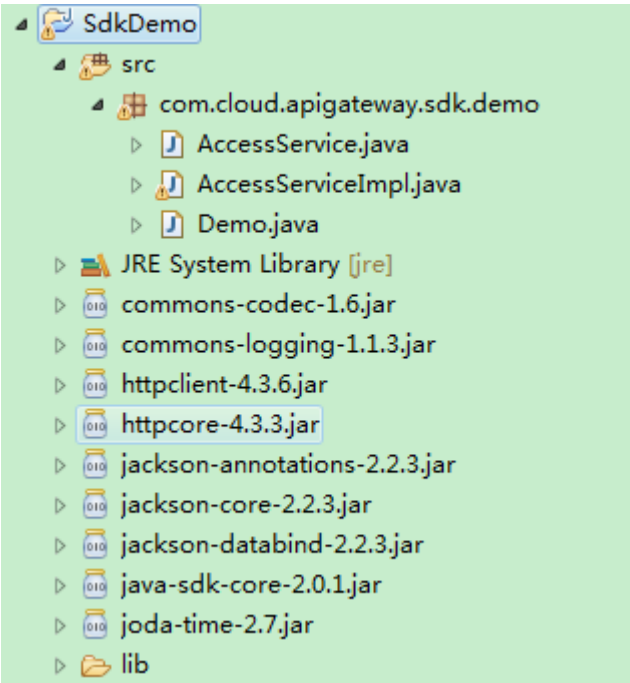


Figure 3-4 Structure of the demo project



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**.

Figure 3-5 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

(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 the List of Domain Names Protected by Dedicated WAF Instances

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-2 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Parameter	Mandatory	Type	Description
page	No	String	**Definition** Page number of the data to be returned in a query. The default value is 1, indicating that data on the first page is returned. **Constraints** N/A **Range** N/A **Default Value** 1
pagesize	No	String	**Definition** Number of results on each page in a pagination query. **Constraints** N/A **Range** The value range is 1 to 100. The default value is **10**, indicating that each page contains 10 results. To query all domain names at a time, set this parameter to **-1**. **Default Value** 10
hostname	No	String	**Definition** Domain name. **Constraints** N/A **Range** Enter a maximum of 63 characters. Only letters, digits, hyphens (-), and periods (.) are allowed, for example, www.domain com. **Default Value** N/A

Parameter	Mandatory	Type	Description
policyname	No	String	**Definition** Protection policy name, which is used to query the domain names using a specified protection policy. This parameter is optional. **Constraints** N/A **Range** Enter a maximum of 64 characters.Only letters, digits, underscores (_), hyphens (-), colons (:), and periods (.) are allowed. **Default Value** N/A
protect_status	No	Integer	**Definition** Domain protection status. **Constraints** N/A **Range** • **0**: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. • **1**: The WAF protection is enabled. WAF detects attacks based on the configured policy. **Default Value** N/A

Request Parameters

Table 4-3 Request header parameters

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

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	**Definition** Domain name ID. **Range** N/A
hostname	String	**Definition** Domain name. **Range** N/A
extend	Map<String,String>	**Definition** Extended field, which is used to save the configuration information of the protected domain name. **Range** N/A
region	String	**Definition** Region ID. This parameter is carried when a domain name is added to WAF on the management console. This parameter is left blank when a domain name is added to WAF using an API. **Range** N/A
flag	**Flag** object	Special identifier, which is used on the console.
description	String	**Definition** Domain name description. **Range** N/A
policyid	String	**Definition** ID of the protection policy initially bound to the protected domain name. You can call the ListPolicy API to query the policy ID based on the policy name. **Range** N/A

Parameter	Type	Description
protect_status	Integer	**Definition** Domain protection status. **Range** ● **0**: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. ● **1**: The WAF protection is enabled. WAF detects attacks based on the configured policy.
access_status	Integer	**Definition** Domain name access status. **Range** ● **0**: Inaccessible. ● **1**: Accessible.
web_tag	String	**Definition** Website name, which is the website name displayed on the domain name details page on the WAF console. **Range** N/A
hostid	String	**Definition** Domain name ID, which is the same as the value of id and is a redundant field. **Range** N/A
enterprise_project_id	String	**Definition** Enterprise project ID. **Range** N/A
pool_ids	Array of strings	**Definition** Dedicated engine group to which the domain name belongs. This field is returned when the domain name is connected to the ELB in cloud mode. **Range** N/A

Parameter	Type	Description
loadbalancer_id	String	**Definition** ELB load balancer ID. This field is returned when the cloud load balancer access mode is used. **Range** N/A
protocol_port	Integer	**Definition** Service port. This field is returned for the ELB access domain name in cloud mode. **Range** N/A

Table 4-6 Flag

Parameter	Type	Description
pci_3ds	String	**Definition** Whether to enable PCI 3DS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A
pci_dss	String	**Definition** Whether to enable PCI_DSS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A

Parameter	Type	Description
cname	String	**Definition** old: The old CNAME record is used. new: new CNAME record is used. **Constraints** N/A **Range** • old: old CNAME used by the domain name • new: The domain name uses a new CNAME. **Default Value** N/A
is_dual_az	String	**Definition** Whether the dual-AZ mode is supported **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A
ipv6	String	**Definition** Whether IPv6 is enabled for the domain name. **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Status code: 400

Table 4-7 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-8 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-9 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-10 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-11 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-12 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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


Example Responses

Status code: 200

OK


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


Status Codes

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

Error Codes

See **Error Codes**.

4.1.2 Adding a Domain Name to a Dedicated WAF Instance

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-13 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-14 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-15 Request header parameters

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

Table 4-16 Request body parameters

Parameter	Mandatory	Type	Description
certificateid	No	String	**Definition** Certificate ID, which can be obtained by calling the ListCertificates API. **Constraints** • This parameter is not required if the client protocol is HTTP. • This parameter is mandatory if the client protocol is HTTPS. **Range** N/A **Default Value** N/A
certificatename	No	String	**Definition** Certificate name. **Constraints** • This parameter is not required if the client protocol is HTTP. • This parameter is mandatory if the client protocol is HTTPS. **Range** N/A **Default Value** N/A
hostname	Yes	String	**Definition** Protected domain name or IP address (port allowed) **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
proxy	Yes	Boolean	**Definition** Whether the protected domain name uses a proxy. **Constraints** N/A **Range** • **false**: No proxy is used. • **true**: At least one proxy is used. **Default Value** N/A
policyid	No	String	**Definition** ID of the protection policy initially bound to the protected domain name. You can call the ListPolicy API to query the policy ID based on the policy name. **Constraints** N/A **Range** N/A **Default Value** N/A
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.

Parameter	Mandatory	Type	Description
forward_header_map	No	Map<String,String>	**Definition** Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of **Value** are as follows: • $time_local • $request_id • $connection_requests • $tenant_id • $project_id • $remote_addr • $remote_port • $scheme • $request_method • $http_host • $origin_uri • $request_length • $ssl_server_name • $ssl_protocol • $ssl_curves • $ssl_session_reused **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
mode	No	String	**Definition** If you use the cloud load balancer access mode, enter **enter elb-shared**. Otherwise, leave this parameter blank. **Constraints** N/A **Range** N/A **Default Value** N/A
loadbalancer_id	No	String	**Definition** Load balancer (ELB) ID, which can be queried on the ELB side. This parameter is mandatory when a cloud ELB access domain name is added. **Constraints** N/A **Range** N/A **Default Value** N/A
listener_id	No	String	**Definition** Listener ID. You can query the listener ID on the **Listeners** tab on the ELB console. If you leave this parameter blank, all listeners configured and to be configured for the load balancer will be protected by WAF. In cloud load balancer access mode, you are advised to set this parameter. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
protocol_port	No	Integer	**Definition** Specifies the service port. This parameter is mandatory when you add an ELB access domain name in cloud mode. **Constraints** N/A **Range** 0 - 65535 **Default Value** N/A
description	No	String	**Definition** Domain NAME REMARKS **Constraints** N/A **Range** 0 - 65535 **Default Value** N/A
web_tag	No	String	**Definition** Website name, which is the website name displayed on the domain name details page on the WAF console. **Constraints** N/A **Range** Enter 0 to 128 characters. **Default Value** N/A

Table 4-17 PremiumWafServer

Parameter	Mandatory	Type	Description
front_protocol	Yes	String	**Definition** Protocol used by the client to access the origin server of the protected domain name. **Constraints** N/A **Range** • HTTP • HTTPS **Default Value** N/A
back_protocol	Yes	String	**Definition** Protocol used by WAF to forward client requests to the origin server of the protected domain name. **Constraints** N/A **Range** • HTTP • HTTPS **Default Value** N/A
weight	No	Integer	**Definition** Weight of the origin server. The load balancing algorithm allocates requests to the origin server based on the weight. The default value is **1**. This parameter is not required for WAF cloud mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
address	Yes	String	**Definition** IP address of origin server accessed by the client. **Constraints** N/A **Range** N/A **Default Value** N/A
port	Yes	Integer	**Definition** Port used by WAF to forward client requests to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
type	Yes	String	**Definition** Type of the origin server address: IPv4 or IPv6 **Constraints** N/A **Range** • ipv4 • ipv6 **Default Value** N/A

Parameter	Mandatory	Type	Description
vpc_id	Yes	String	**Definition** VPC ID. To obtain the VPC ID, perform the following steps: • **1**. Query the name of the VPC where the dedicated engine (instance) is provisioned. To do so, log in to the WAF console and choose **Instance Management** > **Dedicated Engine** . Locate the target instance, and check the **VPC** and **Subnet** column. The VPC name is displayed in the VPC and subnet columns. • **2**. Go to the VPC console and choose **Virtual Private Cloud** > **My VPCs**. You can copy the ID next to the VPC name or click the VPC name and copy the ID in the **VPC Information** area. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-18 BlockPage

Parameter	Mandatory	Type	Description
template	Yes	String	**Definition** Template name. Enter default for the default page, custom for the customized alarm page, and redirect for redirection. **Constraints** N/A **Range** N/A **Default Value** N/A
custom_page	No	**CustomPage** object	Custom alarm page.
redirect_url	No	String	**Definition** URL of the redirection page. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-19 CustomPage

Parameter	Mandatory	Type	Description
status_code	Yes	String	**Definition** Return Code **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
content_type	Yes	String	**Definition** Content type of the custom alarm page. The options are text/html, text/xml, and application/json. **Constraints** N/A **Range** N/A **Default Value** N/A
content	Yes	String	**Definition** Configure the page content based on the selected page type. For details, see the Web Application Firewall User Manual. **Constraints** N/A **Range** N/A **Default Value** N/A

Response Parameters

Status code: 200

Table 4-20 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Protected domain names
protocol	String	Client protocol, which is the protocol used by a client (for example, a browser) to access your website.
server	Array of **PremiumWafServer** objects	Origin server configuration of the protected domain name

Parameter	Type	Description
proxy	Boolean	Whether to use a proxy • **true**: A proxy is used. • **false**: No proxies are 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.

Parameter	Type	Description
cipher	String	**Definition** The cipher parameter (cipher_1, cipher_2, cipher_3, cipher_4, cipher_5, cipher_6, cipher_default) is available only when the external protocol is HTTPS. **Range** • cipher_1: The encryption algorithm is ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH. • cipher_2: The encryption algorithm is EECDH+AESGCM:EDH+AESGCM. • cipher_3: The encryption algorithm is ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH. • cipher_4: The encryption algorithm is ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH. • cipher_5: The encryption algorithm is AES128-SHA:AES256-SHA:AES128-SHA256:AES256-SHA256:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4:!DHE:@STRENGTH. • cipher_6: The encryption algorithm is ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256. • cipher_default: The encryption algorithm is ECDHE-RSA-AES256-SHA384:AES256-

Parameter	Type	Description
		SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM.
extend	Map<String,String>	**Definition** Extended field, which is used to save the configuration information of the protected domain name. **Range** N/A
flag	**Flag** object	Special identifier, which is used on the console.
mode	String	**Definition** **elb-shared** is returned if cloud load balancer access mode is used. **Range** N/A
loadbalancer_id	String	**Definition** ELB load balancer ID. This field is returned when the cloud load balancer access mode is used. **Range** N/A
listener_id	String	ID of the listener configured for the ELB load balancer. This field is returned when the cloud load balancer access mode is used.
protocol_port	Integer	**Definition** Service port. This field is returned when the cloud load balancer access mode is used. **Range** N/A
description	String	**Definition** Domain name description. **Range** N/A

Parameter	Type	Description
policyid	String	**Definition** ID of the protection policy initially bound to the protected domain name. You can call the ListPolicy API to query the policy ID based on the policy name. **Range** N/A
domainid	String	**Definition** Account ID. You can obtain it from **My Credentials** > **Account ID** page on the management console. **Range** N/A
projectid	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Range** N/A
enterprise_project_id	String	**Definition** Enterprise project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **Enterprise** > **Project Management**, click the project name, and locate the project ID. **Range** N/A
certificateid	String	**Definition** HTTPS certificate ID. **Range** N/A
certificatename	String	**Definition** Certificate name. **Range** Enter a maximum of 256 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.

Parameter	Type	Description
protect_status	Integer	**Definition** Domain protection status. **Range** • **0**: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. • **1**: The WAF protection is enabled. WAF detects attacks based on the configured policy.
access_status	Integer	**Definition** Domain name access status. **Range** • **0**: Inaccessible. • **1**: Accessible.
web_tag	String	**Definition** Website name, which is the website name displayed on the domain name details page on the WAF console. **Range** N/A
block_page	**BlockPage** object	Alarm page configuration
traffic_mark	**TrafficMark** object	Traffic identifier.
timeout_config	**TimeoutConfig** object	Timeout settings.

Parameter	Type	Description
forward_header_map	Map<String,String>	**Definition** Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of **Value** are as follows: • $time_local • $request_id • $connection_requests • $tenant_id • $project_id • $remote_addr • $remote_port • $scheme • $request_method • $http_host • $origin_uri • $request_length • $ssl_server_name • $ssl_protocol • $ssl_curves • $ssl_session_reused

Table 4-21 PremiumWafServer

Parameter	Type	Description
front_protocol	String	**Definition** Protocol used by the client to access the origin server of the protected domain name. **Constraints** N/A **Range** • HTTP • HTTPS **Default Value** N/A

Parameter	Type	Description
back_protocol	String	**Definition** Protocol used by WAF to forward client requests to the origin server of the protected domain name. **Constraints** N/A **Range** • HTTP • HTTPS **Default Value** N/A
weight	Integer	**Definition** Weight of the origin server. The load balancing algorithm allocates requests to the origin server based on the weight. The default value is **1**. This parameter is not required for WAF cloud mode. **Constraints** N/A **Range** N/A **Default Value** N/A
address	String	**Definition** IP address of origin server accessed by the client. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Type	Description
port	Integer	**Definition** Port used by WAF to forward client requests to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
type	String	**Definition** Type of the origin server address: IPv4 or IPv6 **Constraints** N/A **Range** • ipv4 • ipv6 **Default Value** N/A

Parameter	Type	Description
vpc_id	String	**Definition** VPC ID. To obtain the VPC ID, perform the following steps: • **1**. Query the name of the VPC where the dedicated engine (instance) is provisioned. To do so, log in to the WAF console and choose **Instance Management** > **Dedicated Engine** . Locate the target instance, and check the **VPC** and **Subnet** column. The VPC name is displayed in the VPC and subnet columns. • **2**. Go to the VPC console and choose **Virtual Private Cloud** > **My VPCs**. You can copy the ID next to the VPC name or click the VPC name and copy the ID in the **VPC Information** area. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-22 Flag

Parameter	Type	Description
pci_3ds	String	**Definition** Whether to enable PCI 3DS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A

Parameter	Type	Description
pci_dss	String	**Definition** Whether to enable PCI_DSS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A
cname	String	**Definition** old: The old CNAME record is used. new: new CNAME record is used. **Constraints** N/A **Range** • old: old CNAME used by the domain name • new: The domain name uses a new CNAME. **Default Value** N/A
is_dual_az	String	**Definition** Whether the dual-AZ mode is supported **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Parameter	Type	Description
ipv6	String	**Definition** Whether IPv6 is enabled for the domain name. **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Table 4-23 BlockPage

Parameter	Type	Description
template	String	**Definition** Template name. Enter default for the default page, custom for the customized alarm page, and redirect for redirection. **Constraints** N/A **Range** N/A **Default Value** N/A
custom_page	**CustomPage** object	Custom alarm page.
redirect_url	String	**Definition** URL of the redirection page. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-24 CustomPage

Parameter	Type	Description
status_code	String	**Definition** Return Code **Constraints** N/A **Range** N/A **Default Value** N/A
content_type	String	**Definition** Content type of the custom alarm page. The options are text/html, text/xml, and application/json. **Constraints** N/A **Range** N/A **Default Value** N/A
content	String	**Definition** Configure the page content based on the selected page type. For details, see the Web Application Firewall User Manual. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-25 TrafficMark

Parameter	Type	Description
sip	Array of strings	**Definition** IP flag, which is the HTTP request header field of the original IP address of the client. **Constraints** N/A **Range** N/A **Default Value** N/A
cookie	String	**Definition** Session flag, which is used for the attack punishment function of malicious cookie requests. This flag must be configured before the attack punishment function for cookie interception is selected. **Constraints** N/A **Range** N/A **Default Value** N/A
params	String	**Definition** User flag, which is used for the attack punishment function of Params malicious requests. Configure this parameter to block requests based on the Params attributes. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-26 TimeoutConfig

Parameter	Type	Description
connect_timeout	Integer	**Definition** Timeout for WAF to connect to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
send_timeout	Integer	**Definition** Timeout for WAF to send requests to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
read_timeout	Integer	**Definition** Timeout for WAF to receive responses from the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-27 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-28 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-29 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-30 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-31 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-32 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to add a website domain name to a dedicated WAF instance in a specific project. The project ID is specified by project_id, and the domain name is www.demo.com. The client protocol and server protocol is HTTP. The origin server address is ipv4 x.x.x.x. The service port used by WAF to forward client requests to the origin server is 80. The ID of the VPC where the dedicated WAF instance is deployed is cf6dbace-b36a-4d51-ae04-52a3319ae247.

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



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

Example Responses

Status code: 200

OK

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

Status Codes

Status Code	Description
200	OK
400	Invalid request.
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-33 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Parameter	Mandatory	Type	Description
host_id	Yes	String	**Definition** ID of the domain name protected by the dedicated WAF engine. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-34 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-35 Request header parameters

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

Table 4-36 Request body parameters

Parameter	Mandatory	Type	Description
proxy	No	Boolean	**Definition** Whether the protected domain name uses a proxy. **Constraints** N/A **Range** • **false**: No proxy is used. • **true**: At least one proxy is used. **Default Value** N/A

Parameter	Mandatory	Type	Description
certificateid	No	String	**Definition** HTTPS certificate ID. You can all the **ListCertificates** API to obtain it. **Constraints** • This parameter is not required if the client protocol is HTTP. • This parameter is mandatory if the client protocol is HTTPS. **Range** N/A **Default Value** N/A
certificatename	No	String	**Definition** Certificate name. **Constraints** • This parameter is not required if the client protocol is HTTP. • This parameter is mandatory if the client protocol is HTTPS. **Range** N/A **Default Value** N/A
server	No	Array of **PremiumWafServer** objects	Origin server configuration of the protected domain name

Parameter	Mandatory	Type	Description
tls	No	String	**Definition** Minimum TLS version (TLS v1.0/TLS v1.1/TLS v1.2). The default version is TLS v1.0. If the TLS version is earlier than TLS v1.0, the website cannot be accessed. **Constraints** N/A **Range** • TLS v1.0 • TLS v1.1 • TLS v1.2 **Default Value** TLS v1.0

Parameter	Mandatory	Type	Description
cipher	No	String	**Definition** Cipher Suite (cipher_1, cipher_2, cipher_3, cipher_4, cipher_5, cipher_6, cipher_default) **Constraints** N/A **Range** • cipher_1: The encryption algorithm is ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH. • cipher_2: The encryption algorithm is EECDH+AESGCM:EDH+AESGCM. • cipher_3: The encryption algorithm is ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH. • cipher_4: The encryption algorithm is ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH. • cipher_5: The encryption algorithm is AES128-SHA:AES256-SHA:AES128-SHA256:AES256-SHA256:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4:!DHE:@STRENGTH. • cipher_6: The encryption algorithm is ECDHE-

Parameter	Mandatory	Type	Description
			ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256. • cipher_default: The encryption algorithm is ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM. **Default Value** N/A
mode	No	String	**Definition** Special domain name node in dedicated mode. This parameter is required only for special WAF modes, such as ELB. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
locked	No	Integer	**Definition** This parameter is reserved for freezing and unlocking domain names. Currently, this parameter is not supported. **Constraints** N/A **Range** N/A **Default Value** N/A
protect_status	No	Integer	**Definition** Domain protection status. **Constraints** N/A **Range** • **0**: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. • **1**: The WAF protection is enabled. WAF detects attacks based on the configured policy. **Default Value** N/A
access_status	No	Integer	**Definition** Domain name access status. **Constraints** N/A **Range** • **0**: Inaccessible. • **1**: Accessible. **Default Value** N/A

Parameter	Mandatory	Type	Description
timestamp	No	Integer	**Definition** Timestamp. **Constraints** N/A **Range** N/A **Default Value** N/A
pool_ids	No	Array of strings	**Definition** Dedicated engine group to which the domain name in special mode belongs (required only in special mode, for example, ELB) **Constraints** N/A **Range** N/A **Default Value** N/A
block_page	No	**BlockPage** object	Alarm page configuration
traffic_mark	No	**TrafficMark** object	Traffic identifier
circuit_breaker	No	**CircuitBreaker** object	Circuit breaker configuration
timeout_config	No	**TimeoutConfig** object	Timeout settings
flag	No	**HostFlag** object	Feature switch for configuring compliance certification checks for domain names protected with the dedicated WAF instance.

Parameter	Mandatory	Type	Description
forward_header_map	No	Map<String,String>	**Definition** Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of **Value** are as follows: • $time_local • $request_id • $connection_requests • $tenant_id • $project_id • $remote_addr • $remote_port • $scheme • $request_method • $http_host • $origin_uri • $request_length • $ssl_server_name • $ssl_protocol • $ssl_curves • $ssl_session_reused **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-37 PremiumWafServer

Parameter	Mandatory	Type	Description
front_protocol	Yes	String	**Definition** Protocol used by the client to access the origin server of the protected domain name. **Constraints** N/A **Range** • HTTP • HTTPS **Default Value** N/A
back_protocol	Yes	String	**Definition** Protocol used by WAF to forward client requests to the origin server of the protected domain name. **Constraints** N/A **Range** • HTTP • HTTPS **Default Value** N/A
weight	No	Integer	**Definition** Weight of the origin server. The load balancing algorithm allocates requests to the origin server based on the weight. The default value is **1**. This parameter is not required for WAF cloud mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
address	Yes	String	**Definition** IP address of origin server accessed by the client. **Constraints** N/A **Range** N/A **Default Value** N/A
port	Yes	Integer	**Definition** Port used by WAF to forward client requests to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
type	Yes	String	**Definition** Type of the origin server address: IPv4 or IPv6 **Constraints** N/A **Range** • ipv4 • ipv6 **Default Value** N/A

Parameter	Mandatory	Type	Description
vpc_id	Yes	String	**Definition** VPC ID. To obtain the VPC ID, perform the following steps: • **1**. Query the name of the VPC where the dedicated engine (instance) is provisioned. To do so, log in to the WAF console and choose **Instance Management** > **Dedicated Engine** . Locate the target instance, and check the **VPC** and **Subnet** column. The VPC name is displayed in the VPC and subnet columns. • **2**. Go to the VPC console and choose **Virtual Private Cloud** > **My VPCs**. You can copy the ID next to the VPC name or click the VPC name and copy the ID in the **VPC Information** area. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-38 BlockPage

Parameter	Mandatory	Type	Description
template	Yes	String	**Definition** Template name. Enter default for the default page, custom for the customized alarm page, and redirect for redirection. **Constraints** N/A **Range** N/A **Default Value** N/A
custom_page	No	**CustomPage** object	Custom alarm page.
redirect_url	No	String	**Definition** URL of the redirection page. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-39 CustomPage

Parameter	Mandatory	Type	Description
status_code	Yes	String	**Definition** Return Code **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
content_type	Yes	String	**Definition** Content type of the custom alarm page. The options are text/html, text/xml, and application/json. **Constraints** N/A **Range** N/A **Default Value** N/A
content	Yes	String	**Definition** Configure the page content based on the selected page type. For details, see the Web Application Firewall User Manual. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-40 TrafficMark

Parameter	Mandatory	Type	Description
sip	No	Array of strings	**Definition** IP flag, which is the HTTP request header field of the original IP address of the client. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
cookie	No	String	**Definition** Session flag, which is used for the attack punishment function of malicious cookie requests. This flag must be configured before the attack punishment function for cookie interception is selected. **Constraints** N/A **Range** N/A **Default Value** N/A
params	No	String	**Definition** User flag, which is used for the attack punishment function of Params malicious requests. Configure this parameter to block requests based on the Params attributes. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-41 CircuitBreaker

Parameter	Mandatory	Type	Description
switch	No	Boolean	**Definition** Circuit breaker switch, indicating whether to enable connection protection **Constraints** N/A **Range** • true: Connection protection is enabled. • false: Connection protection is disabled. **Default Value** N/A
dead_num	No	Integer	**Definition** 502/504 error quantity threshold, that is, the 502/504 error quantity threshold accumulated every 30s. **Constraints** N/A **Range** N/A **Default Value** N/A
dead_ratio	No	Number	**Definition** Percentage of 502/504 errors (%). When the percentage of 502/504 errors in the total number of requests reaches the specified value and the number threshold is met, breakdown protection is triggered. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
block_time	No	Integer	**Definition** Protection period upon the first breakdown. During this period, WAF stops forwarding client requests. **Constraints** N/A **Range** N/A **Default Value** N/A
superposition_num	No	Integer	**Definition** 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, the initial protection time is set to 180s, and the continuous trigger addition coefficient is set to 3. **Constraints** N/A **Range** ● When the number of triggering times is 2 (that is, less than 3), the protection time is 360s. ● When the number of times is greater than or equal to 3, the protection time is 540s. ● When the accumulated protection time exceeds 1 hour (3600s), the number of accumulated times is counted from the beginning. **Default Value** N/A

Parameter	Mandatory	Type	Description
suspend_num	No	Integer	**Definition** Threshold of the number of read waiting URL requests. When the number of read waiting URL requests reaches the threshold, connection protection is triggered. **Constraints** N/A **Range** N/A **Default Value** N/A
sus_block_time	No	Integer	**Definition** Circuit breaker time when the number of read waiting URL requests exceeds the threshold. When the number of read waiting URL requests reaches the protection time triggered by the threshold, WAF stops forwarding user requests. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-42 TimeoutConfig

Parameter	Mandatory	Type	Description
connect_timeout	No	Integer	**Definition** Timeout for WAF to connect to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
send_timeout	No	Integer	**Definition** Timeout for WAF to send requests to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
read_timeout	No	Integer	**Definition** Timeout for WAF to receive responses from the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-43 HostFlag

Parameter	Mandatory	Type	Description
pci_3ds	No	String	**Definition** Status of the PCI 3DS compliance certification check. This parameter must be used together with **tls** and **cipher**. **tls** must be set to **TLS v1.2**, and **cipher** must be set to **cipher_2**. Note: PCI 3DS compliance authentication cannot be disabled after being enabled. Before enabling PCI 3DS compliance authentication, read the description of PCI 3DS compliance authentication in the WAF documentation of Help Center. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A
pci_dss	No	String	**Definition** Status of the PCI DSS compliance certification check. This parameter must be used together with **tls** and **cipher**. **tls** must be set to **TLS v1.2**, and **cipher** must be set to **cipher_2**. Note: Before enabling the check, read the corresponding description in WAF documentation in Help Center. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A

Response Parameters

Status code: 200

Table 4-44 Response body parameters

Parameter	Type	Description
id	String	Domain name ID
hostname	String	Domain name added to the dedicated WAF instance
protocol	String	Client protocol, which is the protocol used by a client (for example, a browser) to access your website.
server	Array of **PremiumWafServer** objects	Origin server configuration of the protected domain name
proxy	Boolean	Whether a proxy is used for the protected domain name. • **false**: No proxies are used. • **true**: A proxy is used.
locked	Integer	This parameter is reserved, which will be used to freeze a domain name.
timestamp	Long	Time the domain name was added to WAF.
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.

Parameter	Type	Description
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.
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.
mode	String	**elb-shared** is returned if cloud load balancer access mode is used.
loadbalancer_id	String	ELB load balancer ID. This field is returned when the cloud load balancer access mode is used.
listener_id	String	ID of the listener configured for the ELB load balancer. This field is returned when the cloud load balancer access mode is used.
protocol_port	Integer	Service port. This field is returned when the cloud load balancer access mode is used.
description	String	Domain name description

Parameter	Type	Description
policyid	String	ID of the policy initially used to the domain name. You can call the **ListPolicy** API to query the policy list and view the ID of the specific policy.
domainid	String	Account ID, which is the same as the account ID on the **My Credentials** page. To go to this page, log in to Huawei 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 Huawei Cloud management cons**. 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 Huawei 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.
lb_algorithm	String	Load balancing algorithm. Weighted round robin is used by default and cannot be changed.

Parameter	Type	Description
block_page	**BlockPage** object	Alarm page configuration
traffic_mark	**TrafficMark** object	Traffic identifier
timeout_config	**TimeoutConfig** object	Timeout settings
forward_header_map	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: • $time_local • $request_id • $connection_requests • $tenant_id • $project_id • $remote_addr • $remote_port • $scheme • $request_method • $http_host • $origin_uri • $request_length • $ssl_server_name • $ssl_protocol • $ssl_curves • $ssl_session_reused
access_progress	Array of **Access_progress** objects	Access progress, which is used only for the new WAF console.

Table 4-45 PremiumWafServer

Parameter	Type	Description
front_protocol	String	**Definition** Protocol used by the client to access the origin server of the protected domain name. **Constraints** N/A **Range** • HTTP • HTTPS **Default Value** N/A
back_protocol	String	**Definition** Protocol used by WAF to forward client requests to the origin server of the protected domain name. **Constraints** N/A **Range** • HTTP • HTTPS **Default Value** N/A
weight	Integer	**Definition** Weight of the origin server. The load balancing algorithm allocates requests to the origin server based on the weight. The default value is **1**. This parameter is not required for WAF cloud mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Type	Description
address	String	**Definition** IP address of origin server accessed by the client. **Constraints** N/A **Range** N/A **Default Value** N/A
port	Integer	**Definition** Port used by WAF to forward client requests to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
type	String	**Definition** Type of the origin server address: IPv4 or IPv6 **Constraints** N/A **Range** • ipv4 • ipv6 **Default Value** N/A

Parameter	Type	Description
vpc_id	String	**Definition** VPC ID. To obtain the VPC ID, perform the following steps: • **1**. Query the name of the VPC where the dedicated engine (instance) is provisioned. To do so, log in to the WAF console and choose **Instance Management** > **Dedicated Engine** . Locate the target instance, and check the **VPC** and **Subnet** column. The VPC name is displayed in the VPC and subnet columns. • **2**. Go to the VPC console and choose **Virtual Private Cloud** > **My VPCs**. You can copy the ID next to the VPC name or click the VPC name and copy the ID in the **VPC Information** area. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-46 Flag

Parameter	Type	Description
pci_3ds	String	**Definition** Whether to enable PCI 3DS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A

Parameter	Type	Description
pci_dss	String	**Definition** Whether to enable PCI_DSS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A
cname	String	**Definition** old: The old CNAME record is used. new: new CNAME record is used. **Constraints** N/A **Range** • old: old CNAME used by the domain name • new: The domain name uses a new CNAME. **Default Value** N/A
is_dual_az	String	**Definition** Whether the dual-AZ mode is supported **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Parameter	Type	Description
ipv6	String	**Definition** Whether IPv6 is enabled for the domain name. **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Table 4-47 BlockPage

Parameter	Type	Description
template	String	**Definition** Template name. Enter default for the default page, custom for the customized alarm page, and redirect for redirection. **Constraints** N/A **Range** N/A **Default Value** N/A
custom_page	**CustomPage** object	Custom alarm page.
redirect_url	String	**Definition** URL of the redirection page. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-48 CustomPage

Parameter	Type	Description
status_code	String	**Definition** Return Code **Constraints** N/A **Range** N/A **Default Value** N/A
content_type	String	**Definition** Content type of the custom alarm page. The options are text/html, text/xml, and application/json. **Constraints** N/A **Range** N/A **Default Value** N/A
content	String	**Definition** Configure the page content based on the selected page type. For details, see the Web Application Firewall User Manual. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-49 TrafficMark

Parameter	Type	Description
sip	Array of strings	**Definition** IP flag, which is the HTTP request header field of the original IP address of the client. **Constraints** N/A **Range** N/A **Default Value** N/A
cookie	String	**Definition** Session flag, which is used for the attack punishment function of malicious cookie requests. This flag must be configured before the attack punishment function for cookie interception is selected. **Constraints** N/A **Range** N/A **Default Value** N/A
params	String	**Definition** User flag, which is used for the attack punishment function of Params malicious requests. Configure this parameter to block requests based on the Params attributes. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-50 TimeoutConfig

Parameter	Type	Description
connect_timeout	Integer	**Definition** Timeout for WAF to connect to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
send_timeout	Integer	**Definition** Timeout for WAF to send requests to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
read_timeout	Integer	**Definition** Timeout for WAF to receive responses from the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-51 Access_progress

Parameter	Type	Description
step	Integer	**Definition** Steps **Range** • **1**: Whitelist the WAF IP addresses. • **2**: Test connectivity. • **3**: Modify DNS resolution.

Parameter	Type	Description
status	Integer	**Definition** Status **Range** • 0: This step is not complete. • 1: completed

Status code: 400

Table 4-52 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-53 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-54 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-55 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-56 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-57 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

{
  "proxy" : false
}
```

Example Responses

Status code: 200

OK

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


Status Codes

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

Error Codes

See **Error Codes**.

4.1.4 Querying Domain Name Settings in Dedicated Mode

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-58 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Parameter	Mandatory	Type	Description
host_id	Yes	String	**Definition** ID of the domain name protected by the dedicated WAF engine. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-59 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-60 Request header parameters

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

Response Parameters

Status code: 200

Table 4-61 Response body parameters

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Range** N/A
hostname	String	**Definition** Domain name created in dedicated mode **Range** N/A

Parameter	Type	Description
protocol	String	**Definition** Protocol used by a client (for example, a browser) to access a website. **Range** • HTTPS • HTTP • HTTP&HTTPS
server	Array of **PremiumWafServer** objects	Origin server configuration of the protected domain name
proxy	Boolean	**Definition** Whether a proxy is used for the domain name. **Range** • **true**: A proxy is used. • **false**: No proxy is used.
locked	Integer	This parameter is reserved, which will be used to freeze a domain name.
timestamp	Long	Time the domain name was added to WAF.
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.

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.
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.
mode	String	**elb-shared** is returned if cloud load balancer access mode is used.
loadbalancer_id	String	ELB load balancer ID. This field is returned when the cloud load balancer access mode is used.
listener_id	String	ID of the listener configured for the ELB load balancer. This field is returned when the cloud load balancer access mode is used.
protocol_port	Integer	Service port. This field is returned when the cloud load balancer access mode is used.
description	String	Domain name description

Parameter	Type	Description
policyid	String	ID of the policy initially used to the domain name. You can call the **ListPolicy** API to query the policy list and view the ID of the specific policy.
domainid	String	Account ID, which is the same as the account ID on the **My Credentials** page. To go to this page, log in to Huawei 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 Huawei Cloud management cons**. 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 Huawei 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.
block_page	**BlockPage** object	Alarm page configuration

Parameter	Type	Description
traffic_mark	**TrafficMark** object	Traffic identifier
timeout_config	**TimeoutConfig** object	Timeout settings
forward_header_map	Map<String,String>	Field forwarding configuration. WAF inserts the added fields into the header and forwards the header to the origin server. The key cannot be the same as the native Nginx field. The options of Value are as follows: • $time_local • $request_id • $connection_requests • $tenant_id • $project_id • $remote_addr • $remote_port • $scheme • $request_method • $http_host • $origin_uri • $request_length • $ssl_server_name • $ssl_protocol • $ssl_curves • $ssl_session_reused
access_progress	Array of **Access_progress** objects	Access progress, which is used only for the new WAF console.

Table 4-62 PremiumWafServer

Parameter	Type	Description
front_protocol	String	**Definition** Protocol used by the client to access the origin server of the protected domain name. **Constraints** N/A **Range** • HTTP • HTTPS **Default Value** N/A
back_protocol	String	**Definition** Protocol used by WAF to forward client requests to the origin server of the protected domain name. **Constraints** N/A **Range** • HTTP • HTTPS **Default Value** N/A
weight	Integer	**Definition** Weight of the origin server. The load balancing algorithm allocates requests to the origin server based on the weight. The default value is **1**. This parameter is not required for WAF cloud mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Type	Description
address	String	**Definition** IP address of origin server accessed by the client. **Constraints** N/A **Range** N/A **Default Value** N/A
port	Integer	**Definition** Port used by WAF to forward client requests to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
type	String	**Definition** Type of the origin server address: IPv4 or IPv6 **Constraints** N/A **Range** • ipv4 • ipv6 **Default Value** N/A

Parameter	Type	Description
vpc_id	String	**Definition** VPC ID. To obtain the VPC ID, perform the following steps: • **1**. Query the name of the VPC where the dedicated engine (instance) is provisioned. To do so, log in to the WAF console and choose **Instance Management** > **Dedicated Engine** . Locate the target instance, and check the **VPC** and **Subnet** column. The VPC name is displayed in the VPC and subnet columns. • **2**. Go to the VPC console and choose **Virtual Private Cloud** > **My VPCs**. You can copy the ID next to the VPC name or click the VPC name and copy the ID in the **VPC Information** area. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-63 Flag

Parameter	Type	Description
pci_3ds	String	**Definition** Whether to enable PCI 3DS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A

Parameter	Type	Description
pci_dss	String	**Definition** Whether to enable PCI_DSS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A
cname	String	**Definition** old: The old CNAME record is used. new: new CNAME record is used. **Constraints** N/A **Range** • old: old CNAME used by the domain name • new: The domain name uses a new CNAME. **Default Value** N/A
is_dual_az	String	**Definition** Whether the dual-AZ mode is supported **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Parameter	Type	Description
ipv6	String	**Definition** Whether IPv6 is enabled for the domain name. **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Table 4-64 BlockPage

Parameter	Type	Description
template	String	**Definition** Template name. Enter default for the default page, custom for the customized alarm page, and redirect for redirection. **Constraints** N/A **Range** N/A **Default Value** N/A
custom_page	**CustomPage** object	Custom alarm page.
redirect_url	String	**Definition** URL of the redirection page. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-65 CustomPage

Parameter	Type	Description
status_code	String	**Definition** Return Code **Constraints** N/A **Range** N/A **Default Value** N/A
content_type	String	**Definition** Content type of the custom alarm page. The options are text/html, text/xml, and application/json. **Constraints** N/A **Range** N/A **Default Value** N/A
content	String	**Definition** Configure the page content based on the selected page type. For details, see the Web Application Firewall User Manual. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-66 TrafficMark

Parameter	Type	Description
sip	Array of strings	**Definition** IP flag, which is the HTTP request header field of the original IP address of the client. **Constraints** N/A **Range** N/A **Default Value** N/A
cookie	String	**Definition** Session flag, which is used for the attack punishment function of malicious cookie requests. This flag must be configured before the attack punishment function for cookie interception is selected. **Constraints** N/A **Range** N/A **Default Value** N/A
params	String	**Definition** User flag, which is used for the attack punishment function of Params malicious requests. Configure this parameter to block requests based on the Params attributes. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-67 TimeoutConfig

Parameter	Type	Description
connect_timeout	Integer	**Definition** Timeout for WAF to connect to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
send_timeout	Integer	**Definition** Timeout for WAF to send requests to the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A
read_timeout	Integer	**Definition** Timeout for WAF to receive responses from the origin server. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-68 Access_progress

Parameter	Type	Description
step	Integer	**Definition** Steps **Range** • **1**: Whitelist the WAF IP addresses. • **2**: Test connectivity. • **3**: Modify DNS resolution.

Parameter	Type	Description
status	Integer	**Definition** Status **Range** • 0: This step is not complete. • 1: completed

Status code: 400

Table 4-69 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-70 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-71 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-72 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-73 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-74 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

Example Responses

Status code: 200

OK

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


Status Codes

Status Code	Description
200	OK
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-75 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A
host_id	Yes	String	**Definition** ID of the domain name protected by the dedicated WAF engine. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-76 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0
keepPolicy	No	Boolean	**Definition** Whether to retain the protection policy. **false**: Do not retain the protection policy of the domain name. **true**: Retain the protection policy of the domain name. This parameter is not passed when the protection policy of the domain name to be deleted protects multiple domain names. **Constraints** N/A **Range** N/A **Default Value** N/A

Request Parameters

Table 4-77 Request header parameters

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

Response Parameters

Status code: 200

Table 4-78 Response body parameters

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Range** N/A
hostname	String	**Definition** Domain Names Protected in Dedicated Mode **Range** N/A

Parameter	Type	Description
extend	Map<String,String>	**Definition** Extended field, which is used to save the configuration information of the protected domain name. **Range** N/A
region	String	**Definition** Region ID. This parameter is carried when a domain name is added to WAF on the management console. This parameter is left blank when a domain name is added to WAF using an API. **Range** N/A
flag	**Flag** object	Special identifier, which is used on the console.
description	String	**Definition** Domain name description. **Range** N/A
policyid	String	**Definition** ID of the protection policy initially bound to the protected domain name. You can call the ListPolicy API to query the policy ID based on the policy name. **Range** N/A
protect_status	Integer	**Definition** Domain protection status. **Range** • **0**: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. • **1**: The WAF protection is enabled. WAF detects attacks based on the configured policy.

Parameter	Type	Description
access_status	Integer	**Definition** Domain name access status. **Range** • **0**: Inaccessible. • **1**: Accessible.
web_tag	String	**Definition** Website name, which is the website name displayed on the domain name details page on the WAF console. **Range** N/A
host_id	String	**Definition** Domain name ID, which is the same as the value of id and is a redundant field. **Range** N/A

Table 4-79 Flag

Parameter	Type	Description
pci_3ds	String	**Definition** Whether to enable PCI 3DS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A

Parameter	Type	Description
pci_dss	String	**Definition** Whether to enable PCI_DSS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A
cname	String	**Definition** old: The old CNAME record is used. new: new CNAME record is used. **Constraints** N/A **Range** • old: old CNAME used by the domain name • new: The domain name uses a new CNAME. **Default Value** N/A
is_dual_az	String	**Definition** Whether the dual-AZ mode is supported **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Parameter	Type	Description
ipv6	String	**Definition** Whether IPv6 is enabled for the domain name. **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Status code: 400

Table 4-80 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-81 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-82 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-83 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-84 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-85 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

Example Responses

Status code: 200

OK

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

Status Codes

Status Code	Description
200	OK
400	Invalid request.
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-86 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A
host_id	Yes	String	**Definition** ID of the domain name protected by the dedicated WAF engine. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-87 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-88 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** Content type. **Constraints** N/A **Range** N/A **Default Value** application/json;charset=utf8

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. It can be obtained by calling the IAM API (value of **X-Subject-Token** in the response header). **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-89 Request body parameters

Parameter	Mandatory	Type	Description
protect_status	Yes	Integer	**Definition** Domain protection status. **Constraints** N/A **Range** • **0**: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. • **1**: The WAF protection is enabled. WAF detects attacks based on the configured policy. **Default Value** N/A

Response Parameters

Status code: 200

Table 4-90 Response body parameters

Parameter	Type	Description
protect_status	Integer	**Definition** Domain protection status. **Constraints** N/A **Range** • **0**: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. • **1**: The WAF protection is enabled. WAF detects attacks based on the configured policy. **Default Value** N/A

Status code: 400

Table 4-91 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-92 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.

Parameter	Type	Description
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-93 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-94 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-95 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-96 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

{
  "protect_status" : 1
}
```

Example Responses

Status code: 200

OK

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

Status Codes

Status Code	Description
200	OK

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

Error Codes

See **Error Codes**.

4.2 Policy Management

4.2.1 Querying the Protection Policy List

Function

This API is used to query the protection policy list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/waf/policy

Table 4-97 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-98 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0
page	No	Integer	**Definition** Start position of the pagination query. This parameter specifies from which record you want to retrieve (counting starts from 1). **Constraints** N/A **Range** N/A **Default Value** 1

Parameter	Mandatory	Type	Description
pagesize	No	Integer	**Definition** Number of results on each page in a pagination query. **Constraints** N/A **Range** The value range is 1 to 100. The default value is **10**, indicating that each page contains 10 results. **Default Value** 10
name	No	String	**Definition** Policy name. **Constraints** N/A **Range** Enter a maximum of 64 characters. Only letters, digits, underscores (_), hyphens (-), colons (:), and periods (.) are allowed. **Default Value** 10

Request Parameters

Table 4-99 Request header parameters

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

Response Parameters

Status code: 200

Table 4-100 Response body parameters

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

Table 4-101 PolicyResponse

Parameter	Type	Description
id	String	**Definition** Protection policy ID. **Range** N/A
name	String	**Definition** Protection policy name. **Range** Enter a maximum of 64 characters. Only letters, digits, underscores (_), hyphens (-), colons (:), and periods (.) are allowed.
level	Integer	**Definition** Basic web protection level. **Range** • **1**: Low. At this level, only requests with obvious attack characteristics are blocked. If a large number of false alarms are reported, this level is recommended. • **2**: Medium. This is the default level, which meets web protection requirements in most scenarios. • **3**: Strict. At this 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.

Parameter	Type	Description
full_detection	Boolean	**Definition** Detection mode in the precise protection rule. **Range** • **false**: Instant detection. If a request matches a configured precise protection rule, WAF immediately ends threat detection and blocks the request. • **true**: Full detection. If a request matches a configured precise protection rule, WAF does not block the request immediately. Instead, WAF continues to detect other threats and then blocks the request.
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>	**Definition** Configurations of intelligent access control protection items. Currently, this feature is still in the open beta test (OBT) phase and available only in certain sites. **Range** N/A
hosts	Array of strings	**Definition** ID array of protected domain names bound to a protection policy. **Range** N/A
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.

Parameter	Type	Description
extend	Map<String,String>	**Definition** Extended field, which is used to store the switch configuration of basic web protection. **Range** N/A
timestamp	Long	**Definition** Time the policy was created. **Range** N/A

Table 4-102 Action

Parameter	Type	Description
category	String	**Definition** Protective action information in feature anti-crawler **Range** • log: Only logs are recorded. • **block**: WAF blocks attacks.

Table 4-103 PolicyAction

Parameter	Type	Description
category	String	**Definition** Basic web protection action (log: record only; block: block) **Range** • block • log
followed_action_id	String	**Definition** Attack penalty rule ID. **Range** N/A

Table 4-104 PolicyOption

Parameter	Type	Description
webattack	Boolean	**Definition** Whether basic web protection is enabled. **Range** • true • false
common	Boolean	**Definition** Whether general check is enabled. **Range** • true • false
crawler	Boolean	**Definition** Reserved parameter. The value is always true and can be ignored. **Range** • true • false
crawler_engine	Boolean	**Definition** Whether the search engine is enabled. **Range** • true • false
crawler_scanner	Boolean	**Definition** Whether the anti-crawler detection is enabled. **Range** • true • false
crawler_script	Boolean	**Definition** Whether the JavaScript anti-crawler is enabled. **Range** • true • false

Parameter	Type	Description
crawler_other	Boolean	**Definition** Whether other crawler check is enabled. **Range** • true • false
webshell	Boolean	**Definition** Whether web shell detection is enabled **Range** • true • false
cc	Boolean	**Definition** Whether the CC attack protection rule is enabled. **Range** • true • false
custom	Boolean	**Definition** Whether precise protection is enabled. **Range** • true • false
whiteblackip	Boolean	**Definition** Whether blacklist and whitelist protection is enabled. **Range** • true • false
geoip	Boolean	**Definition** Whether geolocation access control is enabled. **Range** • true • false

Parameter	Type	Description
ignore	Boolean	**Definition** Whether false alarm masking is enabled. **Range** • true • false
privacy	Boolean	**Definition** Whether data masking is enabled. **Range** • true • false
antitamper	Boolean	**Definition** Whether the web tamper protection is enabled. **Range** • true • false
antileakage	Boolean	**Definition** Whether the information leakage prevention is enabled. **Range** • true • false
bot_enable	Boolean	**Definition** Whether the website anti-crawler function is enabled. **Range** • true • false
modulex_enabled	Boolean	**Definition** 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. **Range** • true • false

Table 4-105 BindHost

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-106 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-107 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-108 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-109 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-110 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-111 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to obtain the policy list in a project. The project ID is specified by project_id.

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

Example Responses

Status code: 200

Request succeeded.


```
{
  "total" : 1,
  "items" : [ {
    "id" : "41cba8aee2e94bcdbf57460874205494",
    "name" : "policy_2FHwFOKz",
    "level" : 2,
    "action" : {
      "category" : "log"
    },
    "options" : {
      "webattack" : true,
      "common" : true,
      "crawler" : true,
      "crawler_engine" : false,
      "crawler_scanner" : true,
      "crawler_script" : false,
      "crawler_other" : false,
      "webshell" : false,
      "cc" : true,
      "custom" : true,
      "whiteblackip" : true,
      "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.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/waf/policy

Table 4-112 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-113 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-114 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. It can be obtained by calling the IAM API (value of **X-Subject-Token** in the response header). **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** Content type. **Constraints** N/A **Range** N/A **Default Value** application/json;charset=utf8

Table 4-115 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	**Definition** Policy name. **Constraints** N/A **Range** Policy name. Only digits, letters, and underscores (_) are allowed. Maximum length : 64 characters. **Default Value** N/A
log_action_replaced	No	Boolean	Enabling basic web protection to block traffic when **Log only** is set for **Protective Action** for a CC attack protection or precise protection rule. The default value is **true**.

Response Parameters

Status code: 200

Table 4-116 Response body parameters

Parameter	Type	Description
id	String	**Definition** Protection policy ID. **Range** N/A
name	String	**Definition** Protection policy name. **Range** Enter a maximum of 64 characters. Only letters, digits, underscores (_), hyphens (-), colons (:), and periods (.) are allowed.
level	Integer	**Definition** Basic web protection level. **Range** • **1**: Low. At this level, only requests with obvious attack characteristics are blocked. If a large number of false alarms are reported, this level is recommended. • **2**: Medium. This is the default level, which meets web protection requirements in most scenarios. • **3**: Strict. At this 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.

Parameter	Type	Description
full_detection	Boolean	**Definition** Detection mode in the precise protection rule. **Range** • **false**: Instant detection. If a request matches a configured precise protection rule, WAF immediately ends threat detection and blocks the request. • **true**: Full detection. If a request matches a configured precise protection rule, WAF does not block the request immediately. Instead, WAF continues to detect other threats and then blocks the request.
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>	**Definition** Configurations of intelligent access control protection items. Currently, this feature is still in the open beta test (OBT) phase and available only in certain sites. **Range** N/A
hosts	Array of strings	**Definition** ID array of protected domain names bound to a protection policy. **Range** N/A
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.

Parameter	Type	Description
extend	Map<String,String>	**Definition** Extended field, which is used to store the switch configuration of basic web protection. **Range** N/A
timestamp	Long	**Definition** Time the policy was created. **Range** N/A

Table 4-117 Action

Parameter	Type	Description
category	String	**Definition** Protective action information in feature anti-crawler **Range** • log: Only logs are recorded. • **block**: WAF blocks attacks.

Table 4-118 PolicyAction

Parameter	Type	Description
category	String	**Definition** Basic web protection action (log: record only; block: block) **Range** • block • log
followed_action_id	String	**Definition** Attack penalty rule ID. **Range** N/A

Table 4-119 PolicyOption

Parameter	Type	Description
webattack	Boolean	**Definition** Whether basic web protection is enabled. **Range** • true • false
common	Boolean	**Definition** Whether general check is enabled. **Range** • true • false
crawler	Boolean	**Definition** Reserved parameter. The value is always true and can be ignored. **Range** • true • false
crawler_engine	Boolean	**Definition** Whether the search engine is enabled. **Range** • true • false
crawler_scanner	Boolean	**Definition** Whether the anti-crawler detection is enabled. **Range** • true • false
crawler_script	Boolean	**Definition** Whether the JavaScript anti-crawler is enabled. **Range** • true • false

Parameter	Type	Description
crawler_other	Boolean	**Definition** Whether other crawler check is enabled. **Range** • true • false
webshell	Boolean	**Definition** Whether web shell detection is enabled **Range** • true • false
cc	Boolean	**Definition** Whether the CC attack protection rule is enabled. **Range** • true • false
custom	Boolean	**Definition** Whether precise protection is enabled. **Range** • true • false
whiteblackip	Boolean	**Definition** Whether blacklist and whitelist protection is enabled. **Range** • true • false
geoip	Boolean	**Definition** Whether geolocation access control is enabled. **Range** • true • false

Parameter	Type	Description
ignore	Boolean	**Definition** Whether false alarm masking is enabled. **Range** • true • false
privacy	Boolean	**Definition** Whether data masking is enabled. **Range** • true • false
antitamper	Boolean	**Definition** Whether the web tamper protection is enabled. **Range** • true • false
antileakage	Boolean	**Definition** Whether the information leakage prevention is enabled. **Range** • true • false
bot_enable	Boolean	**Definition** Whether the website anti-crawler function is enabled. **Range** • true • false
modulex_enabled	Boolean	**Definition** 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. **Range** • true • false

Table 4-120 BindHost

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-121 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-122 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-123 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-124 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 403

Table 4-125 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-126 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-127 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-128 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to create a protection policy named demo in a specific project. The project ID is specified by project_id.

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

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

Example Responses

Status code: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
```



```
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "antileakage" : false,
    "bot_enable" : true,
    "modulex_enabled" : false
  },
  "hosts" : [ ],
  "extend" : { },
  "timestamp" : 1650529538732,
  "full_detection" : false,
  "bind_host" : [ ]
}
```


Status Codes

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

Error Codes

See **Error Codes**.

4.2.3 Querying a Policy by ID

Function

This API is used to query a policy by ID.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-129 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A
policy_id	Yes	String	**Definition** Protection policy ID. You can call the **ListPolicy** API to obtain the policy ID. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-130 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-131 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. It can be obtained by calling the IAM API (value of **X-Subject-Token** in the response header). **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** Content type. **Constraints** N/A **Range** N/A **Default Value** application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-132 Response body parameters

Parameter	Type	Description
id	String	**Definition** Protection policy ID. **Range** N/A
name	String	**Definition** Protection policy name. **Range** Enter a maximum of 64 characters. Only letters, digits, underscores (_), hyphens (-), colons (:), and periods (.) are allowed.

Parameter	Type	Description
level	Integer	**Definition** Basic web protection level. **Range** • **1**: Low. At this level, only requests with obvious attack characteristics are blocked. If a large number of false alarms are reported, this level is recommended. • **2**: Medium. This is the default level, which meets web protection requirements in most scenarios. • **3**: Strict. At this 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.
full_detection	Boolean	**Definition** Detection mode in the precise protection rule. **Range** • **false**: Instant detection. If a request matches a configured precise protection rule, WAF immediately ends threat detection and blocks the request. • **true**: Full detection. If a request matches a configured precise protection rule, WAF does not block the request immediately. Instead, WAF continues to detect other threats and then blocks the request.
robot_action	**Action** object	Protective actions for each rule in anti-crawler protection.
action	**PolicyAction** object	Protective action
options	**PolicyOption** object	Whether a protection type is enabled in protection policy.

Parameter	Type	Description
modulex_options	Map<String,Object>	**Definition** Configurations of intelligent access control protection items. Currently, this feature is still in the open beta test (OBT) phase and available only in certain sites. **Range** N/A
hosts	Array of strings	**Definition** ID array of protected domain names bound to a protection policy. **Range** N/A
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>	**Definition** Extended field, which is used to store the switch configuration of basic web protection. **Range** N/A
timestamp	Long	**Definition** Time the policy was created. **Range** N/A

Table 4-133 Action

Parameter	Type	Description
category	String	**Definition** Protective action information in feature anti-crawler **Range** • log: Only logs are recorded. • **block**: WAF blocks attacks.

Table 4-134 PolicyAction

Parameter	Type	Description
category	String	**Definition** Basic web protection action (log: record only; block: block) **Range** • block • log
followed_action_id	String	**Definition** Attack penalty rule ID. **Range** N/A

Table 4-135 PolicyOption

Parameter	Type	Description
webattack	Boolean	**Definition** Whether basic web protection is enabled. **Range** • true • false
common	Boolean	**Definition** Whether general check is enabled. **Range** • true • false
crawler	Boolean	**Definition** Reserved parameter. The value is always true and can be ignored. **Range** • true • false
crawler_engine	Boolean	**Definition** Whether the search engine is enabled. **Range** • true • false

Parameter	Type	Description
crawler_scanner	Boolean	**Definition** Whether the anti-crawler detection is enabled. **Range** • true • false
crawler_script	Boolean	**Definition** Whether the JavaScript anti-crawler is enabled. **Range** • true • false
crawler_other	Boolean	**Definition** Whether other crawler check is enabled. **Range** • true • false
webshell	Boolean	**Definition** Whether web shell detection is enabled **Range** • true • false
cc	Boolean	**Definition** Whether the CC attack protection rule is enabled. **Range** • true • false
custom	Boolean	**Definition** Whether precise protection is enabled. **Range** • true • false

Parameter	Type	Description
whiteblackip	Boolean	**Definition** Whether blacklist and whitelist protection is enabled. **Range** • true • false
geoip	Boolean	**Definition** Whether geolocation access control is enabled. **Range** • true • false
ignore	Boolean	**Definition** Whether false alarm masking is enabled. **Range** • true • false
privacy	Boolean	**Definition** Whether data masking is enabled. **Range** • true • false
antitamper	Boolean	**Definition** Whether the web tamper protection is enabled. **Range** • true • false
antileakage	Boolean	**Definition** Whether the information leakage prevention is enabled. **Range** • true • false

Parameter	Type	Description
bot_enable	Boolean	**Definition** Whether the website anti-crawler function is enabled. **Range** • true • false
modulex_enabled	Boolean	**Definition** 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. **Range** • true • false

Table 4-136 BindHost

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Type	Description
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-137 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-138 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-139 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-140 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-141 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-142 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to query details about a protection policy in a specific project. The project is specified by project_id, and the policy is specified by policy_id.

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

Example Responses

Status code: 200

OK

```
{
  "id" : "38ff0cb9a10e4d5293c642bc0350fa6d",
  "name" : "demo",
  "level" : 2,
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
```



```
    "whiteblackip" : true,
    "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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-143 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A
policy_id	Yes	String	**Definition** Protection policy ID. You can call the **ListPolicy** API to obtain the policy ID. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-144 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-145 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. It can be obtained by calling the IAM API (value of **X-Subject-Token** in the response header). **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** Content type. **Constraints** N/A **Range** N/A **Default Value** application/json;charset=utf8

Table 4-146 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	**Definition** Policy name. **Constraints** N/A **Range** Policy name. Only digits, letters, and underscores (_) are allowed. Maximum length : 64 characters. **Default Value** N/A

Parameter	Mandatory	Type	Description
level	No	Integer	**Definition** Basic web protection level. **Constraints** N/A **Range** • **1**: Low. At this level, only requests with obvious attack characteristics are blocked. If a large number of false alarms are reported, this level is recommended. • **2**: Medium. This is the default level, which meets web protection requirements in most scenarios. • **3**: Strict. At this 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 Value** N/A

Parameter	Mandatory	Type	Description
full_detection	No	Boolean	**Definition** Detection mode in the precise protection rule. **Constraints** N/A **Range** • **false**: Instant detection. If a request matches a configured precise protection rule, WAF immediately ends threat detection and blocks the request. • **true**: Full detection. If a request matches a configured precise protection rule, WAF does not block the request immediately. Instead, WAF continues to detect other threats and then blocks the request. **Default Value** N/A
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>	**Definition** Configurations of intelligent access control protection items. Currently, this feature is still in the open beta test (OBT) phase and available only in certain sites. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
hosts	No	Array of strings	**Definition** ID array of protected domain names bound to the protection policy. (This parameter is reserved for future function expansion and can be ignored.) **Constraints** N/A **Range** N/A **Default Value** N/A
bind_host	No	Array of **BindHost** objects	Array of domain names protected with the protection policy. Compared with the **hosts** field, this field contains more details. This parameter cannot be edited and is reserved for extended functions. You can ignore it.
extend	No	Map<String,String>	**Definition** Extended field, which is used to store basic web protection configurations. For details, see the example. • **deep_decode**: deep detection • **check_all_headers**: header detection • **shiro_rememberMe_enable**: Shiro decryption detection **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-147 Action

Parameter	Mandatory	Type	Description
category	No	String	**Definition** Protective action information in feature anti-crawler **Range** • log: Only logs are recorded. • **block**: WAF blocks attacks.

Table 4-148 PolicyAction

Parameter	Mandatory	Type	Description
category	No	String	**Definition** Basic web protection action (log: record only; block: block) **Range** • block • log
followed_action_id	No	String	**Definition** Attack penalty rule ID. **Range** N/A

Table 4-149 PolicyOption

Parameter	Mandatory	Type	Description
webattack	No	Boolean	**Definition** Whether basic web protection is enabled. **Range** • true • false
common	No	Boolean	**Definition** Whether general check is enabled. **Range** • true • false

Parameter	Mandatory	Type	Description
crawler	No	Boolean	**Definition** Reserved parameter. The value is always true and can be ignored. **Range** • true • false
crawler_engine	No	Boolean	**Definition** Whether the search engine is enabled. **Range** • true • false
crawler_scanner	No	Boolean	**Definition** Whether the anti-crawler detection is enabled. **Range** • true • false
crawler_script	No	Boolean	**Definition** Whether the JavaScript anti-crawler is enabled. **Range** • true • false
crawler_other	No	Boolean	**Definition** Whether other crawler check is enabled. **Range** • true • false
webshell	No	Boolean	**Definition** Whether web shell detection is enabled **Range** • true • false

Parameter	Mandatory	Type	Description
cc	No	Boolean	**Definition** Whether the CC attack protection rule is enabled. **Range** • true • false
custom	No	Boolean	**Definition** Whether precise protection is enabled. **Range** • true • false
whiteblackip	No	Boolean	**Definition** Whether blacklist and whitelist protection is enabled. **Range** • true • false
geoip	No	Boolean	**Definition** Whether geolocation access control is enabled. **Range** • true • false
ignore	No	Boolean	**Definition** Whether false alarm masking is enabled. **Range** • true • false
privacy	No	Boolean	**Definition** Whether data masking is enabled. **Range** • true • false

Parameter	Mandatory	Type	Description
antitamper	No	Boolean	**Definition** Whether the web tamper protection is enabled. **Range** • true • false
antileakage	No	Boolean	**Definition** Whether the information leakage prevention is enabled. **Range** • true • false
bot_enable	No	Boolean	**Definition** Whether the website anti-crawler function is enabled. **Range** • true • false
modulex_enabled	No	Boolean	**Definition** 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. **Range** • true • false

Table 4-150 BindHost

Parameter	Mandatory	Type	Description
id	No	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	No	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A
waf_type	No	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	No	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Response Parameters

Status code: 200

Table 4-151 Response body parameters

Parameter	Type	Description
id	String	**Definition** Protection policy ID. **Range** N/A
name	String	**Definition** Protection policy name. **Range** Enter a maximum of 64 characters. Only letters, digits, underscores (_), hyphens (-), colons (:), and periods (.) are allowed.
level	Integer	**Definition** Basic web protection level. **Range** • **1**: Low. At this level, only requests with obvious attack characteristics are blocked. If a large number of false alarms are reported, this level is recommended. • **2**: Medium. This is the default level, which meets web protection requirements in most scenarios. • **3**: Strict. At this 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.

Parameter	Type	Description
full_detection	Boolean	**Definition** Detection mode in the precise protection rule. **Range** • **false**: Instant detection. If a request matches a configured precise protection rule, WAF immediately ends threat detection and blocks the request. • **true**: Full detection. If a request matches a configured precise protection rule, WAF does not block the request immediately. Instead, WAF continues to detect other threats and then blocks the request.
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>	**Definition** Configurations of intelligent access control protection items. Currently, this feature is still in the open beta test (OBT) phase and available only in certain sites. **Range** N/A
hosts	Array of strings	**Definition** ID array of protected domain names bound to a protection policy. **Range** N/A
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.

Parameter	Type	Description
extend	Map<String,String>	**Definition** Extended field, which is used to store the switch configuration of basic web protection. **Range** N/A
timestamp	Long	**Definition** Time the policy was created. **Range** N/A

Table 4-152 Action

Parameter	Type	Description
category	String	**Definition** Protective action information in feature anti-crawler **Range** • log: Only logs are recorded. • **block**: WAF blocks attacks.

Table 4-153 PolicyAction

Parameter	Type	Description
category	String	**Definition** Basic web protection action (log: record only; block: block) **Range** • block • log
followed_action_id	String	**Definition** Attack penalty rule ID. **Range** N/A

Table 4-154 PolicyOption

Parameter	Type	Description
webattack	Boolean	**Definition** Whether basic web protection is enabled. **Range** • true • false
common	Boolean	**Definition** Whether general check is enabled. **Range** • true • false
crawler	Boolean	**Definition** Reserved parameter. The value is always true and can be ignored. **Range** • true • false
crawler_engine	Boolean	**Definition** Whether the search engine is enabled. **Range** • true • false
crawler_scanner	Boolean	**Definition** Whether the anti-crawler detection is enabled. **Range** • true • false
crawler_script	Boolean	**Definition** Whether the JavaScript anti-crawler is enabled. **Range** • true • false

Parameter	Type	Description
crawler_other	Boolean	**Definition** Whether other crawler check is enabled. **Range** • true • false
webshell	Boolean	**Definition** Whether web shell detection is enabled **Range** • true • false
cc	Boolean	**Definition** Whether the CC attack protection rule is enabled. **Range** • true • false
custom	Boolean	**Definition** Whether precise protection is enabled. **Range** • true • false
whiteblackip	Boolean	**Definition** Whether blacklist and whitelist protection is enabled. **Range** • true • false
geoip	Boolean	**Definition** Whether geolocation access control is enabled. **Range** • true • false

Parameter	Type	Description
ignore	Boolean	**Definition** Whether false alarm masking is enabled. **Range** • true • false
privacy	Boolean	**Definition** Whether data masking is enabled. **Range** • true • false
antitamper	Boolean	**Definition** Whether the web tamper protection is enabled. **Range** • true • false
antileakage	Boolean	**Definition** Whether the information leakage prevention is enabled. **Range** • true • false
bot_enable	Boolean	**Definition** Whether the website anti-crawler function is enabled. **Range** • true • false
modulex_enabled	Boolean	**Definition** 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. **Range** • true • false

Table 4-155 BindHost

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-156 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-157 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-158 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-159 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-160 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-161 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

- The following example shows how to modify basic web protection settings, including enabling deep inspection, header inspection, and Shiro decryption check, for a specific policy in a project. The project is specified by project_id, and the policy is specified by policy_id.

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

{
  "extend" : {
    "extend" : "{\"deep_decode\":true,\"check_all_headers\":true,\"shiro_rememberMe_enable\":true}"
  }
}
```

- The following example shows how to disable whitelist and blacklist protection for a specific policy in a project. The project is specified by project_id, and the policy is specified by policy_id.

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

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

Example Responses

Status code: 200

OK

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


Status Codes

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

Error Codes

See **Error Codes**.

4.2.5 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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-162 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Parameter	Mandatory	Type	Description
policy_id	Yes	String	**Definition** Protection policy ID. You can call the **ListPolicy** API to obtain the policy ID. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-163 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-164 Request header parameters

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

Response Parameters

Status code: 200

Table 4-165 Response body parameters

Parameter	Type	Description
id	String	**Definition** Protection policy ID. **Range** N/A

Parameter	Type	Description
name	String	**Definition** Protection policy name. **Range** Enter a maximum of 64 characters. Only letters, digits, underscores (_), hyphens (-), colons (:), and periods (.) are allowed.
level	Integer	**Definition** Basic web protection level. **Range** • **1**: Low. At this level, only requests with obvious attack characteristics are blocked. If a large number of false alarms are reported, this level is recommended. • **2**: Medium. This is the default level, which meets web protection requirements in most scenarios. • **3**: Strict. At this 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.
full_detection	Boolean	**Definition** Detection mode in the precise protection rule. **Range** • **false**: Instant detection. If a request matches a configured precise protection rule, WAF immediately ends threat detection and blocks the request. • **true**: Full detection. If a request matches a configured precise protection rule, WAF does not block the request immediately. Instead, WAF continues to detect other threats and then blocks the request.
robot_action	**Action** object	Protective actions for each rule in anti-crawler protection.

Parameter	Type	Description
action	**PolicyAction** object	Protective action
options	**PolicyOption** object	Whether a protection type is enabled in protection policy.
modulex_options	Map<String,Object>	**Definition** Configurations of intelligent access control protection items. Currently, this feature is still in the open beta test (OBT) phase and available only in certain sites. **Range** N/A
hosts	Array of strings	**Definition** ID array of protected domain names bound to a protection policy. **Range** N/A
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>	**Definition** Extended field, which is used to store the switch configuration of basic web protection. **Range** N/A
timestamp	Long	**Definition** Time the policy was created. **Range** N/A

Table 4-166 Action

Parameter	Type	Description
category	String	**Definition** Protective action information in feature anti-crawler **Range** • log: Only logs are recorded. • **block**: WAF blocks attacks.

Table 4-167 PolicyAction

Parameter	Type	Description
category	String	**Definition** Basic web protection action (log: record only; block: block) **Range** • block • log
followed_action_id	String	**Definition** Attack penalty rule ID. **Range** N/A

Table 4-168 PolicyOption

Parameter	Type	Description
webattack	Boolean	**Definition** Whether basic web protection is enabled. **Range** • true • false
common	Boolean	**Definition** Whether general check is enabled. **Range** • true • false

Parameter	Type	Description
crawler	Boolean	**Definition** Reserved parameter. The value is always true and can be ignored. **Range** • true • false
crawler_engine	Boolean	**Definition** Whether the search engine is enabled. **Range** • true • false
crawler_scanner	Boolean	**Definition** Whether the anti-crawler detection is enabled. **Range** • true • false
crawler_script	Boolean	**Definition** Whether the JavaScript anti-crawler is enabled. **Range** • true • false
crawler_other	Boolean	**Definition** Whether other crawler check is enabled. **Range** • true • false
webshell	Boolean	**Definition** Whether web shell detection is enabled **Range** • true • false

Parameter	Type	Description
cc	Boolean	**Definition** Whether the CC attack protection rule is enabled. **Range** • true • false
custom	Boolean	**Definition** Whether precise protection is enabled. **Range** • true • false
whiteblackip	Boolean	**Definition** Whether blacklist and whitelist protection is enabled. **Range** • true • false
geoip	Boolean	**Definition** Whether geolocation access control is enabled. **Range** • true • false
ignore	Boolean	**Definition** Whether false alarm masking is enabled. **Range** • true • false
privacy	Boolean	**Definition** Whether data masking is enabled. **Range** • true • false

Parameter	Type	Description
antitamper	Boolean	**Definition** Whether the web tamper protection is enabled. **Range** • true • false
antileakage	Boolean	**Definition** Whether the information leakage prevention is enabled. **Range** • true • false
bot_enable	Boolean	**Definition** Whether the website anti-crawler function is enabled. **Range** • true • false
modulex_enabled	Boolean	**Definition** 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. **Range** • true • false

Table 4-169 BindHost

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-170 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-171 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-172 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-173 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-174 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-175 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to delete a protection policy in a specific project. The project is specified by project_id, and the policy is specified by policy_id.

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

Example Responses

Status code: 200

Request succeeded.


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


Status Codes

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

Error Codes

See **Error Codes**.

4.2.6 Updating the Domain Name Protection Policy

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-176 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Parameter	Mandatory	Type	Description
policy_id	Yes	String	**Definition** Protection policy ID. You can call the **ListPolicy** API to obtain the policy ID. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-177 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Parameter	Mandatory	Type	Description
hosts	Yes	String	**Definition** Domain name ID. You can call the **ListHost** API to obtain the domain name ID. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Request Parameters

Table 4-178 Request header parameters

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

Response Parameters

Status code: 200

Table 4-179 Response body parameters

Parameter	Type	Description
id	String	**Definition** Protection policy ID. **Range** N/A
name	String	**Definition** Protection policy name. **Range** Enter a maximum of 64 characters. Only letters, digits, underscores (_), hyphens (-), colons (:), and periods (.) are allowed.
level	Integer	**Definition** Basic web protection level. **Range** • **1**: Low. At this level, only requests with obvious attack characteristics are blocked. If a large number of false alarms are reported, this level is recommended. • **2**: Medium. This is the default level, which meets web protection requirements in most scenarios. • **3**: Strict. At this 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.

Parameter	Type	Description
full_detection	Boolean	**Definition** Detection mode in the precise protection rule. **Range** • **false**: Instant detection. If a request matches a configured precise protection rule, WAF immediately ends threat detection and blocks the request. • **true**: Full detection. If a request matches a configured precise protection rule, WAF does not block the request immediately. Instead, WAF continues to detect other threats and then blocks the request.
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>	**Definition** Configurations of intelligent access control protection items. Currently, this feature is still in the open beta test (OBT) phase and available only in certain sites. **Range** N/A
hosts	Array of strings	**Definition** ID array of protected domain names bound to a protection policy. **Range** N/A
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.

Parameter	Type	Description
extend	Map<String,String>	**Definition** Extended field, which is used to store the switch configuration of basic web protection. **Range** N/A
timestamp	Long	**Definition** Time the policy was created. **Range** N/A

Table 4-180 Action

Parameter	Type	Description
category	String	**Definition** Protective action information in feature anti-crawler **Range** • log: Only logs are recorded. • **block**: WAF blocks attacks.

Table 4-181 PolicyAction

Parameter	Type	Description
category	String	**Definition** Basic web protection action (log: record only; block: block) **Range** • block • log
followed_action_id	String	**Definition** Attack penalty rule ID. **Range** N/A

Table 4-182 PolicyOption

Parameter	Type	Description
webattack	Boolean	**Definition** Whether basic web protection is enabled. **Range** • true • false
common	Boolean	**Definition** Whether general check is enabled. **Range** • true • false
crawler	Boolean	**Definition** Reserved parameter. The value is always true and can be ignored. **Range** • true • false
crawler_engine	Boolean	**Definition** Whether the search engine is enabled. **Range** • true • false
crawler_scanner	Boolean	**Definition** Whether the anti-crawler detection is enabled. **Range** • true • false
crawler_script	Boolean	**Definition** Whether the JavaScript anti-crawler is enabled. **Range** • true • false

Parameter	Type	Description
crawler_other	Boolean	**Definition** Whether other crawler check is enabled. **Range** • true • false
webshell	Boolean	**Definition** Whether web shell detection is enabled **Range** • true • false
cc	Boolean	**Definition** Whether the CC attack protection rule is enabled. **Range** • true • false
custom	Boolean	**Definition** Whether precise protection is enabled. **Range** • true • false
whiteblackip	Boolean	**Definition** Whether blacklist and whitelist protection is enabled. **Range** • true • false
geoip	Boolean	**Definition** Whether geolocation access control is enabled. **Range** • true • false

Parameter	Type	Description
ignore	Boolean	**Definition** Whether false alarm masking is enabled. **Range** • true • false
privacy	Boolean	**Definition** Whether data masking is enabled. **Range** • true • false
antitamper	Boolean	**Definition** Whether the web tamper protection is enabled. **Range** • true • false
antileakage	Boolean	**Definition** Whether the information leakage prevention is enabled. **Range** • true • false
bot_enable	Boolean	**Definition** Whether the website anti-crawler function is enabled. **Range** • true • false
modulex_enabled	Boolean	**Definition** 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. **Range** • true • false

Table 4-183 BindHost

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-184 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-185 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-186 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-187 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-188 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-189 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to change a domain name added to a protection policy in a specific project. The project is specified by project_id, and the policy is specified by policy_id. The domain name ID is changed to c0268b883a854adc8a2cd352193b0e13.

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Status Code	Description
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-190 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Parameter	Mandatory	Type	Description
policy_id	Yes	String	**Definition** Protection policy ID. You can call the **ListPolicy** API to obtain the policy ID. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A
ruletype	Yes	String	**Definition** Policy Rule Type **Constraints** N/A **Range** • **whiteblackip**: blacklist and whitelist protection rule • **geoip**: geolocation access control rule • **privacy**: data masking rule • **antitamper**: anti-tamper protection rule • **custom**: precise protection rule • **ignore**: global protection whitelist (formerly false alarm masking) rule • **cc**: CC attack protection rule **Default Value** N/A

Parameter	Mandatory	Type	Description
rule_id	Yes	String	**Definition** Rule ID. You can call the rule list API to obtain the rule ID based on the rule type (**ruletype**). For example, to obtain the ID of a blacklist or whitelist rule (**whiteblackip**), you can call the **ListWhiteblackipRule** API. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-191 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-192 Request header parameters

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

Table 4-193 Request body parameters

Parameter	Mandatory	Type	Description
status	No	Integer	**Definition** Status **Constraints** N/A **Range** • 0: disabled • 1: enabled **Default Value** N/A

Response Parameters

Status code: 200

Table 4-194 Response body parameters

Parameter	Type	Description
id	String	**Definition** Rule ID. **Range** N/A
policyid	String	**Definition** Protection policy ID. **Range** N/A
timestamp	Long	**Definition** Rule creation time. **Range** N/A
description	String	**Definition** Rule description. **Range** N/A
status	Integer	**Definition** Status **Range** • 0: disabled • 1: enabled

Status code: 400

Table 4-195 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-196 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-197 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-198 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-199 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-200 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

{
  "status" : 0
}
```

Example Responses

Status code: 200

OK

```
{
  "id" : "709bfd0d62a9410394ffa9e25eb82c36",
  "policyid" : "62fd7f8c36234a4ebedabc2ce451ed45",
  "timestamp" : 1650362797070,
```



```
  "description" : "demo",
  "status" : 0
}
```

Status Codes

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

Error Codes

See **Error Codes**.

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

Function

Querying Global Protection Whitelist (Formerly False Alarm Masking) Rules

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-201 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. 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 4-202 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the **ListEnterpriseProject** API of EPS. To query resources associated with all enterprise projects in the current account, specify parameter **all_granted_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 4-203 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.

Response Parameters

Status code: 200

Table 4-204 Response body parameters

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

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

Table 4-205 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.
url	String	The path for false masking alarms. This parameter is available only when **mode** is set to **0**.

Parameter	Type	Description
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. • To bypass the basic web protection, set this parameter to **all**. • To bypass all WAF protection, set this parameter to **bypass**. **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
mode	Integer	Version number. **0**: indicates the old version V1. **1**: indicates the new version V2. If the value of mode is **0**, the **conditions** and **multi_conditions** fields do not exist, and the **url** and **url_logic** fields exist. If the value of mode is **1**, the **url** and **url_logic** fields do not exist, and either the **conditions** field or the **multi_conditions** field exists. This is determined by the actual results returned.

Parameter	Type	Description
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	**IgnoreAdvanced** object	Advanced settings.

Table 4-206 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 4-207 IgnoreAdvanced

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**.
contents	Array of strings	Subfield of the specified field type. The default value is **all**.

Status code: 400

Table 4-208 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-209 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-210 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-211 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 403

Table 4-212 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-213 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-214 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-215 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

Example Responses

Status code: 200

OK

```
{
  "total" : 1,
  "items" : [ {
    "id" : "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.
401	The token does not have required permissions.
403	Insufficient resource quota.
500	Internal server error.

Error Codes

See **Error Codes**.

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

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-216 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. 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 4-217 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 4-218 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.

Table 4-219 Request body parameters

Parameter	Mandatory	Type	Description
domain	Yes	Array of strings	Domain names or websites to be protected. If the array length is **0**, the rule takes effect for all domain names or websites. If Cloud Mode - Load balancer access is used for the domain name, set this parameter in the format of [/topic/body/section/table/tgroup/tbody/row/entry/p/br {""}) (br]:<id>, for example, www.example.com:id. If all listeners of the load balancer bound to the domain name are protected by WAF, set this parameter to the load balancer ID. Otherwise, set this parameter to the listener ID. To query the load balancer ID, go to the domain name details page on the WAF console. To query the listener ID, go to the **Listeners** tab on the ELB console.

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.

Parameter	Mandatory	Type	Description
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. • To bypass the basic web protection, set this parameter to **all**. • To bypass all WAF protection, set this parameter to **bypass**. **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
advanced	No	**IgnoreAdvanced** object	"Advanced settings.
description	No	String	Description of a masking rule

Table 4-220 CreateCondition

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

Table 4-221 IgnoreAdvanced

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**.
contents	No	Array of strings	Subfield of the specified field type. The default value is **all**.

Response Parameters

Status code: 200

Table 4-222 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.
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.

Parameter	Type	Description
conditions	Array of **Condition** objects	Condition list
advanced	**IgnoreAdvanced** object	"Advanced settings.
domain	Array of strings	Protected domain name or website

Table 4-223 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 4-224 IgnoreAdvanced

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**.
contents	Array of strings	Subfield of the specified field type. The default value is **all**.

Status code: 400

Table 4-225 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-226 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-227 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-228 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-229 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-230 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

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

Example Responses

Status code: 200

OK

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


Status Codes

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

Error Codes

See **Error Codes**.

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

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-231 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. Then, in the **Projects** area, view **Project ID** of the corresponding project.
policy_id	Yes	String	Policy ID. It can be obtained by calling the **ListPolicy** API.

Parameter	Mandatory	Type	Description
rule_id	Yes	String	ID of 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 4-232 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 4-233 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.

Response Parameters

Status code: 200

Table 4-234 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.
url	String	The path for false masking alarms. This parameter is available only when **mode** is set to **0**.
rule	String	ID of the built-in rule to be masked.You can query the rule ID by choosing **Policies** > **Policy Name** > **Basic Web Protection** > **Protection Rules** on the WAF console or on the event details page.
mode	Integer	Version number. The value can be **0** or **1**. **0**: indicates the old version V1. **1** indicates the new version V2. When the value of **mode** is **0**, the **conditions** field does not exist, but the **url** and **url_logic** fields exist. When the value of **mode** is **1**, the **url** and **url_logic** fields do not exist, but the **conditions** field exists.
url_logic	String	URL match logic
conditions	Array of **Condition** objects	Filter
advanced	**IgnoreAdvanced** object	"Advanced settings.
domains	Array of strings	Protected domain name or website

Table 4-235 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.

Parameter	Type	Description
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 4-236 IgnoreAdvanced

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**.
contents	Array of strings	Subfield of the specified field type. The default value is **all**.

Status code: 400

Table 4-237 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-238 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-239 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-240 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-241 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-242 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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


Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-243 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. 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 4-244 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the **ListEnterpriseProject** API of EPS. To query resources associated with all enterprise projects in the current account, specify parameter **all_granted_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.
name	No	String	Name of the whitelist or blacklist rule.

Request Parameters

Table 4-245 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.

Response Parameters

Status code: 200

Table 4-246 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.
size	Integer	Number of the Ip addresses

Table 4-247 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
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.

Parameter	Type	Description
ip_group	**Ip_group** object	IP address group.
time_mode	String	The rule application method. Default value: **permanent**, indicating that the rule will be applied once it is configured.
start	Long	Effective start time. This parameter is valid only when time_Mode is set to **customize**.
terminal	Long	Effective end time. This parameter is valid only when time_Mode is set to **customize**.

Table 4-248 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 4-249 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-250 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-251 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-252 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-253 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-254 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

Example Responses

Status code: 200

OK

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


Status Codes

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

Error Codes

See **Error Codes**.

4.3.6 Creating a Blacklist/Whitelist Rule

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-255 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. 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 4-256 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 4-257 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.

Table 4-258 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.

Parameter	Mandatory	Type	Description
ip_group_id	No	String	ID of the created IP address group. Use either this parameter or **addr**. To add an IP address group, go to the WAF console, choose **Objects** > **Address Groups**, and click **Add Address Group**.
time_mode	No	String	The rule application method. Default value: **permanent**, indicating that the rule will be applied once it is configured. Please enter **customize** when creating a customized effective rule.
start	No	Integer	Effective start time. This parameter is valid only when time_Mode is set to **customize**. Please enter a timestamp.
terminal	No	Integer	Effective end time. This parameter is valid only when time_Mode is set to **customize**. Please enter a timestamp.

Response Parameters

Status code: 200

Table 4-259 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.
time_mode	String	The rule application method. Default value: **permanent**, indicating that the rule will be applied once it is configured.
start	Long	Effective start time. This parameter is valid only when time_Mode is set to **customize**.
terminal	Long	Effective end time. This parameter is valid only when time_Mode is set to **customize**.
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 4-260 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 4-261 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-262 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-263 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-264 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-265 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-266 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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


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

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.7 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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-267 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. 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 **ListWhiteblacki-pRule API.

Table 4-268 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 4-269 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.

Table 4-270 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Name of the whitelist or blacklist rule.

Parameter	Mandatory	Type	Description
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**.
time_mode	No	String	The rule application method. Default value: **permanent**, indicating that the rule will be applied once it is configured. Please enter **customize** when creating a customized effective rule.
start	No	Integer	Effective start time. This parameter is valid only when time_Mode is set to **customize**. Please enter a timestamp.
terminal	No	Integer	Effective end time. This parameter is valid only when time_Mode is set to **customize**. Please enter a timestamp.

Response Parameters

Status code: 200

Table 4-271 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.
time_mode	String	The rule application method. Default value: **permanent**, indicating that the rule will be applied once it is configured.
start	Long	Effective start time. This parameter is valid only when time_Mode is set to **customize**.
terminal	Long	Effective end time. This parameter is valid only when time_Mode is set to **customize**.
ip_group	**Ip_group** object	IP address group

Table 4-272 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 4-273 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-274 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-275 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-276 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-277 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-278 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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


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

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.8 Deleting a Blacklist or Whitelist Rule

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-279 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. 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 4-280 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 4-281 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.

Response Parameters

Status code: 200

Table 4-282 Response body parameters

Parameter	Type	Description
id	String	Rule ID.

Parameter	Type	Description
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.
time_mode	String	The rule application method. Default value: **permanent**, indicating that the rule will be applied once it is configured.
start	Long	Effective start time. This parameter is valid only when time_Mode is set to **customize**.
terminal	Long	Effective end time. This parameter is valid only when time_Mode is set to **customize**.
ip_group	**Ip_group** object	IP address group

Table 4-283 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 4-284 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-285 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-286 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-287 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-288 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-289 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.9 Querying a Data Masking Rule

Function

Querying a Data Masking Rule

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-290 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei 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 4-291 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the **ListEnterpriseProject** API of EPS. To query resources associated with all enterprise projects in the current account, specify parameter **all_granted_eps**.

Request Parameters

Table 4-292 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.

Response Parameters

Status code: 200

Table 4-293 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	Name of the masked field.

Status code: 400

Table 4-294 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-295 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-296 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-297 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-298 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-299 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

Example Responses

Status code: 200

Request sent.

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



```
  "index" : "demo1"
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.3.10 Creating a Data Masking Rule

Function

This API is used to create a data masking rule.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-300 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei 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 4-301 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.

Table 4-303 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

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 4-304 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

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 4-305 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-306 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-307 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-308 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-309 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-310 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.11 Updating a Data Masking Rule

Function

This API is used to update a data masking rule.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-311 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei 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 4-312 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 4-313 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.

Table 4-314 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
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 4-315 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
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 4-316 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-317 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-318 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-319 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-320 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-321 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

{
```



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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

Status Code	Description
200	Request succeeded.
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-322 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei 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 4-323 Query Parameters

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

Request Parameters

Table 4-324 Request header parameters

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

Response Parameters

Status code: 200

Table 4-325 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 4-326 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-327 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-328 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-329 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-330 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-331 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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


Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.13 Querying the List of Geolocation Access Control Rules

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-332 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei 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 4-333 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the **ListEnterpriseProject** API of EPS. To query resources associated with all enterprise projects in the current account, specify parameter **all_granted_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 4-334 Request header parameters

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

Response Parameters

Status code: 200

Table 4-335 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 4-336 GeOIpItem

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

Parameter	Type	Description
geoip	String	Locations that can be configured in the geolocation access control rule: (Countries/Regions outside China: **CA**: Canada, **South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia Cities inside China: **GD**: Guangdong, **FJ**: Fujian, **JL**: Jilin, **LN**: Liaoning, **TW**: Taiwan (China), **GZ**: Guizhou, **AH**: Anhui, **HL**: Heilongjiang, **HA**: Henan, **SC**: Sichuan, **HE**: Hebei, **YN**: Yunnan, **HB**: Hubei, **HI**: Hainan, **QH**: Qinghai, **HN**: Hunan, **JX**: Jiangxi, **SX**: Shanxi, **SN**: Shaanxi, **ZJ**: Zhejiang, **GS**: Gansu, **JS**: Jiangsu, **SD**: Shandong, **BJ**: Beijing, **SH**: Shanghai, **TJ**: Tianjin, **CQ**: Chongqing, **MO**: Macao (China), **HK**: Hong Kong (China), **NX**: Ningxia, **GX**: Guangxi, **XJ**: Xinjiang, **XZ**: Xizang, **NM**: Inner Mongolia) For details about the location code, see *Appendix - Geographical Location Codes*.
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. • **1**: enabled. • **0**: disabled.
timestamp	Long	Time the rule is created.

Status code: 400

Table 4-337 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-338 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-339 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-340 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-341 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-342 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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


Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.14 Creating a Geolocation Access Control Rule

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-343 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei 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 4-344 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 4-345 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.

Table 4-346 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: (Countries/Regions outside China: **CA**: Canada, **South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia Cities inside China: **GD**: Guangdong, **FJ**: Fujian, **JL**: Jilin, **LN**: Liaoning, **TW**: Taiwan (China), **GZ**: Guizhou, **AH**: Anhui, **HL**: Heilongjiang, **HA**: Henan, **SC**: Sichuan, **HE**: Hebei, **YN**: Yunnan, **HB**: Hubei, **HI**: Hainan, **QH**: Qinghai, **HN**: Hunan, **JX**: Jiangxi, **SX**: Shanxi, **SN**: Shaanxi, **ZJ**: Zhejiang, **GS**: Gansu, **JS**: Jiangsu, **SD**: Shandong, **BJ**: Beijing, **SH**: Shanghai, **TJ**: Tianjin, **CQ**: Chongqing, **MO**: Macao (China), **HK**: Hong Kong (China), **NX**: Ningxia, **GX**: Guangxi, **XJ**: Xinjiang, **XZ**: Xizang, **NM**: Inner Mongolia) For details about the location code, see *Appendix - Geographical Location Codes*.
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. • **1**: enabled. • **0**: disabled.
description	No	String	Rule description.

Response Parameters

Status code: 200

Table 4-347 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: (Countries/Regions outside China: **CA**: Canada, **South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia Cities inside China: **GD**: Guangdong, **FJ**: Fujian, **JL**: Jilin, **LN**: Liaoning, **TW**: Taiwan (China), **GZ**: Guizhou, **AH**: Anhui, **HL**: Heilongjiang, **HA**: Henan, **SC**: Sichuan, **HE**: Hebei, **YN**: Yunnan, **HB**: Hubei, **HI**: Hainan, **QH**: Qinghai, **HN**: Hunan, **JX**: Jiangxi, **SX**: Shanxi, **SN**: Shaanxi, **ZJ**: Zhejiang, **GS**: Gansu, **JS**: Jiangsu, **SD**: Shandong, **BJ**: Beijing, **SH**: Shanghai, **TJ**: Tianjin, **CQ**: Chongqing, **MO**: Macao (China), **HK**: Hong Kong (China), **NX**: Ningxia, **GX**: Guangxi, **XJ**: Xinjiang, **XZ**: Xizang, **NM**: Inner Mongolia) For details about the location code, see *Appendix - Geographical Location Codes*.
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. • **1**: enabled. • **0**: disabled.
timestamp	Long	Time the rule is created.

Status code: 400

Table 4-348 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-349 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-350 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-351 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-352 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-353 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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


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

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.15 Updating a Geolocation Access Control Rule

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-354 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei 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 4-355 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 4-356 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.

Table 4-357 Request body parameters

Parameter	Mandatory	Type	Description
name	No	String	Name of the geolocation access control rue.
description	No	String	Description.
geoip	Yes	String	Locations that can be configured in the geolocation access control rule: (Countries/Regions outside China: **CA**: Canada, **South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia Cities inside China: **GD**: Guangdong, **FJ**: Fujian, **JL**: Jilin, **LN**: Liaoning, **TW**: Taiwan (China), **GZ**: Guizhou, **AH**: Anhui, **HL**: Heilongjiang, **HA**: Henan, **SC**: Sichuan, **HE**: Hebei, **YN**: Yunnan, **HB**: Hubei, **HI**: Hainan, **QH**: Qinghai, **HN**: Hunan, **JX**: Jiangxi, **SX**: Shanxi, **SN**: Shaanxi, **ZJ**: Zhejiang, **GS**: Gansu, **JS**: Jiangsu, **SD**: Shandong, **BJ**: Beijing, **SH**: Shanghai, **TJ**: Tianjin, **CQ**: Chongqing, **MO**: Macao (China), **HK**: Hong Kong (China), **NX**: Ningxia, **GX**: Guangxi, **XJ**: Xinjiang, **XZ**: Xizang, **NM**: Inner Mongolia) For details about the location code, see *Appendix - Geographical Location Codes*.
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 4-358 Response body parameters

Parameter	Type	Description
id	String	Rule ID.
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: (Countries/Regions outside China: **CA**: Canada, **South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia Cities inside China: **GD**: Guangdong, **FJ**: Fujian, **JL**: Jilin, **LN**: Liaoning, **TW**: Taiwan (China), **GZ**: Guizhou, **AH**: Anhui, **HL**: Heilongjiang, **HA**: Henan, **SC**: Sichuan, **HE**: Hebei, **YN**: Yunnan, **HB**: Hubei, **HI**: Hainan, **QH**: Qinghai, **HN**: Hunan, **JX**: Jiangxi, **SX**: Shanxi, **SN**: Shaanxi, **ZJ**: Zhejiang, **GS**: Gansu, **JS**: Jiangsu, **SD**: Shandong, **BJ**: Beijing, **SH**: Shanghai, **TJ**: Tianjin, **CQ**: Chongqing, **MO**: Macao (China), **HK**: Hong Kong (China), **NX**: Ningxia, **GX**: Guangxi, **XJ**: Xinjiang, **XZ**: Xizang, **NM**: Inner Mongolia) For details about the location code, see *Appendix - Geographical Location Codes*.
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 4-359 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-360 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-361 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-362 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-363 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-364 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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


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

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.16 Deleting a Geolocation Access Control Rule

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-365 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei 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 4-366 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 4-367 Request header parameters

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

Response Parameters

Status code: 200

Table 4-368 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: (Countries/Regions outside China: **CA**: Canada, **South Africa**: South Africa, **Mexico**: Mexico, **Peru**: Peru, **Indonesia**: Indonesia Cities inside China: **GD**: Guangdong, **FJ**: Fujian, **JL**: Jilin, **LN**: Liaoning, **TW**: Taiwan (China), **GZ**: Guizhou, **AH**: Anhui, **HL**: Heilongjiang, **HA**: Henan, **SC**: Sichuan, **HE**: Hebei, **YN**: Yunnan, **HB**: Hubei, **HI**: Hainan, **QH**: Qinghai, **HN**: Hunan, **JX**: Jiangxi, **SX**: Shanxi, **SN**: Shaanxi, **ZJ**: Zhejiang, **GS**: Gansu, **JS**: Jiangsu, **SD**: Shandong, **BJ**: Beijing, **SH**: Shanghai, **TJ**: Tianjin, **CQ**: Chongqing, **MO**: Macao (China), **HK**: Hong Kong (China), **NX**: Ningxia, **GX**: Guangxi, **XJ**: Xinjiang, **XZ**: Xizang, **NM**: Inner Mongolia) For details about the location code, see *Appendix - Geographical Location Codes*.
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. • **1**: enabled. • **0**: disabled.
description	String	Description.
timestamp	Long	Time the rule is created.

Status code: 400

Table 4-369 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-370 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-371 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-372 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-373 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-374 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

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

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.17 Querying the List of Web Tamper Protection Rules

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-375 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei 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 4-376 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	You can obtain the ID by calling the **ListEnterpriseProject** API of EPS. To query resources associated with all enterprise projects in the current account, specify parameter **all_granted_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 4-377 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.

Response Parameters

Status code: 200

Table 4-378 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 4-379 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 4-380 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-381 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-382 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-383 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-384 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-385 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to query the web tamper protection rule list in a project. The project ID is specified by project_id, and the policy is specified by policy_id.

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.18 Creating a Web Tamper Protection Rule

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-386 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei 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 4-387 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 4-388 Request header parameters

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

Table 4-389 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).

Parameter	Mandatory	Type	Description
url	Yes	String	URL protected by the web tamper protection rule. The value must be in the standard URL format, for example, /admin/xxx or /admin/. *The asterisk (*) indicates the path prefix.
description	No	String	Rule Description

Response Parameters

Status code: 200

Table 4-390 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 4-391 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-392 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-393 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-394 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-395 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-396 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to create a web tamper protection rule in a policy. The project ID is specified by project_id, and the policy ID is specified by policy_id. The website for the rule is www.demo.com, the URL of the rule is /test, and the rule description is demo.

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

{
```



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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.19 Deleting a Web Tamper Protection Rule

Function

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

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-397 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. 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 4-398 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.

Response Parameters

Status code: 200

Table 4-400 Response body parameters

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

Parameter	Type	Description
url	String	URL protected by the web tamper protection rule.
timestamp	Long	Timestamp the rule was created.

Status code: 400

Table 4-401 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-402 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-403 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-404 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-405 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-406 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to delete a web tamper protection rule. The project ID is specified by project_id, the policy ID is specified by policy_id, and the rule ID is specified by rule_id.

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.3.20 Querying the Reference Table List

Function

This API is used to query the reference table list.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/waf/valuelist

Table 4-407 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. Then, in the **Projects** area, view **Project ID** of the corresponding project.

Table 4-408 Query Parameters

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

Request Parameters

Table 4-409 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.

Response Parameters

Status code: 200

Table 4-410 Response body parameters

Parameter	Type	Description
total	Integer	Number of reference tables
items	Array of **ValueListResponseBody** objects	Reference table list

Table 4-411 ValueListResponseBody

Parameter	Type	Description
id	String	ID of the reference table
name	String	Reference table name.
type	String	Reference table type
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 4-412 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-413 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-414 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-415 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-416 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-417 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to query the reference table list in a project. The project ID is specified by project_id.

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


Example Responses

Status code: 200

Request succeeded.


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


Status Codes

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

Error Codes

See **Error Codes**.

4.3.21 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.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/waf/valuelist

Table 4-418 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. Then, in the **Projects** area, view **Project ID** of the corresponding project.

Table 4-419 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 4-420 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.

Table 4-421 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.
type	Yes	String	Reference table type. For details, see the enumeration list.
values	Yes	Array of strings	Value of the reference table

Parameter	Mandatory	Type	Description
description	No	String	Reference table description. The value contains a maximum of 128 characters.

Response Parameters

Status code: 200

Table 4-422 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 4-423 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-424 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-425 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-426 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-427 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-428 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to create a reference table in the project. The project ID is specified by project_id. The reference table name is demo, the reference table type is url, the value is /124, and the description is demo.

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

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

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "e5d9032d8da64d169269175c3e4c2849",
```



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

Status Codes

Status Code	Description
200	Request succeeded.
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-429 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. 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 4-430 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 4-431 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.

Table 4-432 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Reference table name. It can contain 2 to 32 characters.
type	Yes	String	Reference table type. For details, see the enumeration list.
values	No	Array of strings	Value of the reference table
description	No	String	Reference table description. The value contains a maximum of 128 characters.

Response Parameters

Status code: 200

Table 4-433 Response body parameters

Parameter	Type	Description
id	String	ID of the reference table

Parameter	Type	Description
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 4-434 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-435 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-436 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-437 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-438 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-439 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to update a reference table. Its ID is **valuelistid** in the project. The project ID is specified by **project_id**. The reference table name is **RPmvp0m4**, the reference table type is **response_coderl**, the value is **500**, and the description is **demo**.

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

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

Example Responses

Status code: 200

Request succeeded.

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

Status Codes

Status Code	Description
200	Request succeeded.
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-440 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to Huawei Cloud management cons**. 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 4-441 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 4-442 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.

Response Parameters

Status code: 200

Table 4-443 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 4-444 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-445 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-446 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-447 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-448 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-449 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to delete a reference table in a project. The project ID is specified by project_id. The reference table ID is valuelistid.

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

Example Responses

Status code: 200

Request succeeded.

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


Status Codes

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

Error Codes

See **Error Codes**.

4.4 Certificate Management

4.4.1 Querying the List of Certificates

Function

This API is used to query the list of certificates.

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/waf/certificate

Table 4-450 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-451 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Parameter	Mandatory	Type	Description
page	No	Integer	**Definition** Page number of the data to be returned in a query. The default value is 1, indicating that data on the first page is returned. **Constraints** N/A **Range** N/A **Default Value** 1
pagesize	No	Integer	**Definition** Number of results on each page in a pagination query. **Constraints** N/A **Range** The value range is 1 to 100. The default value is **10**, indicating that each page contains 10 results. **Default Value** 10
name	No	String	**Definition** Certificate name. **Constraints** N/A **Range** Enter a maximum of 256 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. **Default Value** N/A

Parameter	Mandatory	Type	Description
host	No	Boolean	**Definition** Whether to obtain the domain name associated with the certificate. **Constraints** N/A **Range** • **true**: Obtain certificates that have been associated with domain names. • **false**: Obtain the certificate that is not associated with any domain name. **Default Value** false
exp_status	No	Integer	**Definition** Certificate expiration status. **Constraints** N/A **Range** • **0**: not expired • **1**: expired • **2**: The certificate will expire in one month. **Default Value** N/A
query_scm	No	Boolean	**Definition** Whether the certificate source service of the query result includes the SCM service **Constraints** Not applicable **Range** • true: The result includes certificates from the SCM service • false: The result does not include certificates from the SCM service **Default Value** false

Request Parameters

Table 4-452 Request header parameters

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

Response Parameters

Status code: 200

Table 4-453 Response body parameters

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

Table 4-454 CertificateBody

Parameter	Type	Description
id	String	**Definition** Certificate ID. **Range** N/A
name	String	**Definition** Certificate name. **Range** N/A
expire_time	Long	**Definition** Timestamp when the certificate expires. **Range** N/A
exp_status	Integer	**Definition** Certificate expiration status. **Range** • **0**: not expired • **1**: expired • **2**: The certificate will expire in one month.
timestamp	Long	**Definition** Certificate upload timestamp. **Range** 13-bit millisecond timestamp.
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-455 BindHost

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-456 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-457 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-458 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-459 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-460 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-461 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to query the certificate list in a project. The project ID is specified by project_id.

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.4.2 Uploading a Certificate

Function

This API is used to upload a certificate.

Calling Method

For details, see **Calling APIs**.

URI

POST /v1/{project_id}/waf/certificate

Table 4-462 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-463 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-464 Request header parameters

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

Table 4-465 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	**Definition** Certificate name. **Constraints** N/A **Range** Enter a maximum of 256 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. **Default Value** N/A

Parameter	Mandatory	Type	Description
content	Yes	String	**Definition** Certificate file. **Constraints** Only certificates and private key files in PEM format are supported. The newline characters in the files must be replaced with \n, as shown in the request example. **Range** N/A **Default Value** N/A
key	Yes	String	**Definition** Certificate private key. **Constraints** Only certificates and private key files in PEM format are supported. The newline characters in the files must be replaced with \n, as shown in the request example. **Range** N/A **Default Value** N/A

Response Parameters

Status code: 200

Table 4-466 Response body parameters

Parameter	Type	Description
id	String	**Definition** Certificate ID. **Range** N/A

Parameter	Type	Description
name	String	**Definition** Certificate name. **Range** N/A
content	String	**Definition** PEM code **Range** N/A
key	String	**Definition** Private key of the certificate, which is in PEM format. **Range** N/A
expire_time	Long	**Definition** Timestamp when the certificate expires. **Range** N/A
exp_status	Integer	**Definition** Certificate expiration status. **Range** • **0**: not expired • **1**: expired • **2**: The certificate will expire in one month.
timestamp	Long	**Definition** Certificate upload timestamp. **Range** 13-bit millisecond timestamp.
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-467 BindHost

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-468 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-469 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-470 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-471 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-472 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-473 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to create a certificate in the project whose project ID is project_id. The certificate name is demo, the certificate content is -------BEGIN CERTIFICATIONATE-----..., and the certificate key is -------BEGIN Private KEY------.....

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

{
  "name" : "demo",
  "content" : "-----BEGIN CERTIFICATE----- \
\nMIIDyzCCArOgAwIBAgIJAN5U0Z4Bh5ccMA0GCSqGSIb3DQEBCwUAMHwxCzAJBgNV
BAYTAlpIMRIwEAYDVQQIDAlHVUFOR0RPTkcxETAPBgNVBAcMCERPTkdHVUFOMQ0w
CwYDVQQKDARERUtFMQswCQYDVQQLDAJESzELMAkGA1UEAwwCT0QxHTAbBgkqhkiG
9w0BCQEWDk8IZC5odWF3ZWkuY29tMB4XDTIxMTExNTA4MTk0MVoXDTIyMTExNTA4
MTk0MVowfDELMAkGA1UEBhMCWkgxEjAQBgNVBAgMCUdVQU5HRE9ORzERMA8GA1UE
Bw**********VQQD
DAJPRDEdMBsGCSqGSIb3DQEJARYOTwhkLmh1YXdlaS5jb20wggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDcoLFK62//r0RHFyweYBj97S4NsJ8Qj0RG+Y02
OgwhQmRiNNjubJwP8Nqqyd86zr+fsSQxKBaBCosn1PcN2Pj2vPJD6NEk4I6VdOWr /
kFYMlOcimhSfW4wt6VakniOKIYGrCxxvQe1X2OyBxT+ocTLRgEIB8ZbvJyPNseg
feLE**********SusXo FQ/WRbBRH7DrQmxGiXsq4VELEr9Nnc/Kywq+9pYi8L
+mKeRL+lcMMbXC/3k6OfMB tVTiwcmS1Mkr3iG03i8u6H7RSvRwyBz9G9sE
+tmJZTPH6lYtAgMBAAGjUDBOMB0G A1UdDgQWBBQprUUFXW
+gIkpzXdrYlsWjfSahWjAfBgNVHSMEGDAWgBQprUUFXW+g IkpzXdrYlsWjfSahWjAMBgNVHRMEBTADAQH/
MA0GCSqGSIb3DQEBCwUAA4IBAQA2 603K**********iOhU 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
G6**********lcGO1n 4urPBHuNLy04GgGw
+vkaqjqOvZrNLVOMMaFWBxsDWBehgSSBQTj+f3NCxneGYtt8 3SCTZQI5nIkb+r/
M455EwKTSXuEsNHoIwx7L6GEPbQECgYEA8IxgK2fYykloICoh
TFJaRAvyjyKa2+Aza4qT9SGY9Y30VPClPjBB1vUu5M9KrFufzlv06nGEcHmpEwOe
8vbRu7nLAQTGYFi8VK63q8w6FlFdAyCG6Sx+BWCfWxJzXsZLAJTfklwi8HsOSlqh
6QN**********fvx mTblG52Z21OyocNq3Tf/
b1ZwoIc1ik6cyBzY6z1bIrbSzArCqm0sb2iD+kJL81O0 /qqdXjBxZUkKiVAMNNp7xJGZHHFKWUxT2+UX/
tlyx4tT4dzrFIkdDXkcMmqfsRxd 1NEVaAaT8SECgYAoU7BPtpIun43YTpfUfr3pSIN6oZeKoxSbw9i4MNC
+4fSDRPC+ 80ImcmZRL7taF+Y7p0jxAOTuIkdJC8NbAiv5J9WzrwQ+5MF2BPB/2bYnRa6tNofH
kZD**********QC9 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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-474 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A
certificate_id	Yes	String	**Definition** ID of the HTTPS certificate. You can call the **ListCertificates** API to obtain the certificate ID. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-475 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-476 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. It can be obtained by calling the IAM API (value of **X-Subject-Token** in the response header). **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** Content type. **Constraints** N/A **Range** N/A **Default Value** application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-477 Response body parameters

Parameter	Type	Description
id	String	**Definition** Certificate ID. **Range** N/A
name	String	**Definition** Certificate name. **Range** N/A
content	String	**Definition** Certificate file, PEM encoding **Range** N/A
key	String	**Definition** Private key of the certificate, which is in PEM format. **Range** N/A
expire_time	Long	**Definition** Timestamp when the certificate expires. **Range** N/A

Parameter	Type	Description
exp_status	Integer	**Definition** Certificate expiration status. **Range** • **0**: not expired • **1**: expired • **2**: The certificate will expire in one month.
timestamp	Long	**Definition** Certificate upload timestamp. **Range** 13-bit millisecond timestamp.
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-478 BindHost

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Type	Description
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-479 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-480 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-481 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-482 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-483 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-484 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to query a certificate in a project. The project ID is specified by project_id, and the certificate ID is specified by certificate_id.

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

Example Responses

Status code: 200

OK

```
{
  "id" : "6e2be127b79f4a418414952ad5d8c59f",
  "name" : "certificatename94319",
  "content" : "-----BEGIN CERTIFICATE-----\nMIIB
+TCCAaOgAwIBAgIUJP9I8OupQ77w0bGL2yWOQXreM4kwDQYJKoZIhvcNAQELBQAwUTELMAkGA1UEBhMC
QVUxEzARBgNVBAgMClNvbWUtU3RhdGUxDzANBgNVBAoMBkh1YXdlaTEcMBoGA1UEAwwTd2FmLmh1YXdl
aW**********MRMwEQYDVQQIDApTb21lLVN0YXRlMQ8wDQYDVQQKDAZIdWF3ZWkxH
DAaBgNVBAMME3dhZi5odWF3ZWljbG91ZC5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIAkEA0UEbMzbvgOJ
TKrKcDUw9xjFqxM7BaQFM3SLsQlmD5hkzygyL1ra
+cWajPJlTCxz9Ph6qldna2+Orl**********wYDV
R0jBBgwFoAUE7ZQNcgl3lmryx1s5gy9mnC1rsYwDwYDVR0TAQH/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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-485 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A
certificate_id	Yes	String	**Definition** ID of the HTTPS certificate. You can call the **ListCertificates** API to obtain the certificate ID. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-486 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-487 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. It can be obtained by calling the IAM API (value of **X-Subject-Token** in the response header). **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** Content type. **Constraints** N/A **Range** N/A **Default Value** application/json;charset=utf8

Table 4-488 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	**Definition** Certificate name. **Constraints** N/A **Range** Enter a maximum of 256 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. **Default Value** N/A
content	No	String	**Definition** Certificate file. **Constraints** Only certificates and private key files in PEM format are supported. The newline characters in the files must be replaced with \n, as shown in the request example. **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
key	No	String	**Definition** Certificate private key. **Constraints** Only certificates and private key files in PEM format are supported. The newline characters in the files must be replaced with \n, as shown in the request example. **Range** N/A **Default Value** N/A

Response Parameters

Status code: 200

Table 4-489 Response body parameters

Parameter	Type	Description
id	String	**Definition** Certificate ID. **Range** N/A
name	String	**Definition** Certificate name. **Range** N/A
expire_time	Long	**Definition** Timestamp when the certificate expires. **Range** N/A
timestamp	Long	**Definition** Certificate upload timestamp. **Range** 13-bit millisecond timestamp.

Status code: 400

Table 4-490 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-491 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-492 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-493 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-494 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-495 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to update a certificate name in a project. The project ID is specified by project_id, and the certificate ID is specified by certificate_id. The certificate name is updated to demo.

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

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

Example Responses

Status code: 200

OK

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

Status Codes

Status Code	Description
200	OK
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-496 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A
certificate_id	Yes	String	**Definition** ID of the HTTPS certificate. You can call the **ListCertificates** API to obtain the certificate ID. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-497 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-498 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. It can be obtained by calling the IAM API (value of **X-Subject-Token** in the response header). **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** Content type. **Constraints** N/A **Range** N/A **Default Value** application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-499 Response body parameters

Parameter	Type	Description
id	String	**Definition** Certificate ID. **Range** N/A
name	String	**Definition** Certificate name. **Range** N/A
content	String	**Definition** PEM code. **Range** N/A
key	String	**Definition** Private key of the certificate, which is in PEM format. **Range** N/A
expire_time	Long	**Definition** Timestamp when the certificate expires. **Range** N/A

Parameter	Type	Description
exp_status	Integer	**Definition** Certificate expiration status. **Range** • **0**: not expired • **1**: expired • **2**: The certificate will expire in one month.
timestamp	Long	**Definition** Certificate upload timestamp. **Range** 13-bit millisecond timestamp.
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-500 BindHost

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Constraints** N/A **Range** N/A **Default Value** N/A
hostname	String	**Definition** Domain name. **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Type	Description
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Constraints** N/A **Range** • cloud • premium **Default Value** N/A
mode	String	**Definition** This parameter is required only by the dedicated mode. **Constraints** N/A **Range** N/A **Default Value** N/A

Status code: 400

Table 4-501 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-502 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-503 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-504 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-505 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-506 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to delete a certificate in a project. The project ID is specified by project_id, and the certificate ID is specified by certificate_id.

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

Example Responses

Status code: 200

OK

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

Status Codes

Status Code	Description
200	OK
400	Request failed.

Status Code	Description
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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-507 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	**Definition** ID of the HTTPS certificate. You can call the **ListCertificates** API to obtain the certificate ID. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-508 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-509 Request header parameters

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

Table 4-510 Request body parameters

Parameter	Mandatory	Type	Description
cloud_host_ids	No	Array of strings	**Definition** ID of the HTTPS domain name in cloud mode. It can be obtained by calling the ListHost API. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Parameter	Mandatory	Type	Description
premium_host_ids	No	Array of strings	**Definition** ID of the HTTPS domain name in dedicated mode. It can be obtained by calling the ListPremiumHost API. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Response Parameters

Status code: 200

Table 4-511 Response body parameters

Parameter	Type	Description
id	String	**Definition** Certificate ID. **Range** N/A
name	String	**Definition** Certificate name. **Range** N/A
timestamp	Long	**Definition** Certificate upload timestamp. **Range** 13-bit millisecond timestamp.
expire_time	Long	**Definition** Timestamp when the certificate expires **Range** N/A

Parameter	Type	Description
bind_host	Array of **CertificateBundingHostBody** objects	Domain name list

Table 4-512 CertificateBundingHostBody

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

Status code: 400

Table 4-513 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-514 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-515 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-516 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-517 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-518 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to use a certificate for two domain names in a project. The project ID is specified by project_id, and certificate ID is specified by certificate_id The ID of the domain name protected in cloud mode is 85e554189d494c0f97789e93531c9f90, and the ID of the domain name protected in dedicated mode is 4e9e97c425fc463c8f374b90124e8392.

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

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

Example Responses

Status code: 200

OK

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


Status Codes

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

Error Codes

See **Error Codes**.

4.5 Event Management

4.5.1 Querying Details About an Event of a Specified ID

Function

Querying Details About an Event of a Specified ID

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-519 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A
eventid	Yes	String	**Definition** Event ID. You can call the **ListEvent** API to obtain the event ID. **Constraints** N/A **Range** N/A **Default Value** N/A

Table 4-520 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-521 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. It can be obtained by calling the IAM API (value of **X-Subject-Token** in the response header). **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** Content type. **Constraints** N/A **Range** N/A **Default Value** application/json;charset=utf8
X-Language	No	String	**Definition** Language. The default value is **zh-cn**. **zh-cn**: Chinese; **en-us**: English **Constraints** N/A **Range** • **zh-cn**: Chinese • **en-us**: English • **zh-cn** **Default Value**

Response Parameters

Status code: 200

Table 4-522 Response body parameters

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

Table 4-523 ShowEventItems

Parameter	Type	Description
time	Long	**Definition** Timestamp when the attack occurs, in milliseconds. **Range** N/A
policyid	String	**Definition** Policy ID **Range** N/A
sip	String	**Definition** Source IP address, which is the IP address of the web visitor, or potential attacker. **Range** N/A
host	String	**Definition** Domain name. **Range** N/A
url	String	**Definition** Attacked URL **Range** N/A

Parameter	Type	Description
attack	String	**Definition** Attack type. **Range** • **vuln**: other attack types • **sqli**: SQL injections • **lfi**: local file inclusion attacks • **cmdi**: command injections • **xss**: XSS attacks • **robot**: malicious crawlers • **rfi**: remote file inclusion attacks • **custom_custom**: precise protection • **webshell**: website Trojans • **custom_whiteblackip**: attacks blocked based on blacklist and whitelist settings • **custom_geoip**: attacks blocked based on geolocations • **antitamper**: anti-tamper events • **anticrawler**: anti-crawler events • **leakage**: website data leakage prevention • illegal: The request is invalid. • **antiscan_high_freq_scan**: blocking of high-frequency scanning • **antiscan_dir_traversal**: directory traversal protection
rule	String	**Definition** ID of the matched rule **Range** N/A
action	String	**Definition** Protective action. **Range** N/A
cookie	String	**Definition** Request cookie **Range** N/A

Parameter	Type	Description
headers	Object	**Definition** HTTP request header **Range** N/A
host_id	String	**Definition** Domain name ID. **Range** N/A
id	String	**Definition** Event ID **Range** N/A
payload	String	**Definition** Malicious Load **Range** N/A
payload_location	String	**Definition** Malicious load location **Range** N/A
region	String	**Definition** Geographical location of the source IP address **Range** N/A
process_time	Integer	**Definition** Handing duration **Range** N/A
request_line	String	**Definition** Body of the attack request **Range** N/A

Parameter	Type	Description
response_size	Integer	**Definition** Response body size (byte) **Range** N/A
response_time	Long	**Definition** Response Duration **Range** N/A
status	String	**Definition** Response code status **Range** N/A
request_body	String	**Definition** Request body **Range** N/A

Status code: 400

Table 4-524 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-525 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-526 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-527 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-528 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-529 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to query details about an event in a project. The event ID is specified by event_id, and the project ID is specified by project_id.

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

Example Responses

Status code: 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "09-0000-0000-0000-12120220421093806-a60a6166",
    "time" : 1650505086000,
    "policyid" : "173ed802272a4b0798049d7edffeff03",
    "host" : "x.x.x.x:xxxxxx-xxx-xxx-xxx-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**.

4.5.2 Querying the List of Attack Events

Function

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

Calling Method

For details, see **Calling APIs**.

URI

GET /v1/{project_id}/waf/event

Table 4-530 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-531 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Parameter	Mandatory	Type	Description
recent	No	String	**Definition** Time range of logs to be queried. **Constraints** You need to specify either parameter **recent** or parameters **from** and **to**. If bot parameter **recent** and parameter **from** or **to** are specified, **recent** takes effect. **Range** • yesterday • today • 3days • 1week • 1month **Default Value** N/A
from	No	Long	**Definition** Start time. **Constraints** Parameter **from** must be used together with parameter **to**. You need to specify either parameter **recent** or parameters **from** and **to**. If bot parameter **recent** and parameter **from** or **to** are specified, **recent** takes effect. **Range** 13-bit millisecond timestamp. **Default Value** N/A

Parameter	Mandatory	Type	Description
to	No	Long	**Definition** End time. **Constraints** Parameter **to** must be used together with parameter **from**. You need to specify either parameter **recent** or parameters **from** and **to**. If bot parameter **recent** and parameter **from** or **to** are specified, **recent** takes effect. **Range** 13-bit millisecond timestamp. **Default Value** N/A

Parameter	Mandatory	Type	Description
attacks	No	Array of strings	**Definition** Attack type. **Constraints** N/A **Range** • **vuln**: other attack types • **sqli**: SQL injections • **lfi**: local file inclusion attacks • **cmdi**: command injections • **xss**: XSS attacks • **robot**: malicious crawlers • **rfi**: remote file inclusion attacks • **custom_custom**: precise protection • **cc**: CC attacks • **webshell**: website Trojans • **custom_whiteblackip**: attacks blocked based on blacklist and whitelist settings • **custom_geoip**: attacks blocked based on geolocations • **antitamper**: anti-tamper events • **anticrawler**: anti-crawler events • **leakage**: website data leakage prevention • **illegal**: unauthorized requests • **antiscan_high_freq_scan**: blocking of high-frequency scanning • **antiscan_dir_traversal**: directory traversal protection **Default Value** N/A

Parameter	Mandatory	Type	Description
hosts	No	Array of strings	**Definition** Domain name ID. You can call the **ListHost** API to obtain it. **Constraints** N/A **Range** N/A **Default Value** N/A
sips	No	Array of strings	**Definition** Source IP address, which is the IP address of the web visitor, or potential attacker. **Constraints** N/A **Range** N/A **Default Value** N/A
page	No	Integer	**Definition** Page number of the data to be returned in a query. The default value is 1, indicating that data on the first page is returned. **Constraints** N/A **Range** N/A **Default Value** 1

Parameter	Mandatory	Type	Description
pagesize	No	Integer	**Definition** Number of results on each page in a pagination query. The default value is **10**, indicating that each page contains 10 results. **Constraints** N/A **Range** N/A **Default Value** 10

Request Parameters

Table 4-532 Request header parameters

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

Parameter	Mandatory	Type	Description
X-Language	No	String	**Definition** Language. The default value is **zh-cn**. **zh-cn**: Chinese; **en-us**: English **Constraints** N/A **Range** • **zh-cn**: Chinese • **en-us**: English • **zh-cn** **Default Value**

Response Parameters

Status code: 200

Table 4-533 Response body parameters

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

Table 4-534 ListEventItems

Parameter	Type	Description
id	String	**Definition** Incident ID **Range** N/A
time	Long	**Definition** Timestamp when the attack occurs, in milliseconds. **Range** N/A

Parameter	Type	Description
policyid	String	**Definition** Policy ID. **Range** N/A
sip	String	**Definition** Source IP address, which is the IP address of the web visitor, or potential attacker. **Range** N/A
host	String	**Definition** Domain name. **Range** N/A
url	String	**Definition** Attacked URL. **Range** N/A

Parameter	Type	Description
attack	String	**Definition** Attack type. **Range** • **vuln**: other attack types • sqli: SQL injections • lfi: local file inclusion attacks • **cmdi**: command injections • **xss**: XSS attacks • **robot**: malicious crawlers • **rfi**: remote file inclusion attacks • **custom_custom**: precise protection • **webshell**: website Trojans • **custom_whiteblackip**: attacks blocked based on blacklist and whitelist settings • **custom_geoip**: attacks blocked based on geolocations • **antitamper**: anti-tamper events • **anticrawler**: anti-crawler events • **leakage**: website data leakage prevention • illegal: The request is invalid. • **antiscan_high_freq_scan**: blocking of high-frequency scanning • **antiscan_dir_traversal**: directory traversal protection
rule	String	**Definition** ID of the matched rule **Range** N/A
payload	String	**Definition** Hit payload **Range** N/A
payload_location	String	**Definition** Hit payload position **Range** N/A

Parameter	Type	Description
action	String	**Definition** Protective action. **Range** N/A
request_line	String	**Definition** Request method and path **Range** N/A
headers	Object	**Definition** HTTP request header **Range** N/A
cookie	String	**Definition** Request cookie **Range** N/A
status	String	**Definition** Response code status **Range** N/A
process_time	Integer	**Definition** Handing duration **Range** N/A
region	String	**Definition** Geographical location. **Range** N/A
host_id	String	**Definition** Domain name ID. **Range** N/A
response_time	Long	**Definition** Response Duration **Range** N/A

Parameter	Type	Description
response_size	Integer	**Definition** Response Body Size **Range** N/A
response_body	String	**Definition** Response body **Range** N/A
request_body	String	**Definition** Request body **Range** N/A

Status code: 400

Table 4-535 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-536 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-537 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-538 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-539 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.

Parameter	Type	Description
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-540 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to query the event list for the current day in a project. The project ID is specified by project_id.

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

Example Responses

Status code: 200

ok

```
{
  "total" : 1,
  "items" : [ {
    "id" : "04-0000-0000-0000-21120220421152601-2f7a5ceb",
    "time" : 1650525961000,
    "policyid" : "25f1d179896e4e3d87ceac0598f48d00",
    "host" : "x.x.x.x:xxxxx-xxxx-xxxx-xxxx-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**.

4.6 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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-541 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-542 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Parameter	Mandatory	Type	Description
page	No	Integer	**Definition** Page number of the data to be returned in a query. The default value is 1, indicating that data on the first page is returned. **Constraints** N/A **Range** N/A **Default Value** 1
pagesize	No	Integer	**Definition** Number of results on each page in a pagination query. **Constraints** N/A **Range** The value range is 1 to 100. The default value is **10**, indicating that each page contains 10 results. To query all domain names at a time, set this parameter to **-1**. **Default Value** 10
hostname	No	String	**Definition** Protected domain dame. **Constraints** N/A **Range** Enter a maximum of 63 characters. Only letters, digits, hyphens (-), and periods (.) are allowed, for example, www.domain com. **Default Value** N/A

Parameter	Mandatory	Type	Description
policyname	No	String	**Definition** Protection policy name, which is used to query the domain names using a specified protection policy. This parameter is optional. **Constraints** N/A **Range** Enter a maximum of 64 characters.Only letters, digits, underscores (_), hyphens (-), colons (:), and periods (.) are allowed. **Default Value** N/A
protect_status	No	Integer	**Definition** Domain protection status. **Constraints** N/A **Range** • **-1**: Bypassed. Requests are directly sent to the backend servers without passing through WAF. • **0**: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. • **1**: The WAF protection is enabled. WAF detects attacks based on the configured policy. **Default Value** N/A

Parameter	Mandatory	Type	Description
waf_type	No	String	**Definition** WAF mode of the domain name. **Constraints** N/A **Range** N/A **Default Value** N/A
is_https	No	Boolean	**Definition** Whether HTTPS is used for the domain name. **Constraints** N/A **Range** N/A **Default Value** N/A

Request Parameters

Table 4-543 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. It can be obtained by calling the IAM API (value of **X-Subject-Token** in the response header). **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** Content type. **Constraints** N/A **Range** N/A **Default Value** application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-544 Response body parameters

Parameter	Type	Description
total	Integer	**Definition** Number of protected domain names. **Range** N/A
cloud_total	Integer	**Definition** Number of domain names protected in cloud mode. **Range** N/A
premium_total	Integer	**Definition** Number of domain names protected in dedicated mode **Range** N/A
items	Array of **CompositeHostResponse** objects	Details about the protected domain name.

Table 4-545 CompositeHostResponse

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Range** N/A
hostid	String	**Definition** Domain name ID. **Range** N/A
hostname	String	**Definition** Domain name added to cloud WAF. **Range** N/A
policyid	String	**Definition** Policy ID **Range** N/A
access_code	String	**Definition** CNAME prefix **Range** N/A
protect_status	Integer	**Definition** Domain protection status. **Range** • **-1**: Bypassed. Requests are directly sent to the backend servers without passing through WAF. • **0**: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. • **1**: The WAF protection is enabled. WAF detects attacks based on the configured policy.

Parameter	Type	Description
access_status	Integer	**Definition** Domain name access status. **Range** • 0: not connected • **1**: Accessible.
proxy	Boolean	**Definition** Whether the protected domain name uses a proxy. • **false**: No proxy is used. • **true**: At least one proxy is used. **Range** • false • true
timestamp	Long	**Definition** Time a domain name is added to WAF. **Range** 13-bit millisecond timestamp.
paid_type	String	**Definition** Package payment mode. The default value is **prePaid**. **Range** • **prePaid**: yearly/monthly • **postPaid**: pay-per-use
flag	**Flag** object	Special identifier, which is used on the console.
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Range** • cloud • premium
web_tag	String	**Definition** Website name, which is the website name displayed on the domain name details page on the WAF console. **Range** Enter 0 to 128 characters.

Parameter	Type	Description
access_progress	Array of **Access_progress** objects	Access progress, which is used only for the new WAF console.
premium_waf_instances	Array of **Premium_waf_instances** objects	List of dedicated WAF instances
description	String	**Definition** Domain name description. **Range** N/A
exclusive_ip	Boolean	**Definition** Whether to use the dedicated public IP address. This parameter is reserved for future function expansion and can be ignored. **Range** • **true**: A dedicated IP address is used. • **false**: No dedicated IP address is used.
region	String	**Definition** Region ID. This parameter is carried when a domain name is added to WAF on the management console. This parameter is left blank when a domain name is added to WAF using an API. **Range** N/A
server	Array of **WafServer** objects	Origin server settings of the protected domain name. The value of **vpc_id** is returned only for domain names protected with dedicated instances.
enterprise_project_id	String	**Definition** Enterprise project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **Enterprise** > **Project Management**, click the project name, and locate the project ID. **Range** N/A

Table 4-546 Flag

Parameter	Type	Description
pci_3ds	String	**Definition** Whether to enable PCI 3DS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A
pci_dss	String	**Definition** Whether to enable PCI_DSS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A
cname	String	**Definition** old: The old CNAME record is used. new: new CNAME record is used. **Constraints** N/A **Range** • old: old CNAME used by the domain name • new: The domain name uses a new CNAME. **Default Value** N/A

Parameter	Type	Description
is_dual_az	String	**Definition** Whether the dual-AZ mode is supported **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A
ipv6	String	**Definition** Whether IPv6 is enabled for the domain name. **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Table 4-547 Access_progress

Parameter	Type	Description
step	Integer	**Definition** Steps **Range** • **1**: Whitelist the WAF IP addresses. • **2**: Test connectivity. • **3**: Modify DNS resolution.
status	Integer	**Definition** Status **Range** • 0: This step is not complete. • 1: completed

Table 4-548 Premium_waf_instances

Parameter	Type	Description
id	String	**Definition** Engine instance ID. **Range** N/A
name	String	**Definition** Engine instance name. **Range** N/A
accessed	Boolean	**Definition** Whether the engine instance has been connected **Range** • false: not connected • true: connected

Table 4-549 WafServer

Parameter	Type	Description
front_protocol	String	**Definition** Protocol used by the client to access the origin server of the protected domain name. **Range** • HTTP • HTTPS
back_protocol	String	**Definition** Protocol used by WAF to forward client requests to the origin server of the protected domain name. **Range** • HTTP • HTTPS

Parameter	Type	Description
weight	Integer	**Definition** Weight of the origin server. The load balancing algorithm allocates requests to the origin server based on the weight. The default value is **1**. This parameter is not required for WAF cloud mode. **Range** N/A
address	String	**Definition** IP address of origin server accessed by the client. **Range** N/A
port	Integer	**Definition** Port used by WAF to forward client requests to the origin server. **Range** N/A
type	String	**Definition** Type of the origin server address: IPv4 or IPv6 **Range** • ipv4 • ipv6

Parameter	Type	Description
vpc_id	String	**Definition** VPC ID. You can query the VPC ID in either of the following way: • **1**. Query the name of the VPC where the dedicated engine (instance) is provisioned. To do so, log in to the WAF console and choose **Instance Management** > **Dedicated Engine** . Locate the target instance, and check the **VPC** and **Subnet** column. The VPC name is displayed in the VPC and subnet columns. • **2**. Go to the VPC console and choose **Virtual Private Cloud** > **My VPCs**. You can copy the ID next to the VPC name or click the VPC name and copy the ID in the **VPC Information** area. **Range** N/A

Status code: 400

Table 4-550 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-551 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-552 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-553 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-554 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-555 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following example shows how to query the protected domain name list in a project. The project ID is specified by project_id.

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

Example Responses

Status code: 200

OK


```
{
  "items" : [ {
    "id" : "31af669f567246c289771694f2112289",
    "hostid" : "31af669f567246c289771694f2112289",
    "description" : "",
    "proxy" : false,
    "flag" : {
      "pci_3ds" : "false",
      "pci_dss" : "false",
      "ipv6" : "false",
      "cname" : "new",
      "is_dual_az" : "true"
    },
    "region" : "cn-north-4",
    "hostname" : "www.demo.com",
    "access_code" : "1b18879b9d064f8bbcbf8abce7294cac",
    "policyid" : "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.

Calling Method

For details, see **Calling APIs**.

URI

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

Table 4-556 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	**Definition** Project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A
host_id	Yes	String	**Definition** Domain name ID. In the cloud mode, you can call the **ListHost API** to obtain it. In the dedicated mode, you can call the **ListPremiumHost** API to obtain it. **Constraints** N/A **Range** Enter 32 characters. Only letters and digits are allowed. **Default Value** N/A

Table 4-557 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	**Definition** Obtain the enterprise project ID by calling the **ListEnterpriseProject** API of Enterprise Project Management Service (EPS). To obtain the resource details in all enterprise projects of a user, set this parameter to **all_granted_eps**. **Constraints** N/A **Range** • **0**: the default enterprise project. • **all_granted_eps**: all enterprise projects. • **A specific enterprise project ID**: Enter a maximum of 36 characters. **Default Value** 0

Request Parameters

Table 4-558 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	**Definition** User token. It can be obtained by calling the IAM API (value of **X-Subject-Token** in the response header). **Constraints** N/A **Range** N/A **Default Value** N/A

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	**Definition** Content type. **Constraints** N/A **Range** N/A **Default Value** application/json;charset=utf8

Response Parameters

Status code: 200

Table 4-559 Response body parameters

Parameter	Type	Description
id	String	**Definition** Domain name ID. **Range** N/A
hostid	String	**Definition** Domain name ID. **Range** N/A
hostname	String	**Definition** Domain name added to cloud WAF. **Range** N/A
policyid	String	**Definition** Policy ID **Range** N/A
access_code	String	**Definition** CNAME prefix **Range** N/A

Parameter	Type	Description
protect_status	Integer	**Definition** Domain protection status. **Range** • **-1**: Bypassed. Requests are directly sent to the backend servers without passing through WAF. • **0**: The WAF protection is suspended. WAF only forwards requests for the domain name but does not detect attacks. • **1**: The WAF protection is enabled. WAF detects attacks based on the configured policy.
access_status	Integer	**Definition** Domain name access status. **Range** • 0: not connected • **1**: Accessible.
proxy	Boolean	**Definition** Whether the protected domain name uses a proxy. • **false**: No proxy is used. • **true**: At least one proxy is used. **Range** • false • true
timestamp	Long	**Definition** Time a domain name is added to WAF. **Range** 13-bit millisecond timestamp.
paid_type	String	**Definition** Package payment mode. The default value is **prePaid**. **Range** • **prePaid**: yearly/monthly • **postPaid**: pay-per-use
flag	**Flag** object	Special identifier, which is used on the console.

Parameter	Type	Description
waf_type	String	**Definition** Domain name mode. The value can be cloud for cloud mode or premium for dedicated mode. **Range** • cloud • premium
web_tag	String	**Definition** Website name, which is the website name displayed on the domain name details page on the WAF console. **Range** Enter 0 to 128 characters.
access_progress	Array of **Access_progress** objects	Access progress, which is used only for the new WAF console.
premium_waf_instances	Array of **Premium_waf_instances** objects	List of dedicated WAF instances
description	String	**Definition** Domain name description. **Range** N/A
exclusive_ip	Boolean	**Definition** Whether to use the dedicated public IP address. This parameter is reserved for future function expansion and can be ignored. **Range** • **true**: A dedicated IP address is used. • **false**: No dedicated IP address is used.
region	String	**Definition** Region ID. This parameter is carried when a domain name is added to WAF on the management console. This parameter is left blank when a domain name is added to WAF using an API. **Range** N/A

Parameter	Type	Description
server	Array of **WafServer** objects	Origin server settings of the protected domain name. The value of **vpc_id** is returned only for domain names protected with dedicated instances.
enterprise_project_id	String	**Definition** Enterprise project ID. To obtain it, log in to the Huawei Cloud console, click the username, choose **Enterprise** > **Project Management**, click the project name, and locate the project ID. **Range** N/A

Table 4-560 Flag

Parameter	Type	Description
pci_3ds	String	**Definition** Whether to enable PCI 3DS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A
pci_dss	String	**Definition** Whether to enable PCI_DSS compliance authentication. **Constraints** N/A **Range** • **true**: enabled • **false**: disabled **Default Value** N/A

Parameter	Type	Description
cname	String	**Definition** old: The old CNAME record is used. new: new CNAME record is used. **Constraints** N/A **Range** • old: old CNAME used by the domain name • new: The domain name uses a new CNAME. **Default Value** N/A
is_dual_az	String	**Definition** Whether the dual-AZ mode is supported **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A
ipv6	String	**Definition** Whether IPv6 is enabled for the domain name. **Constraints** N/A **Range** • **true**: supported • **false**: not supported **Default Value** N/A

Table 4-561 Access_progress

Parameter	Type	Description
step	Integer	**Definition** Steps **Range** • **1**: Whitelist the WAF IP addresses. • **2**: Test connectivity. • **3**: Modify DNS resolution.
status	Integer	**Definition** Status **Range** • 0: This step is not complete. • 1: completed

Table 4-562 Premium_waf_instances

Parameter	Type	Description
id	String	**Definition** Engine instance ID. **Range** N/A
name	String	**Definition** Engine instance name. **Range** N/A
accessed	Boolean	**Definition** Whether the engine instance has been connected **Range** • false: not connected • true: connected

Table 4-563 WafServer

Parameter	Type	Description
front_protocol	String	**Definition** Protocol used by the client to access the origin server of the protected domain name. **Range** • HTTP • HTTPS
back_protocol	String	**Definition** Protocol used by WAF to forward client requests to the origin server of the protected domain name. **Range** • HTTP • HTTPS
weight	Integer	**Definition** Weight of the origin server. The load balancing algorithm allocates requests to the origin server based on the weight. The default value is **1**. This parameter is not required for WAF cloud mode. **Range** N/A
address	String	**Definition** IP address of origin server accessed by the client. **Range** N/A
port	Integer	**Definition** Port used by WAF to forward client requests to the origin server. **Range** N/A
type	String	**Definition** Type of the origin server address: IPv4 or IPv6 **Range** • ipv4 • ipv6

Parameter	Type	Description
vpc_id	String	**Definition** VPC ID. You can query the VPC ID in either of the following way: • **1**. Query the name of the VPC where the dedicated engine (instance) is provisioned. To do so, log in to the WAF console and choose **Instance Management** > **Dedicated Engine** . Locate the target instance, and check the **VPC** and **Subnet** column. The VPC name is displayed in the VPC and subnet columns. • **2**. Go to the VPC console and choose **Virtual Private Cloud** > **My VPCs**. You can copy the ID next to the VPC name or click the VPC name and copy the ID in the **VPC Information** area. **Range** N/A

Status code: 400

Table 4-564 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-565 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 401

Table 4-566 Response body parameters

Parameter	Type	Description
error_code	String	Error code.
error_msg	String	Error message.
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of **IAM5ErrorDetails** objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-567 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Status code: 500

Table 4-568 Response body parameters

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

Parameter	Type	Description
encoded_authorization_message	String	You can call the decode-authorization-message interface of the STS service to decode the rejection reason. For details, see the STS5 joint commissioning and self-verification. This parameter is returned only when an IAM 5 authentication error occurs.
details	Array of IAM5ErrorDetails objects	The set of error messages reported when a downstream service is invoked. This parameter is returned only when an IAM 5 authentication error occurs.

Table 4-569 IAM5ErrorDetails

Parameter	Type	Description
error_code	String	Error codes of the downstream service.
error_msg	String	Error messages of the downstream service.

Example Requests

The following shows how to obtain details about a domain name. The project ID is specified by **project_id**, and the domain ID is specified by **host_id**.

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

Example Responses

Status code: 200

OK

```
{
  "id" : "31af669f567246c289771694f2112289",
  "hostid" : "31af669f567246c289771694f2112289",
  "description" : "",
  "proxy" : false,
  "flag" : {
    "pci_3ds" : "false",
    "pci_dss" : "false",
    "ipv6" : "false",
    "cname" : "new",
    "is_dual_az" : "true"
  },
  "region" : "cn-north-4",
  "hostname" : "www.demo.com",
  "access_code" : "1b18879b9d064f8bbcbf8abce7294cac",
  "policyid" : "41cba8aee2e94bcdbf57460874205494",
  "timestamp" : 1650527546454,
  "protect_status" : 0,
  "access_status" : 0,
```



```
  "exclusive_ip" : false,
  "web_tag" : "",
  "paid_type" : "prePaid",
  "waf_type" : "cloud",
  "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"
  } ]
}
```

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.00011015	spec.code.illegal	Illegal spec code of WAF	Replacing Valid WAF Specifications
400	WAF.00011016	name.duplicate	Duplicated name.	Change the name.

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00011017	ipv6.switch.illegal	IPv6 defense cannot be disabled.	Enable IPv6 defense.
400	WAF.00011018	action.type.illegal	Illegal action type	Replace a valid defense action type.
400	WAF.00011019	cert.illegal	Illegal certificate	Use a valid certificate.
400	WAF.00011020	cve.num.illegal	Invalid CVE ID	Use a valid CVE ID.
400	WAF.00011021	cert.expired	Certificate has expired	Replacing an Unexpired Certificate
400	WAF.00011022	gocm.action.illegal	Illegal GOCM ACTION	Check the action in the GOCM ticket and use a correct and valid action rule.
400	WAF.00011023	repeat.purchases	It is not allowed to purchase twice	It is not allowed to purchase twice
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.00013004	protocol.not.support	Protocol not supported	Through ELB conversion protocol
400	WAF.00013010	custom.ruleset.does.not.support.for.shared.policy	Custom rule set does not support for shared policy	nothing
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

Status Code	Error Codes	Error Message	Description	Solution
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.00014010	port.protocol.mismatch	Port and protocol mismatch	Select the matching protocol and port
400	WAF.00014011	host.blacklist	It is forbidden to add the protection website, and the domain name is blacklisted	-
400	WAF.00014012	website.not.register	Website is not registered	Filing website
400	WAF.00014013	host.already.access	The domain name already has accessed waf	nothing
400	WAF.00014014	exclusive.ip.config.error	exclusive.ip.config.error	Check exclusive IP configuration
400	WAF.00014015	resource.is.being.used	Resource is in use	nothing
400	WAF.00014016	ip.group.is.being.shared	IP group is being shared	nothing

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00014017	policy.is.being.shared	Policy is being shared	nothing
400	WAF.00014018	certificate.is.being.shared	Certificate is being shared	nothing
400	WAF.00014019	policy.is.being.disconnecting	Policy is being disconnecting	nothing
400	WAF.00014026	sdk.already.exists	Sdk config already exists	Check the SDK configuration.
400	WAF.00014027	certificate.already.exists	Certificate already exists	Check the certificate file.
400	WAF.00014028	host.already.exists	Website already exists	Check the protected domain name.
400	WAF.00014029	certificateSharing.already.exists	Current certificate already exists in target enterprise project	Check the certificate file of the target enterprise project.
400	WAF.00014030	policySharing.already.exists	Current policy already exists in target enterprise project	Check the protection policy of the target enterprise project.
400	WAF.00014031	ipGroupSharing.already.exists	Current ip address group already exists in target enterprise project	Check the IP address group of the target enterprise project.
400	WAF.00015001	premium.instance.not.available	Dedicated WAF instance is not available. Please check configurations	check configurations
400	WAF.00015005	premium.instance.illegal.flavor	Illegal ECS flavor of dedicated WAF instance	Change the ECS specifications.

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00015006	premium.instance.purchase.config.not.found	Purchase options of Premium WAF is not configured	Check the option configuration on the Premium WAF purchase page.
400	WAF.00016001	elb.mode.not.available	ELB mode is not available	Check the ELB mode configuration.
400	WAF.00021001	bad.request	Bad request	nothing
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	pageOrPageSize.illegal	Illegal page or pagesize	It is recommended to view the parameter limits according to the documentation in the help center
400	WAF.00021022	name.duplicate	name duplicate	Modify the name
400	WAF.00021023	server.mode.illegal	Illegal mode	Check the service mode.
400	WAF.00021024	proxyConfig.illegal	Illegal SDK proxy config	Check the SDK configuration.
400	WAF.00021025	cookie.secure.conflict	Cookie with Secure/ HttpOnly conflicts with HTTP client protocol	Check the configuration.
400	WAF.00021026	condition.repeat	Duplicate rules in the condition list	Checking Rules in the Condition List
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

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00022004	rule.conflict	Rule conflict	Check whether the target rule conflicts with the existing rule
400	WAF.00022006	host.conflict	Someone else has already added this domain name, Please confirm whether the domain name belongs to you. If so, contact the service staff to help you solve it	Someone else has already added this domain name, Please confirm whether the domain name belongs to you. If so, contact the service staff to help you solve it
400	WAF.00022007	open.protect.failed	Failed to enable protection, please access the traffic first	please access the traffic first
400	WAF.00022012	rule.resource.already.exists	Same condition rule already exists	Check the added rule condition.
400	WAF.00023001	policy.not.bind.domain	The policy is not bound a domain	Bind the domain name first
400	WAF.00023002	domain.not.session.tag	Please set session tag on the domain setting page	Please configure the session tag on the domain first
400	WAF.00023003	domain.not.user.tag	Please set user tag on the domain setting page	Please configure the user tag on the domain first
401	WAF.00010005	request.iam.failed	Failed to request IAM. Please check current user's IAM permissions	Please check current user's IAM permissions

Status Code	Error Codes	Error Message	Description	Solution
401	WAF.00010006	update.iam.failed	Failed to request IAM. Please check current user's IAM permissions	Please check current user's IAM permissions
401	WAF.00012003	permission.denied	No permission	Assign WAF required permissions to account
401	WAF.00012008	jwt.authentication.invalid.token	Illegal JWT token	Check whether the account has JWT permission
401	WAF.00012009	jwt.authentication.failed	JWT authentication failed	Give the account authorization first
401	WAF.00012011	cop.permission.denied	No cop permission.	Check the COP permission.
401	WAF.00015004	premium.instance.agency.not.ready	The IAM agency needed for dedicated WAF instance is not ready	Check the IAM Agency Permissions
401	WAF.00016003	elb.mode.elb.unauthorized	No permission to get ELB info and update ELB options	Check the user permission.
403	WAF.00012004	account.frozen	Account freezing	Account unfreezing
403	WAF.00012005	not.subscribe	Unsubscribed	Subscribe to WAF service first
403	WAF.00012006	pdp.permission.denied	No permission	Check the PDP authority of the account
403	WAF.00012007	jwt.authentication.disabled	JWT certification off	Open JWT certification
403	WAF.00012010	eps.all.not.support	eps.all.not.support	Open the write permission of enterprise project

Status Code	Error Codes	Error Message	Description	Solution
403	WAF.00012012	not.subscribe.cloud	The target enterprise project has not subscribed to the cloud-mode WAF instance	Subscribe to a cloud-mode WAF instance.
403	WAF.00012013	not.subscribe.premium	The target enterprise project has not subscribed to the dedicated WAF instance	Subscribe to the dedicated WAF instance
403	WAF.00013001	insufficient.quota	Insufficient function quota	Purchase function quota upgrade package
403	WAF.00013002	feature.not.support	Function not supported	nothing
403	WAF.00013003	port.not.support	Port not supported	Port conversion via ELB
403	WAF.00013005	wildcard.domain.not.support	Pan domain name not supported	Use specific domain names
403	WAF.00013006	ipv6.not.support	IPv6 is not supported	The current version does not support IPv6
403	WAF.00013007	insufficient.tenant.quota	insufficient.tenant.quota	Purchase quota upgrade package
403	WAF.00013008	product.sold.out	The selected product has been sold out	Change Product Specification
403	WAF.00013009	degrade.not.support	Forbidden to degrade, current host num exceeds degraded quota	Reduce domain name usage

Status Code	Error Codes	Error Message	Description	Solution
403	WAF.00013011	insufficient.domain.quota	Insufficient root domain quota, please purchase expansion package or upgrade specification	purchase expansion package or upgrade specification
403	WAF.00013012	insufficient.port.quota	Insufficient port quota, please purchase expansion package or upgrade specification	please purchase expansion package or upgrade specification
403	WAF.00013013	insufficient.host.quota	Insufficient domain quota, please purchase expansion package or upgrade specification	please purchase expansion package or upgrade specification
403	WAF.00013014	insufficient.policy.quota	Insufficient policy quota	Purchase the domain name expansion package or upgrade the specification
403	WAF.00015002	premium.instance.sold.out	Dedicated WAF instance is currently sold out. Please change ECS flavor or wait for restock	Please change ECS flavor or wait for restock
403	WAF.00015003	premium.instance.not.allowed	The account is not allowed to create dedicated WAF instance	Check the current account configuration.

Status Code	Error Codes	Error Message	Description	Solution
403	WAF.00016004	elb.mode.unsupported.elb	ELB is not eligible for WAF. Only ELBv3 supports WAF	Check the ELB Mode
403	WAF.00016005	elb.mode.unsupported.elb.spec	ELB is not eligible for WAF due to its spec. Please ensure ELB has L7 flavor	Check the ELB configuration.
403	WAF.00016006	elb.mode.unsupported.elb.flavor	ELB is not eligible for WAF due to its flavor. Please ensure ELB has supported L7 flavor	Check the ELB configuration
403	WAF.00022005	insufficient.quota	Insufficient resources	It is recommended to purchase the upgrade package of corresponding resources
404	WAF.00014001	resource.not.found	Resource not found	The resource has been deleted or does not exist
404	WAF.00014009	api.not.found	The interface does not exist	Check interface URL
404	WAF.00014020	certificate.not.found	Certificate not found	Add the certificate resource.
404	WAF.00014021	ipGroup.not.found	Ip address group not found	Add an IP address group.
404	WAF.00014022	host.not.found	Domain name not found	Add a domain name.
404	WAF.00014023	premium.waf.instance.not.found	Dedicated engine not found	Add Dedicated engine WAF instance.

Status Code	Error Codes	Error Message	Description	Solution
404	WAF.00014024	projectId.not.found	Project id not found	Check the project ID.
404	WAF.00014025	policy.not.found	Policy not found	Adding a defense policy
404	WAF.00016002	elb.mode.elb.not.found	Provided ELB not found	Check the ELB
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
404	WAF.00022008	rule.not.found	Policy rule not found	Check the policy rule.
404	WAF.00022009	certificate.not.found	certificate not found	Check whether the certificate resource has been added.
404	WAF.00022010	ipGroup.not.found	Address group not found	Add an IP address group first
404	WAF.00022011	policy.not.found	Policy not found	Add a protection policy first.
409	WAF.00016007	elb.mode.conflict	ELB is only allowed to bind either dedicated WAF pool or shared WAF pool	Repeated binding is not allowed.
409	WAF.00016008	elb.mode.ep.conflict	ELB is allowed to config in only one enterprise project	Repeated binding is not allowed.
500	WAF.00010001	internal.error	Server internal error	Contact technical support
500	WAF.00010002	system.busy	The system is busy, please try again later	Contact technical support

Status Code	Error Codes	Error Message	Description	Solution
500	WAF.00010003	cname.failed	Failed to create or modify CNAME	Contact technical support
500	WAF.00010004	obs.failed	Failed to get OBS file download link	Contact technical support
500	WAF.00010007	risk.action.is.blocking	Due to security reasons, your account has been restricted from purchasing certain pay-per-use cloud service resources according to the HUAWEI CLOUD Customer Agreement. If you have any questions, contact customer service	contact customer service
500	WAF.00010008	frozen.deposit.failed	Insufficient account balance. Top up your account	Top up your account
500	WAF.00010009	list.eps.failed	Failed to list enterprise project	nothing
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

Scenario

A project ID is required for some URLs when an API is called. Obtain the required project ID using either of the following methods:

- **Obtaining a Project ID by Calling an API**
- **Obtaining a Project ID from the Console**

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 steps:

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.

