Edge Security

API Reference

Issue 02

Date 2023-11-24

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

1.1 Overview

Edge Security (EdgeSec) is a security service based on the edge nodes of Huawei Cloud Content Delivery Network (CDN). It provides functions such as Edge Anti-DDoS, CC attack protection, Web protection, and bot behavior analysis. If you have purchased CDN or Whole Site Acceleration (WSA), you can enable security protection for acceleration domain names to safeguard content delivery.

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

If you plan to access EdgeSec through an API, ensure that you are familiar with EdgeSec. For more information, see **What Is EdgeSec?**

1.2 API Calling

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

1.3 Endpoints

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

1.4 Concepts

- Account

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

- User

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

- Region

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

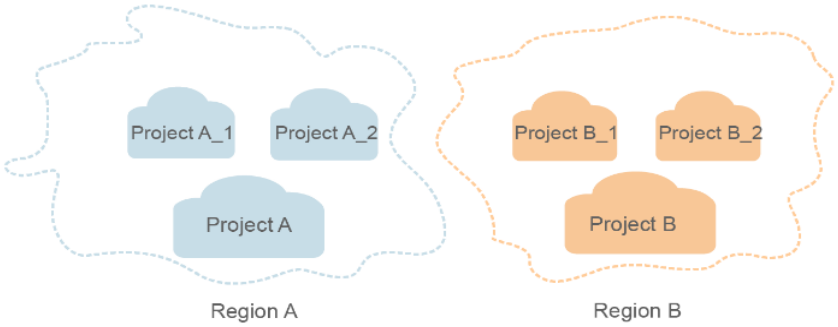
- Availability Zone (AZ)

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

- Project

  A region corresponds to a project. Default projects are defined to group and physically isolate resources (including computing, storage, and network resources) across regions. You can grant users 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 purchase resources in the subprojects. Users can then be assigned permissions to access only specific resources in the subprojects.

  Figure 1-1 Project isolation model



2 API Overview

You can use all functions of EdgeSec via APIs.

Type	Description
Anti-DDoS Data Query	Edge anti-DDoS data query APIs, including APIs for querying tenants' attack event data and tenant traffic data.
WAF Domain Name	Edge WAF domain name APIs, including APIs for querying the CDN domain name list, querying the edge WAF domain name list, and creating a protected domain name.
WAF Protection Policy	Edge WAF protection policy APIs, including APIs for creating and modifying protection policies, and querying the protection policy list.
Anti-DDoS Domain Name	Edge anti-DDoS domain name APIs, including adding, querying, and updating protected domain names.
Tenant Subscription Management	APIs used by tenants to query subscription information, including the API for querying purchased edge security products.
WAF Certificate Management	Edge WAF certificate management APIs, including creating, querying, and deleting certificates.

3 API Calling

3.1 Making an API Request

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

Request URI

A request URI is in the following format:

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

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

- **URI-scheme**:

  Protocol used to transmit requests. All APIs use HTTPS.
- **Endpoint**:

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

  For example, the endpoint of IAM in region **CN-Hong Kong** is **iam.ap-southeast-1.myhuaweicloud.com**.
- **resource-path**:

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

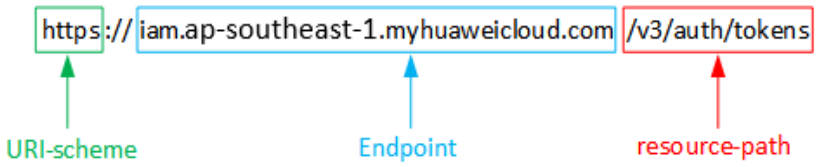
  Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

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

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

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

Figure 3-1 Example URI



NOTE

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

Request Methods

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

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

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

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

Request Header

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

Common request header fields are as follows:

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

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

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

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

Request Body

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

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

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

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

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



```
    }
}
```

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

3.2 Authentication

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

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

Token-based Authentication

NOTE

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

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

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

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

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


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

AK/SK-based Authentication

NOTE

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

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

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

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

NOTICE

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

3.3 Returned Values

Status Code

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

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

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

Response Header

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

Figure 3-2 shows the response header for the API of **obtaining a user token**, in which **x-subject-token** is the desired user token. Then, you can use the token to authenticate the calling of other APIs.

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

(Optional) Response Body

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

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

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

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

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

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

4 API

4.1 Anti-DDoS Data Query

4.1.1 Querying Attack Event Data of a Tenant

Function

This API is used to query attack event data of a tenant.

URI

GET /v1/statistics/event

Table 4-1 Query Parameters

Parameter	Mandatory	Type	Description
start_time	Yes	Long	Start time (13-digit timestamp). This parameter must be used together with end_time.
end_time	Yes	Long	End time (13-digit timestamp). This parameter must be used together with start_time.

Parameter	Mandatory	Type	Description
type	Yes	String	Type: • attack_count (number of attack events of different types) • flow_drop_count (number of accesses and attacks) • ddos_attack_count (number of DDoS attacks) Enumeration values: • **attack_count** • **flow_drop_count** • **ddos_attack_count**
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Request Parameters

Table 4-2 Request header parameters

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

Response Parameters

Status code: 200

Table 4-3 Response body parameters

Parameter	Type	Description
value	Long	Number of DDoS attacks. This parameter is returned when type is set to ddos_attack_count.
waf	Array of **TimeSeriesData** objects	Number of WAF attacks. This parameter is returned when type is set to attack_count.

Parameter	Type	Description
bot	Array of **TimeSeriesData** objects	Number of bot attacks. This parameter is returned when type is set to attack_count.
cc	Array of **TimeSeriesData** objects	Number of CC attacks. This parameter is returned when type is set to attack_count.
ddos	Array of **TimeSeriesData** objects	Number of DDoS attacks. This parameter is returned when type is set to attack_count.
flow	Array of **TimeSeriesData** objects	Number of accesses. This parameter is returned when type is set to flow_drop_count.
drop	Array of **TimeSeriesData** objects	Number of attacks. This parameter is returned when type is set to flow_drop_count.

Table 4-4 TimeSeriesData

Parameter	Type	Description
time	Long	13-digit timestamp.
value	Double	Data value. Unit: kbit/s (for traffic query) or number of events (for event query)

Status code: 400

Table 4-5 Response body parameters

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

Status code: 401

Table 4-6 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Status code: 500

Table 4-7 Response body parameters

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

Example Requests

Query DDoS attacks.

```
GET https://{Endpoint}/v1/statistics/event?
type=ddos_attack_count&end_time=1691916827257&start_time=1691312027000
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "value" : 100
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	The account corresponding to the token does not have sufficient permission.
500	Internal server error.

Error Codes

See **Error Codes**.

4.1.2 Querying Tenant Traffic Data

Function

This API is used to query tenant traffic data.

URI

GET /v1/statistics/traffic

Table 4-8 Query Parameters

Parameter	Mandatory	Type	Description
start_time	Yes	Long	Start time (13-digit timestamp). This parameter must be used together with end_time.
end_time	Yes	Long	End time (13-digit timestamp). This parameter must be used together with start_time.
type	Yes	String	Type: • max_flow_bandwidth (peak inbound DDoS traffic bandwidth) • max_drop_bandwidth (peak inbound DDoS traffic bandwidth) • ddos_flow (inbound DDoS traffic) • flow_drop_traffic (inbound traffic and cleaned traffic) • attack_traffic (different types of attack traffic) Enumeration values: • **max_flow_bandwidth** • **max_drop_bandwidth** • **ddos_flow** • **flow_drop_traffic** • **attack_traffic**
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Request Parameters

Table 4-9 Request header parameters

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

Response Parameters

Status code: 200

Table 4-10 Response body parameters

Parameter	Type	Description
value	Long	Traffic data value, which is returned when type is set to max_flow_bandwidth, max_drop_bandwidth, or ddos_flow. Unit: kbit/s
flow	Array of **TimeSeriesData** objects	Incoming traffic. This parameter is returned when type is set to flow_drop_traffic.
drop	Array of **TimeSeriesData** objects	Cleaned traffic. This parameter is returned when type is set to flow_drop_traffic.
waf	Array of **TimeSeriesData** objects	WAF attack traffic. This parameter is returned when type is set to attack_traffic.
bot	Array of **TimeSeriesData** objects	Bot attack traffic. This parameter is returned when type is set to attack_traffic.
cc	Array of **TimeSeriesData** objects	CC attack traffic. This parameter is returned when type is set to attack_traffic.
ddos	Array of **TimeSeriesData** objects	DDoS attack traffic. This parameter is returned when type is set to attack_traffic.

Table 4-11 TimeSeriesData

Parameter	Type	Description
time	Long	13-digit timestamp.
value	Double	Data value. Unit: kbit/s (for traffic query) or number of events (for event query)

Status code: 400

Table 4-12 Response body parameters

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

Status code: 401

Table 4-13 Response body parameters

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

Status code: 500

Table 4-14 Response body parameters

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

Example Requests

Query the peak bandwidth of inbound DDoS traffic.

```
GET https://{Endpoint}/v1/statistics/traffic?
type=max_flow_bandwidth&end_time=1691916827257&start_time=1691312027000
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "value" : 100
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	The account corresponding to the token does not have sufficient permission.
500	Internal server error.

Error Codes

See **Error Codes**.

4.2 WAF Domain Name Management

4.2.1 Viewing the CDN Domain Name List

Function

This API is used to view the CDN domain name list.

URI

GET /v1/edgesec/cdn/domains

Table 4-15 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset in query pagination. Minimum: **0** Default: **0**
limit	No	Integer	Maximum number of records displayed on each page. Minimum: **1** Maximum: **100** Default: **10**

Parameter	Mandatory	Type	Description
domain_name	No	String	Domain name.
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Request Parameters

Table 4-16 Request header parameters

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

Response Parameters

Status code: 200

Table 4-17 Response body parameters

Parameter	Type	Description
total	Integer	Total number of CDN domain names.
count	Integer	Number of CDN domain names in the query result.
domains	Array of **ShowCdnDomainResponseBody** objects	CDN domain name details.

Table 4-18 ShowCdnDomainResponseBody

Parameter	Type	Description
domain_name	String	Domain name.

Parameter	Type	Description
domain_status	String	Status of an acceleration domain name. Values: • **online**: CDN has been enabled for this domain name. • **offline**: CDN has been disabled for this domain name. • **configuring**: The domain name configuration is in progress. • **configure_failed*: The configuration fails. • **checking**: The domain is being reviewed. • **check_failed**: The domain name fails the review. • **deleting**: The domain name is being deleted.
domain_id	String	Domain name ID.
certificate_id	String	ID of the certificate used for the domain name.
service_area	String	Domain name service area. Enumeration values: • **mainland_china** • **outside_mainland_china** • **global** • **europe**
ipv6_accelerate	Integer	Whether to enable IPv6 acceleration. The value can be 0 (disabled) or 1 (enabled). Enumeration values: • **1**
business_type	String	Service type of the domain name. Possible values: • web: website acceleration • download: file download acceleration • video: VOD acceleration • wholeSite: whole site acceleration
https_status	Integer	Whether to enable HTTPS. The value can be 0 (disabled) and 1 (enabled). Enumeration values: • **0** • **1**

Parameter	Type	Description
force_redirect	Integer	Forced redirection. 0: disabled; 1: forced redirection to HTTP; 2: forced redirection to HTTPS
extended_tags	**CdnDomainTags** object	CDN domain name security service constraint.
is_added	Boolean	Whether a domain name is protected by WAF. Default: **false**

Table 4-19 CdnDomainTags

Parameter	Type	Description
notes	String	Reason
constraint	String	Content

Status code: 400

Table 4-20 Response body parameters

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

Status code: 401

Table 4-21 Response body parameters

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

Status code: 500

Table 4-22 Response body parameters

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

Example Requests

View the CDN domain name list.

```
GET https://{Endpoint}/v1/edgesec/cdn/domains?offset=0&limit=10
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 12,
  "count" : 10,
  "domains" : [ {
    "domain_name" : "domain_name",
    "domain_status" : "online",
    "domain_id" : "3e9df5da33744bae90bf73291c6e5c6c",
    "certificate_id" : "8da2b3da33744bae90bf73291c6e5c6c",
    "service_area" : "outside_mainland_china",
    "ipv6_accelerate" : 0,
    "business_type" : "web",
    "https_status" : 1,
    "force_redirect" : 0,
    "extended_tags" : [ {
      "notes" : "example",
      "constraint" : "example"
    } ],
    "is_added" : true
  } ]
}
```

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 Querying the List of Domain Names Protected by WAF

Function

This API is used to querying the list of domain names protected by WAF.

URI

GET /v1/edgewaf/domains

Table 4-23 Query Parameters

Parameter	Mandatory	Type	Description
page_num	No	Integer	Page number. The value 0 indicates that all pages are queried. Minimum: **0** Default: **1**
page_size	No	Integer	Number of items displayed on each page. A maximum of 100 items can be queried in a batch in WAF. Minimum: **1** Maximum: **100** Default: **10**
domain_name	No	String	Domain name.
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).
type	No	Integer	WAF domain name configuration type. 0: basic information; 1: WAF protection configuration Enumeration values: • **0** • **1**

Request Parameters

Table 4-24 Request header parameters

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

Response Parameters

Status code: 200

Table 4-25 Response body parameters

Parameter	Type	Description
total	Long	Total number of protected domain names. Minimum: **0** Default: **0**
domain_list	Array of **ShowWafDomainResponseBody** objects	Details about the protected domain name.

Table 4-26 ShowWafDomainResponseBody

Parameter	Type	Description
id	String	Domain name ID.
domain_name	String	Domain name.
enterprise_project_id	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).
tenant_id	String	Tenant ID.
open_time	Long	Last time when protection was last enabled.
close_time	Long	Last time when protection was last disabled.
dispatch_status	Integer	CDN domain name scheduling status (0: not protected; 1: configuring; 2: protected; 3: deleting)
service_area	String	Region that the domain name belongs to.

Parameter	Type	Description
web_tag	String	Domain name.
description	String	Domain name description.
policy_id	String	Policy ID.
protocol	String	Protocol. Enumeration values: • **http** • **https**
certificate_id	String	Certificate ID.
certificate_name	String	Certificate name.
tls	String	Minimum TLS version (TLS v1.0, TLS v1.1, or TLS v1.2). The default value is TLS v1.0. The TLS parameter is configured only if the client protocol is HTTPS. Enumeration values: • **TLS v1.0** • **TLS v1.1** • **TLS v1.2**

Parameter	Type	Description
cipher	String	The cipher parameter is available only if the client protocol is HTTPS. Its values are as follows, each representing a cryptographic algorithm: • cipher_1: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH • cipher_2: EECDH+AESGCM:EDH+AESGCM • cipher_3: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH • cipher_4: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH • cipher_default: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM Enumeration values: • **cipher_1** • **cipher_2** • **cipher_3** • **cipher_4** • **cipher_default**
protect_status	Integer	Protection status: • 0: disabled • 1: enabled Enumeration values: • **0** • **1**
access_status	Integer	Access status: • 0: not connected • 1: connected Enumeration values: • **0** • **1**
create_time	Long	Time when a domain name was created. The value is a 13-digit timestamp.

Parameter	Type	Description
block_page	**WafBlockPage** object	Alarm page configuration.
traffic_mark	**WafTrafficMark** object	Traffic identifier.
flag	**Flag** object	Special domain name tag.
extend	Map<String,String>	Extensible attribute of the domain name.
is_added	Boolean	Whether a domain name is an anti-DDoS domain name. Default: **false**

Table 4-27 WafBlockPage

Parameter	Type	Description
template	String	Blocking template name
custom_page	**WafCustomPage** object	User-defined blocking page
redirect_url	String	Redirection URL

Table 4-28 WafCustomPage

Parameter	Type	Description
status_code	String	Status code
content_type	String	Content type of alarm page
content	String	Page content Minimum: **1** Maximum: **4096**

Table 4-29 WafTrafficMark

Parameter	Type	Description
sip	Array of strings	IP address in the known attack source rule

Parameter	Type	Description
cookie	String	cookie Minimum: **1** Maximum: **4096**
params	String	Parameter Minimum: **1** Maximum: **4096**

Table 4-30 Flag

Parameter	Type	Description
pci_3ds	String	Whether to enable PCI 3DS compliance certification. • true: yes • false: no Enumeration values: • **true** • **false**
pci_dss	String	Whether to enable PCI DSS compliance certification. • true: yes • false: no Enumeration values: • **true** • **false**
cname	String	old: The old CNAME record is used. new: new CNAME record is used. Enumeration values: • **old** • **new**
is_dual_az	String	Whether IPv6 is enabled for the domain name. • true: yes • false: no Enumeration values: • **true** • **false**

Parameter	Type	Description
ipv6	String	Whether IPv6 is enabled for the domain name. • true: yes • false: no Enumeration values: • **true** • **false**

Status code: 400

Table 4-31 Response body parameters

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

Status code: 401

Table 4-32 Response body parameters

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

Status code: 500

Table 4-33 Response body parameters

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

Example Requests

Query the list of domain names protected by WAF.

```
GET https://{Endpoint}/v1/edgewaf/domains?page_num=1&page_size=10
```


Example Responses

Status code: 200

Request succeeded.


```
{
  "total" : 12,
  "domain_list" : [ {
    "id" : "095b60b21ac248579426f97379b3fbec",
    "domain_name" : "domain_name",
    "enterprise_project_id" : 0,
    "tenant_id" : "090f4899f400d33c0f17c00d4c8435e0",
    "open_time" : 1691478912415,
    "dispatch_status" : 3,
    "service_area" : "outside_mainland_china",
    "web_tag" : "domain_name",
    "description" : "example",
    "policy_id" : "1771a426afcc4e16b8636cb72c2d53e4",
    "protocol" : "https",
    "certificate_id" : "3e9df5da33744bae90bf73291c6e5c6c",
    "certificate_name" : "example",
    "tls" : "TLS v1.0",
    "cipher" : "cipher_1",
    "protect_status" : 1,
    "access_status" : 0,
    "is_added" : false
  } ]
}
```


Status Codes

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

Error Codes

See **Error Codes**.

4.2.3 Adding a Domain Name to WAF

Function

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

URI

POST /v1/edgewaf/domains

Request Parameters

Table 4-34 Request header parameters

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

Table 4-35 Request body parameters

Parameter	Mandatory	Type	Description
domain_name	Yes	String	Protected domain name, which can be obtained by calling the CDN domain name query API. The domain name can contain a port number.
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).
policy_id	No	String	ID of the policy associated with the protected domain name. It can be obtained by calling the API for querying WAF protection policies.
certificate_id	No	String	Certificate ID, which is obtained through the ListCertificates API. • This parameter is not required if the client protocol is HTTP. • This parameter is mandatory if the client protocol is HTTPS. • If the API for querying the certificate list is unavailable, log in to the EdgeSec console, and obtain the certificate ID from the certificate management page of Edge WAF.

Parameter	Mandatory	Type	Description
web_tag	No	String	Domain name.
description	No	String	Domain name description.
area_type	Yes	String	Region that the domain name belongs to. Obtain the value by calling the API for querying the CDN domain name. Enumeration values: • **mainland_china** • **outside_mainland_china** • **global** • **europe**

Response Parameters

Status code: 400

Table 4-36 Response body parameters

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

Status code: 401

Table 4-37 Response body parameters

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

Status code: 500

Table 4-38 Response body parameters

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

Example Requests

Add domain_name to be protected by WAF.

```
POST https://{Endpoint}/v1/edgewaf/domains

{
  "domain_name" : "domain_name",
  "enterprise_project_id" : 0,
  "policy_id" : "1771a426afcc4e16b8636cb72c2d53e4",
  "web_tag" : "domain_name",
  "description" : "demo",
  "area_type" : "outside_mainland_china"
}
```

Example Responses

None

Status Codes

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

Error Codes

See **Error Codes**.

4.2.4 Updating a Protected Domain Name

Function

This API is used to update a protected domain name.

URI

PUT /v1/edgewaf/domains/{domainid}

Table 4-39 Path Parameters

Parameter	Mandatory	Type	Description
domainid	Yes	String	Domain name.

Request Parameters

Table 4-40 Request header parameters

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

Table 4-41 Request body parameters

Parameter	Mandatory	Type	Description
protect_status	No	Integer	Protection status Minimum: **0** Maximum: **1**
access_status	No	Integer	Access status Minimum: **0** Maximum: **1**
web_tag	No	String	Domain name
description	No	String	Domain name description
certificate_id	No	String	Certificate ID, which is obtained through the ListCertificates API. • This parameter is not required if the client protocol is HTTP. • This parameter is mandatory if the client protocol is HTTPS. • If the API for querying the certificate list is unavailable, log in to the EdgeSec console, and obtain the certificate ID from the certificate management page of Edge WAF.
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Parameter	Mandatory	Type	Description
tls	No	String	Minimum TLS version (TLS v1.0, TLS v1.1, or TLS v1.2). The default value is TLS v1.0. The TLS parameter is configured only if the client protocol is HTTPS. Enumeration values: • **TLS v1.0** • **TLS v1.1** • **TLS v1.2**

Parameter	Mandatory	Type	Description
cipher	No	String	The cipher parameter is available only if the client protocol is HTTPS. Its values are as follows, each representing a cryptographic algorithm: • cipher_1: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH • cipher_2: EECDH+AESGCM:EDH+AESGCM • cipher_3: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH • cipher_4: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH • cipher_default: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM Enumeration values: • **cipher_1** • **cipher_2** • **cipher_3** • **cipher_4** • **cipher_default**
block_page	No	**WafBlockPage** object	Blocking page configuration

Parameter	Mandatory	Type	Description
traffic_mark	No	**WafTrafficMark** object	Traffic identifier (used for known attack source rules)
flag	No	**Flag** object	Special identifier, which is used by the frontend.
extend	No	Map<String,String>	Extensible field of the domain name.

Table 4-42 WafBlockPage

Parameter	Mandatory	Type	Description
template	Yes	String	Blocking template name
custom_page	No	**WafCustomPage** object	User-defined blocking page
redirect_url	No	String	Redirection URL

Table 4-43 WafCustomPage

Parameter	Mandatory	Type	Description
status_code	Yes	String	Status code
content_type	Yes	String	Content type of alarm page
content	Yes	String	Page content Minimum: **1** Maximum: **4096**

Table 4-44 WafTrafficMark

Parameter	Mandatory	Type	Description
sip	No	Array of strings	IP address in the known attack source rule
cookie	No	String	cookie Minimum: **1** Maximum: **4096**
params	No	String	Parameter Minimum: **1** Maximum: **4096**

Table 4-45 Flag

Parameter	Mandatory	Type	Description
pci_3ds	No	String	Whether to enable PCI 3DS compliance certification. • true: yes • false: no Enumeration values: • **true** • **false**
pci_dss	No	String	Whether to enable PCI DSS compliance certification. • true: yes • false: no Enumeration values: • **true** • **false**
cname	No	String	old: The old CNAME record is used. new: new CNAME record is used. Enumeration values: • **old** • **new**
is_dual_az	No	String	Whether IPv6 is enabled for the domain name. • true: yes • false: no Enumeration values: • **true** • **false**
ipv6	No	String	Whether IPv6 is enabled for the domain name. • true: yes • false: no Enumeration values: • **true** • **false**

Response Parameters

Status code: 400

Table 4-46 Response body parameters

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

Status code: 401

Table 4-47 Response body parameters

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

Status code: 500

Table 4-48 Response body parameters

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

Example Requests

Updating the WAF protection status of a domain name.

```
PUT https://{Endpoint}/v1/edgewaf/domains/1771a426afcc4e16b8636cb72c2d53e4

{
  "protect_status" : 1,
  "enterprise_project_id" : 0
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.

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

Error Codes

See **Error Codes**.

4.2.5 Deleting a Protected Domain Name

Function

This API is used to delete a protected domain name.

URI

DELETE /v1/edgewaf/domains/{domainid}

Table 4-49 Path Parameters

Parameter	Mandatory	Type	Description
domainid	Yes	String	Protected domain name ID.

Table 4-50 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Request Parameters

Table 4-51 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-52 Response body parameters

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

Status code: 401

Table 4-53 Response body parameters

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

Status code: 500

Table 4-54 Response body parameters

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

Example Requests

Delete domain_name protected by WAF.

```
Delete https://{Endpoint}/v1/edgewaf/domains/1771a426afcc4e16b8636cb72c2d53e4
```

Example Responses

None

Status Codes

Status Code	Description
200	ok

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

Error Codes

See **Error Codes**.

4.2.6 Querying a Protected Domain Name

Function

This API is used to query a protected domain name.

URI

GET /v1/edgewaf/domains/{domainid}

Table 4-55 Path Parameters

Parameter	Mandatory	Type	Description
domainid	Yes	String	Protected domain name ID.

Table 4-56 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Request Parameters

Table 4-57 Request header parameters

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

Response Parameters

Status code: 200

Table 4-58 Response body parameters

Parameter	Type	Description
id	String	Domain name ID.
domain_name	String	Domain name.
enterprise_project_id	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).
tenant_id	String	Tenant ID.
open_time	Long	Last time when protection was last enabled.
close_time	Long	Last time when protection was last disabled.
dispatch_status	Integer	CDN domain name scheduling status (0: not protected; 1: configuring; 2: protected; 3: deleting)
service_area	String	Region that the domain name belongs to.
web_tag	String	Domain name.
description	String	Domain name description.
policy_id	String	Policy ID.
protocol	String	Protocol. Enumeration values: • **http** • **https**
certificate_id	String	Certificate ID.
certificate_name	String	Certificate name.

Parameter	Type	Description
tls	String	Minimum TLS version (TLS v1.0, TLS v1.1, or TLS v1.2). The default value is TLS v1.0. The TLS parameter is configured only if the client protocol is HTTPS. Enumeration values: • **TLS v1.0** • **TLS v1.1** • **TLS v1.2**
cipher	String	The cipher parameter is available only if the client protocol is HTTPS. Its values are as follows, each representing a cryptographic algorithm: • cipher_1: ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH • cipher_2: EECDH+AESGCM:EDH+AESGCM • cipher_3: ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH • cipher_4: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH • cipher_default: ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM Enumeration values: • **cipher_1** • **cipher_2** • **cipher_3** • **cipher_4** • **cipher_default**
protect_status	Integer	Protection status: • 0: disabled • 1: enabled Enumeration values: • **0** • **1**

Parameter	Type	Description
access_status	Integer	Access status: • 0: not connected • 1: connected Enumeration values: • **0** • **1**
create_time	Long	Time when a domain name was created. The value is a 13-digit timestamp.
block_page	**WafBlockPage** object	Alarm page configuration.
traffic_mark	**WafTrafficMark** object	Traffic identifier.
flag	**Flag** object	Special domain name tag.
extend	Map<String,String>	Extensible attribute of the domain name.
is_added	Boolean	Whether a domain name is an anti-DDoS domain name. Default: **false**

Table 4-59 WafBlockPage

Parameter	Type	Description
template	String	Blocking template name
custom_page	**WafCustomPage** object	User-defined blocking page
redirect_url	String	Redirection URL

Table 4-60 WafCustomPage

Parameter	Type	Description
status_code	String	Status code
content_type	String	Content type of alarm page
content	String	Page content Minimum: **1** Maximum: **4096**

Table 4-61 WafTrafficMark

Parameter	Type	Description
sip	Array of strings	IP address in the known attack source rule
cookie	String	cookie Minimum: **1** Maximum: **4096**
params	String	Parameter Minimum: **1** Maximum: **4096**

Table 4-62 Flag

Parameter	Type	Description
pci_3ds	String	Whether to enable PCI 3DS compliance certification. • true: yes • false: no Enumeration values: • **true** • **false**
pci_dss	String	Whether to enable PCI DSS compliance certification. • true: yes • false: no Enumeration values: • **true** • **false**
cname	String	old: The old CNAME record is used. new: new CNAME record is used. Enumeration values: • **old** • **new**

Parameter	Type	Description
is_dual_az	String	Whether IPv6 is enabled for the domain name. • true: yes • false: no Enumeration values: • **true** • **false**
ipv6	String	Whether IPv6 is enabled for the domain name. • true: yes • false: no Enumeration values: • **true** • **false**

Status code: 400

Table 4-63 Response body parameters

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

Status code: 401

Table 4-64 Response body parameters

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

Status code: 500

Table 4-65 Response body parameters

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

Example Requests

Query details about domain names protected by WAF.

```
GET https://{Endpoint}/v1/edgewaf/domains/1771a426afcc4e16b8636cb72c2d53e4
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "id" : "095b60b21ac248579426f97379b3fbec",
  "domain_name" : "domain_name",
  "enterprise_project_id" : 0,
  "tenant_id" : "090f4899f400d33c0f17c00d4c8435e0",
  "open_time" : 1691478912415,
  "dispatch_status" : 3,
  "service_area" : "outside_mainland_china",
  "web_tag" : "domain_name",
  "description" : "example",
  "policy_id" : "1771a426afcc4e16b8636cb72c2d53e4",
  "protocol" : "https",
  "certificate_id" : "3e9df5da33744bae90bf73291c6e5c6c",
  "certificate_name" : "example",
  "tls" : "TLS v1.0",
  "cipher" : "cipher_1",
  "protect_status" : 1,
  "access_status" : 0,
  "is_added" : false
}
```

Status Codes

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

Error Codes

See **Error Codes**.

4.2.7 Updating Domain Names in a Protection Policy

Function

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

URI

POST /v1/edgewaf/policies/{policy_id}/hosts

Table 4-66 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Protection policy ID, which can be obtained by querying the policy list (ListPolicy).

Request Parameters

Table 4-67 Request header parameters

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

Table 4-68 Request body parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).
hosts	Yes	Array of strings	ID of the domain name to be associated.

Response Parameters

Status code: 200

Table 4-69 Response body parameters

Parameter	Type	Description
id	String	Policy ID.
name	String	Policy name.
action	**WafPolicyAction** object	Protection action
options	**WafPolicyOption** object	Whether a protection item is enabled in a protection policy.

Parameter	Type	Description
level	Integer	Protection level.
full_detection	Boolean	Detection mode in the precise protection rule.
robot_action	**WafPolicyAction** object	Information about anti-crawler protection with feature libraries
bind_host	Array of **WafPolicyBindHost** objects	Basic information about the protected domain.
timestamp	Long	Time a policy was created.
extend	Map<String,String>	Extended field.

Table 4-70 WafPolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled. Enumeration values: • **true** • **false**
common	Boolean	Whether general check is enabled. Enumeration values: • **true** • **false**
bot_enable	Boolean	Whether full anti-crawler protection is enabled. Enumeration values: • **true** • **false**
crawler	Boolean	Whether anti-crawler protection with feature libraries is enabled. Enumeration values: • **true** • **false**
crawler_engine	Boolean	Whether the search engine is enabled. Enumeration values: • **true** • **false**

Parameter	Type	Description
crawler_scanner	Boolean	Whether the scanner is enabled. Enumeration values: • **true** • **false**
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled. Enumeration values: • **true** • **false**
crawler_other	Boolean	Whether other crawler check is enabled. Enumeration values: • **true** • **false**
webshell	Boolean	Whether web shell detection is enabled Enumeration values: • **true** • **false**
cc	Boolean	Whether the CC attack protection rules are enabled. Enumeration values: • **true** • **false**
custom	Boolean	Whether precise protection is enabled. Enumeration values: • **true** • **false**
followed_action	Boolean	Whether known attack source detection is enabled. Enumeration values: • **true** • **false**
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled. Enumeration values: • **true** • **false**

Parameter	Type	Description
geoip	Boolean	Whether the geolocation rule is enabled. Enumeration values: • **true** • **false**
ignore	Boolean	Whether false alarm masking is enabled. Enumeration values: • **true** • **false**
privacy	Boolean	Whether data masking is enabled. Enumeration values: • **true** • **false**
antitamper	Boolean	Whether the web tamper protection is enabled. Enumeration values: • **true** • **false**
antileakage	Boolean	Whether the information leakage prevention is enabled. Enumeration values: • **true** • **false**
anticrawler	Boolean	Whether the JavaScript anti-crawler rule is enabled. Enumeration values: • **true** • **false**

Table 4-71 WafPolicyAction

Parameter	Type	Description
category	String	Basic web protection action (log: record only; block: block) Enumeration values: • **block** • **log**
followed_action_id	String	Known attack source rule ID

Table 4-72 WafPolicyBindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-73 Response body parameters

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

Status code: 401

Table 4-74 Response body parameters

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

Status code: 500

Table 4-75 Response body parameters

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

Example Requests

Apply the policy whose ID is 1771a426afcc4e16b8636cb72c2d53e4 to the domain name whose ID is 095b60b21ac248579426f97379b3fbec.

```
POST https://{Endpoint}/v1/edgewaf/policies/1771a426afcc4e16b8636cb72c2d53e4/hosts

{
  "enterprise_project_id" : 0,
  "hosts" : [ "095b60b21ac248579426f97379b3fbec" ]
}
```


Example Responses

Status code: 200

Request succeeded.


```
{
  "id" : "1771a426afcc4e16b8636cb72c2d53e4",
  "name" : "demo_policy",
  "action" : {
    "category" : "log"
  },
  "options" : {
    "webattack" : true,
    "common" : true,
    "bot_enable" : true,
    "crawler" : true,
    "crawler_engine" : false,
    "crawler_scanner" : true,
    "crawler_script" : false,
    "crawler_other" : false,
    "webshell" : false,
    "cc" : true,
    "custom" : true,
    "followed_action" : false,
    "whiteblackip" : true,
    "geoip" : true,
    "ignore" : true,
    "privacy" : true,
    "antitamper" : true,
    "antileakage" : false,
    "anticrawler" : false
  },
  "level" : 2,
  "full_detection" : false,
  "robot_action" : {
    "category" : "log"
  },
  "bind_host" : [ {
    "id" : "095b60b21ac248579426f97379b3fbec",
    "name" : "domain_name"
  } ],
  "timestamp" : 1691478911117
}
```


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 WAF Policy Management

4.3.1 Querying a Policy List

Function

This API is used to query the policy list.

URI

GET /v1/{project_id}/waf/policy

Table 4-76 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain its value, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list.

Table 4-77 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).
page	No	Integer	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. Default: **1**
pagesize	No	Integer	Number of results on each page in query pagination. The value range is 1 to 100. The default value is **10**, indicating that each page contains 10 results. Default: **10**

Parameter	Mandatory	Type	Description
name	No	String	Policy name.

Request Parameters

Table 4-78 Request header parameters

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

Response Parameters

Status code: 200

Table 4-79 Response body parameters

Parameter	Type	Description
total	Integer	Total number of policies
items	Array of **PolicyResponse** objects	Content of the policy

Table 4-80 PolicyResponse

Parameter	Type	Description
id	String	Policy ID
name	String	Policy name

Parameter	Type	Description
level	Integer	Basic web protection level: • 1: Loose. The protection granularity is coarse. Only requests with obvious attack characteristics are blocked. If a large number of false alarms are reported, Low 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: **2** Enumeration values: • **1** • **2** • **3**
full_detection	Boolean	Detection mode in the precise protection rule. • 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 finishes its scan first and then blocks all requests that match the configured precise protection rule.
robot_action	**Action** object	Information about anti-crawler protection with feature libraries
action	**PolicyAction** object	Protection action
options	**PolicyOption** object	Whether a protection item is enabled in a protection policy.
modulex_options	Map<String,Object>	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.
hosts	Array of strings	ID array of protected domain names bound to a protection policy.

Parameter	Type	Description
bind_host	Array of **BindHost** objects	Array of protected domain names bound to a protection policy. It contains more detailed domain name information than the hosts field.
extend	Map<String,String>	Extended field, which is used to store the switch configuration of basic web protection.
timestamp	Long	Time a policy was created.

Table 4-81 Action

Parameter	Type	Description
category	String	Action to be taken in anti-crawler protection with feature libraries: • log: record only • block: block

Table 4-82 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action (log: record only; block: block) Enumeration values: • **block** • **log**

Table 4-83 PolicyOption

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

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

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

Table 4-84 BindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-85 Response body parameters

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

Status code: 401

Table 4-86 Response body parameters

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

Status code: 500

Table 4-87 Response body parameters

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

Example Requests

Query WAF protection policies.

```
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_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" : 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**.

4.3.2 Creating a Protection Policy

Function

A protection policy you create contains default configuration items. To modify these configuration items, you need to call this API to update the protection policy.

URI

POST /v1/{project_id}/waf/policy

Table 4-88 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain its value, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list.

Table 4-89 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Request Parameters

Table 4-90 Request header parameters

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

Table 4-91 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Policy name (The policy name can contain only digits, letters, and underscores (_) and cannot exceed 64 characters.)

Response Parameters

Status code: 200

Table 4-92 Response body parameters

Parameter	Type	Description
id	String	Policy ID
name	String	Policy name
level	Integer	Basic web protection level: • 1: Loose. The protection granularity is coarse. Only requests with obvious attack characteristics are blocked. If a large number of false alarms are reported, Low 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: **2** Enumeration values: • **1** • **2** • **3**

Parameter	Type	Description
full_detection	Boolean	Detection mode in the precise protection rule. • 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 finishes its scan first and then blocks all requests that match the configured precise protection rule.
robot_action	**Action** object	Action taken for anti-crawler protection with feature libraries
action	**PolicyAction** object	Action
options	**PolicyOption** object	Whether to enable the protection policy detection module, for example, whether to enable basic web protection.
modulex_options	Map<String,Object>	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.
hosts	Array of strings	ID array of protected domain names bound to a protection policy.
bind_host	Array of **BindHost** objects	Array of protected domain names bound to a protection policy. It contains more detailed domain name information than the hosts field.
extend	Map<String,String>	Extended field, which is used to store the switch configuration of basic web protection.
timestamp	Long	Time a policy was created.

Table 4-93 Action

Parameter	Type	Description
category	String	Action to be taken in anti-crawler protection with feature libraries: • log: record only • block: block

Table 4-94 PolicyAction

Parameter	Type	Description
category	String	Basic web protection action (log: record only; block: block) Enumeration values: • **block** • **log**

Table 4-95 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled. Enumeration values: • **true** • **false**
common	Boolean	Whether general check is enabled. Enumeration values: • **true** • **false**
crawler	Boolean	Reserved parameter. Its value is always true. You can ignore this parameter. Enumeration values: • **true** • **false**
crawler_engine	Boolean	Whether the search engine is enabled. Enumeration values: • **true** • **false**
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled. Enumeration values: • **true** • **false**
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled. Enumeration values: • **true** • **false**

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

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

Table 4-96 BindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-97 Response body parameters

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

Status code: 401

Table 4-98 Response body parameters

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

Status code: 403

Table 4-99 Response body parameters

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

Status code: 500

Table 4-100 Response body parameters

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

Example Requests

Create a protection policy named **demo** in the project whose ID is 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**.

4.3.3 Deleting a Protection Policy

Function

This API is used to delete a protection policy. If the policy is in use, you need to unbind domain names from the policy first.

URI

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

Table 4-101 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain its value, log in to the Huawei Cloud console, click the username, choose **My Credentials**, and find the project ID in the **Projects** list.
policy_id	Yes	String	Protection policy ID. You can call the ListPolicy API to obtain the policy ID.

Table 4-102 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Request Parameters

Table 4-103 Request header parameters

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

Response Parameters

Status code: 200

Table 4-104 Response body parameters

Parameter	Type	Description
id	String	Policy ID.
name	String	Policy name.
level	Integer	Basic web protection level: • 1: Loose. The protection granularity is coarse. Only requests with obvious attack characteristics are blocked. If a large number of false alarms are reported, Low 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: **2** Enumeration values: • **1** • **2** • **3**
full_detection	Boolean	Detection mode in the precise protection rule. • 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 finishes its scan first and then blocks all requests that match the configured precise protection rule.
robot_action	**Action** object	Action used for anti-crawler protection with feature libraries.
action	**WafPolicyAction** object	Protection action.
options	**PolicyOption** object	Whether a protection item is enabled in a protection policy.

Parameter	Type	Description
modulex_options	Map<String,Object>	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.
hosts	Array of strings	ID array of protected domain names bound to a protection policy.
bind_host	Array of **BindHost** objects	Array of protected domain names bound to a protection policy. It contains more detailed domain name information than the hosts field.
extend	Map<String,String>	Extended field, which is used to store the switch configuration of basic web protection.
timestamp	Long	Time a policy was created.

Table 4-105 Action

Parameter	Type	Description
category	String	Action to be taken in anti-crawler protection with feature libraries: • log: record only • block: block

Table 4-106 WafPolicyAction

Parameter	Type	Description
category	String	Basic web protection action (log: record only; block: block) Enumeration values: • **block** • **log**
followed_action_id	String	Known attack source rule ID

Table 4-107 PolicyOption

Parameter	Type	Description
webattack	Boolean	Whether basic web protection is enabled. Enumeration values: • **true** • **false**
common	Boolean	Whether general check is enabled. Enumeration values: • **true** • **false**
crawler	Boolean	Reserved parameter. Its value is always true. You can ignore this parameter. Enumeration values: • **true** • **false**
crawler_engine	Boolean	Whether the search engine is enabled. Enumeration values: • **true** • **false**
crawler_scanner	Boolean	Whether the anti-crawler detection is enabled. Enumeration values: • **true** • **false**
crawler_script	Boolean	Whether the JavaScript anti-crawler is enabled. Enumeration values: • **true** • **false**
crawler_other	Boolean	Whether other crawler check is enabled. Enumeration values: • **true** • **false**
webshell	Boolean	Whether webshell detection is enabled. Enumeration values: • **true** • **false**

Parameter	Type	Description
cc	Boolean	Whether the CC attack protection rules are enabled. Enumeration values: • **true** • **false**
custom	Boolean	Whether precise protection is enabled. Enumeration values: • **true** • **false**
whiteblackip	Boolean	Whether blacklist and whitelist protection is enabled. Enumeration values: • **true** • **false**
geoip	Boolean	Whether geolocation access control is enabled. Enumeration values: • **true** • **false**
ignore	Boolean	Whether false alarm masking is enabled. Enumeration values: • **true** • **false**
privacy	Boolean	Whether data masking is enabled. Enumeration values: • **true** • **false**
antitamper	Boolean	Whether the web tamper protection is enabled. Enumeration values: • **true** • **false**
antileakage	Boolean	Whether the information leakage prevention is enabled. Enumeration values: • **true** • **false**

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

Table 4-108 BindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-109 Response body parameters

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

Status code: 401

Table 4-110 Response body parameters

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

Status code: 500

Table 4-111 Response body parameters

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

Example Requests

Delete the protection policy whose ID is policy_id from the project whose ID is project_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**.

4.4 Anti-DDoS Domain Name Management

4.4.1 Adding a Domain Name to WAF for Anti-DDoS Protection

Function

This API is used to add a domain name for DDoS protection.

URI

POST /v1/edgeddos/domains

Request Parameters

Table 4-112 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-113 Request body parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	WAF protection domain name ID

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Response Parameters

Status code: 400

Table 4-114 Response body parameters

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

Status code: 401

Table 4-115 Response body parameters

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

Status code: 500

Table 4-116 Response body parameters

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

Example Requests

Add the domain name whose ID is 095b60b21ac248579426f97379b3fbec as an anti-DDoS domain name.

```
POST https://{Endpoint}/v1/edgeddos/domains

{
```



```
  "domain_id" : "095b60b21ac248579426f97379b3fbec",
  "enterprise_project_id" : 0
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	The account corresponding to the token does not have sufficient permission.
500	Internal server error.

Error Codes

See **Error Codes**.

4.4.2 Querying an Anti-DDoS Domain Name

Function

This API is used to query a tenant's Anti-DDoS domain name.

URI

GET /v1/edgeddos/domains

Table 4-117 Query Parameters

Parameter	Mandatory	Type	Description
domain_name	No	String	Domain name.
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Parameter	Mandatory	Type	Description
offset	No	Integer	Offset, which is the position where the query starts. The value must be greater than or equal to 0. Minimum: **0** Default: **0**
limit	No	Integer	Number of records displayed on each page Minimum: **1** Maximum: **1000** Default: **10**

Request Parameters

Table 4-118 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 200

Table 4-119 Response body parameters

Parameter	Type	Description
domain_list	Array of **EdgeDDoSDomainVo** objects	Domain name.
total	Long	Total number of domain names Minimum: **0** Default: **0**

Table 4-120 EdgeDDoSDomainVo

Parameter	Type	Description
id	String	Domain name ID

Parameter	Type	Description
domain_name	String	Domain name.
tenant_id	String	Tenant ID.
area_type	String	Region that the domain name belongs to. Enumeration values: • **mainland_china** • **outside_mainland_china** • **europe** • **global**
dispatch_status	Integer	CDN domain name scheduling status (0: not protected; 1: configuring; 2: protected; 3: deleting)
protected_switch	Integer	Protection switch (0: off; 1: on)
open_date	Long	Start time
close_date	Long	Closing time
enterprise_project_id	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Status code: 400

Table 4-121 Response body parameters

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

Status code: 401

Table 4-122 Response body parameters

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

Status code: 500

Table 4-123 Response body parameters

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

Example Requests

View the list of anti-DDoS domain names.

```
GET https://{Endpoint}/v1/edgeddos/domains?limit=10
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 1,
  "domain_list" : [ {
    "id" : "095b60b21ac248579426f97379b3fbec",
    "domain_name" : "domain_name",
    "tenant_id" : "e5865897eb404d2e88e104f3fe3abff1",
    "area_type" : "outside_mainland_china",
    "dispatch_status" : 2,
    "protected_switch" : 1,
    "open_date" : 1691478911117,
    "enterprise_project_id" : 0
  } ]
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	The account corresponding to the token does not have sufficient permission.
500	Internal server error.

Error Codes

See **Error Codes**.

4.4.3 Updating an Anti-DDoS Domain Name

Function

This API is used to update an anti-DDoS domain name.

URI

PUT /v1/edgeddos/domains/{domainid}

Table 4-124 Path Parameters

Parameter	Mandatory	Type	Description
domainid	Yes	String	Domain name ID.

Request Parameters

Table 4-125 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Table 4-126 Request body parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).
protected_switch	Yes	Integer	Protection switch (0: off; 1: on) Default: **0** Enumeration values: • **0** • **1**

Response Parameters

Status code: 400

Table 4-127 Response body parameters

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

Status code: 401

Table 4-128 Response body parameters

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

Status code: 500

Table 4-129 Response body parameters

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

Example Requests

Enable protection for the domain name whose ID is 095b60b21ac248579426f97379b3fbec.

```
PUT https://{Endpoint}/v1/edgeddos/domains/095b60b21ac248579426f97379b3fbec

{
  "protected_switch" : 1
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.

Status Code	Description
400	Invalid request parameter.
401	The account corresponding to the token does not have sufficient permission.
500	Internal server error.

Error Codes

See **Error Codes**.

4.4.4 Deleting an Anti-DDoS Domain Name

Function

This API is used to delete an anti-DDoS domain name.

URI

DELETE /v1/edgeddos/domains/{domainid}

Table 4-130 Path Parameters

Parameter	Mandatory	Type	Description
domainid	Yes	String	Domain name ID.

Table 4-131 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Request Parameters

Table 4-132 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	auth token

Response Parameters

Status code: 400

Table 4-133 Response body parameters

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

Status code: 401

Table 4-134 Response body parameters

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

Status code: 500

Table 4-135 Response body parameters

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

Example Requests

Delete the anti-DDoS domain name whose ID is 095b60b21ac248579426f97379b3fbec.

```
DELETE https://{Endpoint}/v1/edgeddos/domains/095b60b21ac248579426f97379b3fbec
```

Example Responses

None

Status Codes

Status Code	Description
200	Request succeeded.

Status Code	Description
400	Invalid request parameter.
401	The account corresponding to the token does not have sufficient permission.
500	Internal server error.

Error Codes

See **Error Codes**.

4.5 Tenant Subscription Management

4.5.1 Querying Purchased EdgeSec Products

Function

This API is used to query purchased EdgeSec products.

URI

GET /v1/edgesec/subscription

Table 4-136 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Obtain the enterprise project ID by calling the ListEnterpriseProject API of Enterprise Project Management Service (EPS).

Request Parameters

Table 4-137 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token. It can be obtained by calling the IAM API (value of X-Subject-Token in the response header).

Response Parameters

Status code: 200

Table 4-138 Response body parameters

Parameter	Type	Description
waf_domain_num	Integer	Number of WAF domain names that have been added
waf_rule_num	Integer	Number of added WAF IP address blacklist and whitelist rules
ddos_domain_num	Integer	Number of added anti-DDoS domain names
product_infos	Array of **EdgeSecProductResource** objects	Product details

Table 4-139 EdgeSecProductResource

Parameter	Type	Description
order_id	String	ID of the order for purchasing the resource.
cloud_service_type	String	Cloud service type. The value for EdgeSec is hws.service.type.edgesec.
product_id	String	Product ID
resource_id	String	Resource ID
enterprise_project_id	String	Enterprise project ID
region_id	String	region ID
resource_type	String	Resource type
resource_spec_code	String	The resource specification code.
resource_size	Integer	Number of extension package resources.
bill_type	Integer	Billing method (0: not billed by traffic; 1: billed by peak bandwidth; 2: billed by traffic) Enumeration values: • **0** • **1** • **2**

Parameter	Type	Description
charging_mode	String	Billing mode. The value can be 1 (one-off, yearly/monthly) or 2 (pay-per-use). Enumeration values: • 1 • 2

Status code: 400

Table 4-140 Response body parameters

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

Status code: 401

Table 4-141 Response body parameters

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

Status code: 500

Table 4-142 Response body parameters

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

Example Requests

Query purchased EdgeSec products.

```
GET https://{Endpoint}/v1/edgesec/products

{
  "enterprise_project_id" : 0
}
```


Example Responses

Status code: 200

Request succeeded.


```
{
  "waf_domain_num" : 4,
  "waf_rule_num" : 0,
  "ddos_domain_num" : 30,
  "ddos_rule_num" : 0,
  "product_infos" : [ {
    "order_id" : "CS23051715154AMJZ",
    "cloud_service_type" : "hws.service.type.edgesec",
    "product_id" : "OFFI847313454219157506",
    "resource_id" : "148bdfa5-6b79-47d3-86ea-eed43f887248",
    "enterprise_project_id" : 0,
    "region_id" : "ap-south-east-1",
    "resource_type" : "hws.resource.type.edgeddos",
    "resource_spec_code" : "edgesec.ddos.basic.abroad",
    "resource_size" : 0,
    "bill_type" : 0,
    "charging_mode" : "prePaid"
  }, {
    "order_id" : "CS23051715154AMJZ",
    "cloud_service_type" : "hws.service.type.edgesec",
    "product_id" : "OFFI847291260949225474",
    "resource_id" : "7ee6a5c8-2fe4-45e5-8ac7-1192248a5969",
    "enterprise_project_id" : 0,
    "region_id" : "ap-south-east-1",
    "resource_type" : "hws.resource.type.edgewaf",
    "resource_spec_code" : "edgewaf.professional.abroad",
    "resource_size" : "0,",
    "bill_type" : "0,",
    "charging_mode" : "prePaid"
  } ]
}
```


Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	The account corresponding to the token does not have sufficient permission.
500	Internal server error.

Error Codes

See **Error Codes**.

4.6 WAF Certificate Management

4.6.1 Querying the Certificate List

Function

This API is used to query the list of certificates.

URI

GET /v1/{project_id}/waf/certificate

Table 4-143 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to the 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.

Table 4-144 Query Parameters

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

Parameter	Mandatory	Type	Description
host	No	Boolean	Whether to obtain the domain name for which the certificate is used. The default value is **false**. • **true**: Obtain the certificates that have been used for domain names. • **false**: Obtain the certificates that have not been used for any domain name. Default: **false**
exp_status	No	Integer	Certificate status. The options are as follows: 0: not expired; 1: expired; 2: about to expire (The certificate will expire within one month.)

Request Parameters

Table 4-145 Request header parameters

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

Response Parameters

Status code: 200

Table 4-146 Response body parameters

Parameter	Type	Description
items	Array of **CertificateBody** objects	Certificate list.

Parameter	Type	Description
total	Integer	Total number of certificates

Table 4-147 CertificateBody

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name.
expire_time	Long	Certificate expiration time, in timestamp format.
exp_status	Integer	Certificate status. The value can be: **0**: The certificate is valid. **1**: The certificate has expired. **2**: The certificate will expire within one month.
timestamp	Long	Time the certificate was uploaded, in timestamp format.
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-148 BindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-149 Response body parameters

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

Status code: 401

Table 4-150 Response body parameters

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

Status code: 500

Table 4-151 Response body parameters

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

Example Requests

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

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

Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.6.2 Creating a Certificate

Function

This API is used to create a certificate.

URI

POST /v1/{project_id}/waf/certificate

Table 4-152 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to the 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.

Table 4-153 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 4-154 Request header parameters

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

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

Table 4-155 Request body parameters

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

Response Parameters

Status code: 200

Table 4-156 Response body parameters

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name.
content	String	Certificate file in PEM format
key	String	Private key of the certificate, which is in PEM format.
expire_time	Long	Certificate expiration timestamp

Parameter	Type	Description
exp_status	Integer	Certificate status. The options can be: **0**: The certificate has not expire. **1**: The certificate expired. **2**: The certificate is about to expire.
timestamp	Long	Certificate upload timestamp
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-157 BindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-158 Response body parameters

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

Status code: 401

Table 4-159 Response body parameters

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

Status code: 500

Table 4-160 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

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


Example Responses

Status code: 200

OK

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

Status Codes

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

Error Codes

See **Error Codes**.

4.6.3 Querying a Certificate

Function

This API is used to query a certificate.

URI

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

Table 4-161 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to the 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.

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	HTTPS certificate ID. It can be obtained by calling the **ListCertificates** API.

Table 4-162 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 4-163 Request header parameters

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

Response Parameters

Status code: 200

Table 4-164 Response body parameters

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name.
content	String	Certificate file, PEM encoding
key	String	Private key of the certificate, which is in PEM format.
expire_time	Long	Certificate expiration timestamp

Parameter	Type	Description
exp_status	Integer	Certificate status. The options can be: **0**: The certificate has not expire. **1**: The certificate expired. **2**: The certificate is about to expire.
timestamp	Long	Certificate upload timestamp
bind_host	Array of **BindHost** objects	Domain name associated with the certificate

Table 4-165 BindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-166 Response body parameters

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

Status code: 401

Table 4-167 Response body parameters

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

Status code: 500

Table 4-168 Response body parameters

Parameter	Type	Description
error_code	String	Error code.

Parameter	Type	Description
error_msg	String	Error message.

Example Requests

The following example shows how to query a 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
aWNsb3VkLmNvbTAeFw0yMDA3MDkwNTQ2MDRaFw0yMDA4MDgwNTQ2MDRaMFExCzAJBgNVBAYTAkFV
MRMwEQYDVQQIDApTb21lLVN0YXRlMQ8wDQYDVQQKDAZIdWF3ZWkxHDAaBgNVBAMME3dhZi5odWF3Z
WljbG91ZC5jb20wXDANBgkqhkiG9w0BAQEFAANLADBIAkEA0UEbMzbvgOJTKrKcDUw9xjFqxM7BaQFM3SLs
QlmD5hkzygyL1ra
+cWajPJlTCxz9Ph6qldna2+OrIuTdvCcpjwIDAQABo1MwUTAdBgNVHQ4EFgQUE7ZQNcgl3lmryx1s5gy9mnC1rs
YwHwYDVR0jBBgwFoAUE7ZQNcgl3lmryx1s5gy9mnC1rsYwDwYDVR0TAQH/BAUwAwEB/
zANBgkqhkiG9w0BAQsFAANBAM5wGi88jYWLgOnGbae5hH3I9lMBKxGqv17Cbm1tjWuUogVINz86lqvCpuhzLv
D/vzJAqPIuDwqM8uvzjgRfZs8=\n-----END CERTIFICATE-----",
  "key" : "-----BEGIN RSA PRIVATE KEY-----
\nMIIBOQIBAAJBANFBGzM274DiUyqynA1MPcYxasTOwWkBTN0i7EJZg+YZM8oMi9a2vnFmozyZUwsc/
T4eqpXZ2tvjqyLk3bwnKY8CAwEAAQJBAI7LMPaH/HQk/b/bVmY0qsr
+me9nb9BqFLuqwzKbx0hSmWPOWFsd3rOFlSopyHqgYtAsPfvPumEdGbdnCyU8zAEClQD71768K1ejb
+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**.

4.6.4 Deleting a Certificate

Function

This API is used to delete a certificate.

URI

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

Table 4-169 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to the 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.
certificate_id	Yes	String	HTTPS certificate ID. It can be obtained by calling the **ListCertificates** API.

Table 4-170 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 4-171 Request header parameters

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

Response Parameters

Status code: 200

Table 4-172 Response body parameters

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

Table 4-173 BindHost

Parameter	Type	Description
id	String	Domain name ID.
hostname	String	Domain name.

Status code: 400

Table 4-174 Response body parameters

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

Status code: 401

Table 4-175 Response body parameters

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

Status code: 500

Table 4-176 Response body parameters

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

Example Requests

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

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

Example Responses

Status code: 200

OK

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


Status Codes

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

Error Codes

See **Error Codes**.

4.6.5 Modifying a Certificate

Function

This API is used to modify a certificate.

URI

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

Table 4-177 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. To obtain it, go to the 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.
certificate_id	Yes	String	HTTPS certificate ID. It can be obtained by calling the **ListCertificates** API.

Table 4-178 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 4-179 Request header parameters

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

Table 4-180 Request body parameters

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

Response Parameters

Status code: 200

Table 4-181 Response body parameters

Parameter	Type	Description
id	String	Certificate ID.
name	String	Certificate name.
expire_time	Long	Time the certificate expires, in timestamp format.
timestamp	Long	Timestamp

Status code: 400

Table 4-182 Response body parameters

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

Status code: 401

Table 4-183 Response body parameters

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

Status code: 500

Table 4-184 Response body parameters

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

Example Requests

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

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

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

Example Responses

Status code: 200

OK

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

Status Codes

Status Code	Description
200	OK
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

Status Code	Description	Description
200	OK	The request is successfully processed.

- Abnormal

Status Code	Description	Description
400	Bad Request	It is a bad request.
401	Unauthorized	You do not have permissions to perform this action.
403	Forbidden	Access is denied.
404	Not Found	The page is not found.
500	Internal Server Error	There is an internal server error.

A.2 Error Codes

If an error code starting with APIGW is returned after you call an API, rectify the fault by referring to the instructions provided in **API Gateway Error Codes**.

Status Code	Error Codes	Error Message	Description	Solution
400	EdgeSec.00000007	Invalid Domain dispatch status.	Invalid domain name scheduling status.	Contact technical support.
400	EdgeSec.00000009	Invalid domain.	Invalid domain name.	Check the domain name.
400	EdgeSec.00000012	Invalid area type.	Invalid service region.	Check the domain name and the service region of the purchased product.
400	EdgeSec.00000014	Not support operation in this enterprise project.	Operation not supported for the current enterprise project.	Check the permissions for the current enterprise project.
400	EdgeSec.00000015	All enterprise projects do not support write operations.	Write operation not supported for "All project".	Check the permissions for "All project".
400	EdgeSec.00000016	Tms Illegal Request.	Invalid request for the tag management system.	Check the request input parameters or contact Huawei technical support.
400	EdgeSec.00000017	Duplicate resource id.	Duplicate resource IDs.	Check the resource ID in the request input parameters or contact technical support.
400	EdgeSec.00000018	This version only supports default enterprise project.	The current version only supports resource management using the default enterprise project.	Use the default enterprise project to manage resources.

Status Code	Error Codes	Error Message	Description	Solution
400	EdgeSec.00000019	Frozen can not create eps tag.	EdgeSec resources are frozen and tags cannot be managed.	Unfreeze EdgeSec resources.
400	EdgeSec.00010003	Domain name ineligible for this feature.	The domain name does not support this function.	Check the domain name.
400	EdgeSec.00010004	Domain Already Exists.	The domain name already exists.	Check the domain name.
400	EdgeSec.00010006	Blacklist and whitelist rules of an edge WAF policy exceed the quota.	Blacklist and Whitelist Rules of Edge WAF Exceed the Quota	1.Delete unnecessary blacklist and whitelist rules so that the number of blacklist and whitelist rules in each policy does not exceed the current quota;Blacklist and whitelist rule quota = Edition quota + Number of rule expansion packages x 10. For example, if you use the professional edition of edge WAF and have two rule expansion packages, you can create 120 blacklist and whitelist rules (100 + 2 x 10 = 120).

Status Code	Error Codes	Error Message	Description	Solution
400	EdgeSec.00010007	The IP address group quota of edge WAF is insufficient.	Insufficient IP Address Group Quota of Edge WAF	For details about how to view the IP address group quota, see https://support.huaweicloud.com/en-us/usermanual-edgesec/edgesec_01_0058.html#section1. If the IP address group quota is insufficient, contact technical support.
400	EdgeSec.00010008	The edge WAF certificate quota is insufficient.	Insufficient Edge WAF Certificate Quota	The certificate quota is the same as the domain name quota. Purchase the domain name expansion package of the edge WAF.
400	EdgeSec.00020001	Must enable waf protection first.	To enable anti-DDoS protection for a domain name, enable WAF first.	Enable WAF for the domain name.
400	EdgeSec.00020002	Domain Already Exists.	The anti-DDoS domain name already exists.	Check the domain name.
400	EdgeSec.00030001	Illegal ElasticSearch Request.	An error occurred when querying protection data.	Check the query parameters.
400	EdgeSec.00030002	Search Error.	An error occurred when querying protection data.	Check the query parameters.

Status Code	Error Codes	Error Message	Description	Solution
400	EdgeSec.00030003	Statistic Type Error.	An error occurred when querying the protected data type.	Check the protected data type.
400	EdgeSec.00040004	The customer has purchased this product.	You have purchased the product.	Cancel purchase or contact technical support.
400	EdgeSec.00040007	No Permission To Operate.	EdgeSec has been unsubscribed from or frozen. You do not have the permission to perform this operation.	Purchase EdgeSec or contact technical support.
400	EdgeSec.00040008	The customer has not purchased this main resource.	You have not purchased EdgeSec.	Purchase EdgeSec or contact technical support.
400	EdgeSec.00040009	The domain name scope does not match the service scope.	The domain name is not in the region you purchased EdgeSec.	Check the region of the domain name or purchase EdgeSec in the correct region.
400	EdgeSec.00040010	The remaining resources are insufficient.	Insufficient resources.	Expand resources or delete unnecessary resources.
400	EdgeSec.00040011	Please wait until the release is complete.	Resources are being released.	Please wait.

Status Code	Error Codes	Error Message	Description	Solution
400	EdgeSec.00040012	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.	Account restricted. The current product cannot be purchased.	Contact customer service.
400	EdgeSec.00050001	Domain is in processing, please wait it.	The domain name is being scheduled.	Please wait.
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.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.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

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00012003	permission.denied	No permission	Assign WAF required permissions to account
400	WAF.00012004	account.frozen	Account freezing	Account unfreezing
400	WAF.00012005	not.subscribe	Unsubscribed	Subscribe to WAF service first
400	WAF.00012006	pdp.permission.denied	No permission	Check the PDP authority of the account
400	WAF.00012007	jwt.authentication.disabled	JWT certification off	Open JWT certification
400	WAF.00012008	jwt.authentication.invalid.token	Illegal JWT token	Check whether the account has JWT permission
400	WAF.00012009	jwt.authentication.failed	JWT authentication failed	Give the account authorization first
400	WAF.00012010	eps.all.not.support	eps.all.not.support	Open the write permission of enterprise project
400	WAF.00013001	insufficient.quota	Insufficient function quota	Purchase function quota upgrade package
400	WAF.00013002	feature.not.support	Function not supported	nothing
400	WAF.00013003	port.not.support	Port not supported	Port conversion via ELB
400	WAF.00013004	protocol.not.support	Protocol not supported	Through ELB conversion protocol
400	WAF.00013005	wildcard.domain.not.support	Pan domain name not supported	Use specific domain names
400	WAF.00013006	ipv6.not.support	IPv6 is not supported	The current version does not support IPv6

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00013007	insufficient.tenant.quota	insufficient.tenant.quota	Purchase quota upgrade package
400	WAF.00014001	resource.not.found	Resource not found	The resource has been deleted or does not exist
400	WAF.00014002	resource.already.exists	Resource already exists	Resource already exists
400	WAF.00014003	open.protect.failed	Failed to open protection	Check domain name protection status
400	WAF.00014004	access.failed	Failed to access WAF	Modify DNS resolution
400	WAF.00014005	bypass.failed	Bypasswaf failed	Check the protection status and try again
400	WAF.00014006	proxy.config.error	Agent configuration error	Reconfigure the agent correctly and try again
400	WAF.00014007	host.conflict	Domain name conflict	Check that the domain name already exists in the website configuration
400	WAF.00014008	cert.inconsistent	The same domain name, but the certificate is inconsistent	Use the same certificate
400	WAF.00014009	api.not.found	The interface does not exist	Check interface URL
400	WAF.00014010	port.protocol.mismatch	Port and protocol mismatch	Select the matching protocol and port
400	WAF.00014011	host.blacklist	It is forbidden to add the protection website, and the domain name is blacklisted	

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

Status Code	Error Codes	Error Message	Description	Solution
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
400	WAF.00021014	action.illegal	Illegal protective action	It is recommended to configure protection actions according to the enumerated values in the document

Status Code	Error Codes	Error Message	Description	Solution
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
400	WAF.00021020	offsetOrLimit.illegal	Paging parameter error	It is recommended to fill in pagination parameters according to the documents in the help center

Status Code	Error Codes	Error Message	Description	Solution
400	WAF.00021021	param.exceed.limit	Parameter exceeds limit	It is recommended to view the parameter limits according to the documentation in the help center
400	WAF.00022002	resource.already.exists	Resource already exists	It is recommended to check whether the created resource already exists in the console
400	WAF.00022003	resource.is.being.used	The resource is in use	Remove the relationship between the resource and the user before deleting the resource
400	WAF.00022004	rule.conflict	Rule conflict	Check whether the target rule conflicts with the existing rule
401	EdgeSec.00000002	Get Request Attributes Error.	An error occurred when obtaining IAM system parameters.	Contact technical support.
401	EdgeSec.00000003	Get IAM Context Error.	Failed to obtain the IAM context.	Contact technical support.
401	EdgeSec.00000004	Get Token Result Error.	Failed to obtain the IAM token.	Contact technical support.
401	EdgeSec.00000005	Invalid parameters.	Invalid parameter.	Check parameters or contact technical support.
401	EdgeSec.00000020	The project id does not match the token.	The project ID and x-auth-token do not match.	Check the Project ID and x-auth-token.

Status Code	Error Codes	Error Message	Description	Solution
401	EdgeSec.00010001	Failed to get IAM projects.	Failed to obtain the IAM project.	Use the current account to log in to Huawei Cloud and check whether the project exists in IAM. If it does not exist, contact technical support.
401	EdgeSec.00010002	IAM project not ready for WAF.	The current project does not support WAF functions.	Contact technical support.
403	WAF.00022005	insufficient.quota	Insufficient resources	It is recommended to purchase the upgrade package of corresponding resources
404	WAF.00022001	resource.not.found	Resource does not exist	It is recommended to check the resource status on the console or ask for technical support
500	EdgeSec.00000001	An internal error occurs in the system.	Internal service error.	Contact technical support.
500	EdgeSec.00000006	send request fail.	Failed to send the request.	Try again later or contact technical support.
500	EdgeSec.00000010	Service returned nothing.	The returned result is empty.	Try again later or contact technical support.
500	EdgeSec.00000013	Please try again.	Please try again.	Please try again.
500	WAF.00010001	internal.error	Internal error	Contact technical support
500	WAF.00010002	system.busy	Internal error	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	cname.failed	Failed to get OBS file download link	Contact technical support
500	WAF.00020001	internal.error	Service internal exception	It is recommended to try again in five minutes
500	WAF.00020002	system.busy	System busy	It is recommended to try again in five minutes

A.3 Troubleshooting

A.3.1 EdgeSec.00000005 Invalid Parameter

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

- The page is not refreshed for a long time.
- Invalid input

Solution

Step 1 Refresh the page. Then, select a proper time range and try again.

Step 2 Enter information about the edge WAF policy or rule as prompted.

----End

A.3.2 EdgeSec.00000013 Concurrent Modification Exception

Root Cause

This error code is triggered when too many concurrent access requests are performed on APIs.

Troubleshooting and Solution

<table>
<tr><th colspan="2">Event Scenario</th><th>Cause</th><th>Check Items</th><th>Solution</th></tr>
<tr><td rowspan="8">Creating an edge WAF policy rule</td><td>Adding a CC attack protection rule</td><td rowspan="13">This error code is triggered when there are a large number of concurrent requests performed on APIs.</td><td rowspan="8">Whether concurrent requests are performed on the console.</td><td rowspan="8">Retry on the console.</td></tr>
<tr><td>Adding a precise protection rule</td></tr>
<tr><td>Creating a geolocation access control rule</td></tr>
<tr><td>Creating a global whitelist rule</td></tr>
<tr><td>Adding a data masking rule</td><td rowspan="5">Check whether users concurrently invoke related APIs.</td><td rowspan="5">Reduce the concurrency of invoking related APIs.</td></tr>
<tr><td>Adding an IP address blacklist or whitelist rule</td></tr>
<tr><td>Creating a reference table rule</td></tr>
<tr><td colspan="2">Creating an edge WAF certificate</td></tr>
<tr><td colspan="2">Creating an edge WAF address group</td></tr>
</table>

A.3.3 EdgeSec.00000014 Only Default Enterprise Project Supported (Not support operation in this enterprise project)

Root Cause

Currently, EdgeSec can be purchased only in the default enterprise project. If you add a domain name to edge WAF or edge DDoS in other enterprise projects, this error will be reported.

Solution

- Console: Switch to the default enterprise project and add a domain name again.

- API: When calling the API for adding a domain name to WAF, change the value of **enterprise_project_id** to **0** (default enterprise project).

A.3.4 EdgeSec.00000015 Write Operation Not Supported When All Enterprise Projects Are Selected (All enterprise projects do not support the write operation)

Root Cause

This error is reported when a user selected **All projects** for **Enterprise Project** and attempted to add a domain name to edge WAF or edge Anti-DDoS. When **All projects** is selected for **Enterprise Project**, only query is supported.

Solution

- Console: Switch to the default enterprise project and add a domain name again.
- API: When calling the API for adding a domain name to WAF, change the value of **enterprise_project_id** to **0** (default enterprise project).

A.3.5 EdgeSec.00000018 Migration of Resources to Non-Default Enterprise Project Not Supported (This version only supports default enterprise project)

Root Cause

Currently, EdgeSec can be purchased only in the default enterprise project. Resources cannot be migrated to a non-default enterprise project.

Troubleshooting and Solution

Event Scenario	Cause	Solution
An error was reported when a user attempted to migrate resources to a non-default enterprise project on the EPS console.	The current edition of EdgeSec does not support non-default enterprise projects.	The current edition does not support this operation. You can upgrade your edition and try again.

A.3.6 EdgeSec.00000019 Frozen Resources Cannot Be Migrated to or from an Enterprise Project (frozen cannot create eps tag)

Root Cause

Frozen resources cannot be added to or removed from an enterprise project.

Troubleshooting Methods

Check whether the resource is frozen.

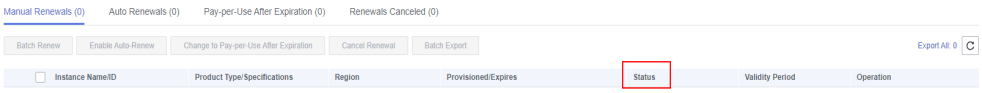
Procedure

Step 1 Log in to the management console.

Step 2 In the upper right corner of the page, choose **Billing & Costs** > **Renewal**. The **Renewals** page is displayed.

Step 3 Check the status of the resource.

Figure A-1 Resource status



----End

Solution

The current version supports only default enterprise project. Migrations to or from other enterprise projects are not supported.

NOTE

Note: The later version will support custom enterprise projects. You can migrate renewed resources between enterprise projects then.

A.3.7 EdgeSec.00000023 Operation Not Supported by the Current Specifications (Current specification does not support this option)

Root Cause

This error is reported when the specifications in-use do not support some operations.

Troubleshooting Methods

For details, see **Service Edition Differences**.

Solution

Upgrade the service to the edition that supports the operation.

A.3.8 EdgeSec.00000025 Invalid Block Time (Invalid block time)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

When adding or modifying a protection rule for an edge WAF, enter the block time as instructed.

Solution

Refresh the page and enter a valid block time for the edge WAF protection rule.

A.3.9 EdgeSec.00000026 Invalid Whitelist Rule Type (Invalid rule type)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

Check the condition length.

Solution

Refresh the page and enter the whitelist rule type as instructed.

A.3.10 EdgeSec.00000027 Invalid CC Rule Condition Length (Invalid cc condition length value)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

Check the condition length.

Solution

Refresh the page and enter the length as prompted.

A.3.11 EdgeSec.00010001 Invalid IAM Service Project (Failed to get IAM projects)

Root Cause

This error was reported when an IAM project is abnormal.

Troubleshooting Methods

Check the IAM projects.

Solution

Step 1 **Log in to the management console.**

Step 2 Hover your mouse over ☰ in the upper left corner of the page and choose **Management & Governance** > **Identity Access and Management**.

Step 3 In the navigation pane on the left, choose **Projects** and view the region to which the project belongs.

- If you have registered with the Huawei Cloud International website, there should be a project in the **AP-Singapore** region.
- If you have registered with the Huawei Cloud Chinese Mainland website, there should be a project in the **CN North-Beijing4** region.

NOTE

If there is no such a project, **Submit a Service Ticket** enables the project in the region.

----End

A.3.12 EdgeSec.00010005 Insufficient WAF Policy Rule Quota (WAF policy rule quota is not enough)

Root Cause

The edge WAF policy rule quota is insufficient.

Troubleshooting Methods

For details about how to view the policy rule quota of each edition, see **Edition Description**.

Solution

Scenario	Solution
The edition with the largest quota can meet the requirements.	Upgrade the service edition to the required edition.
	If the quota of IP address blacklist and whitelist rules is insufficient, you can upgrade the service edition, or purchase the rule expansion package of edge WAF.
The edition with the largest quota still fails to meet the requirements.	**Submit a service ticket**.

A.3.13 EdgeSec.00010006 Blacklist and Whitelist Rules of Edge WAF Exceed the Quota

Root Cause

Blacklist and whitelist rules of an edge WAF policy exceed the quota.

Troubleshooting Methods

Step 1 **Viewing Blacklist and Whitelist Rule Quotas**

Step 2 Check whether there are protection policies in which the number of blacklist and whitelist rules exceeds the current quota.

----End

Viewing Blacklist and Whitelist Rule Quotas

Step 1 **Log in to the management console.**

Step 2 Click  in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

Step 3 Click **Edge WAF** in the upper right corner of the page to view the current rule quota.

Figure A-2 Rule Quota

NOTE

Rule quota shows an example. If the rule quota is 1010, the blacklist and whitelist rule quota for a single protection policy is 1010.

----End

Solution

Scenario	Solution
Some blacklist and whitelist rules can be deleted.	Delete unnecessary blacklist and whitelist rules so that the number of blacklist and whitelist rules in each policy does not exceed the current quota.
Existing blacklist and whitelist rules cannot be deleted.	Upgrade the edition or purchase a rule expansion package to ensure that the number of blacklist and whitelist rules in each policy does not exceed the new quota. Blacklist and whitelist rule quota = Edition quota + Number of rule expansion packages x 10. For example, if you use the professional edition of edge WAF and have two rule expansion packages, you can create 120 blacklist and whitelist rules (100 + 2 x 10 = 120). **NOTE** • For details about the blacklist and whitelist rule quotas of each edition, see **Edition Description**. • A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.

A.3.14 EdgeSec.00010007 Insufficient IP Address Group Quota of Edge WAF

Root Cause

The IP address group quota of edge WAF is insufficient.

Troubleshooting Methods

For details about how to view the IP address group quota, see **Specifications Restrictions**

Solution

If the IP address group quota is insufficient, contact technical support.

A.3.15 EdgeSec.00010008 Insufficient Edge WAF Certificate Quota

Root Cause

The edge WAF certificate quota is insufficient.

Troubleshooting Methods

View the domain name quota of edge WAF.

NOTE

The certificate quota is the same as the domain name quota.

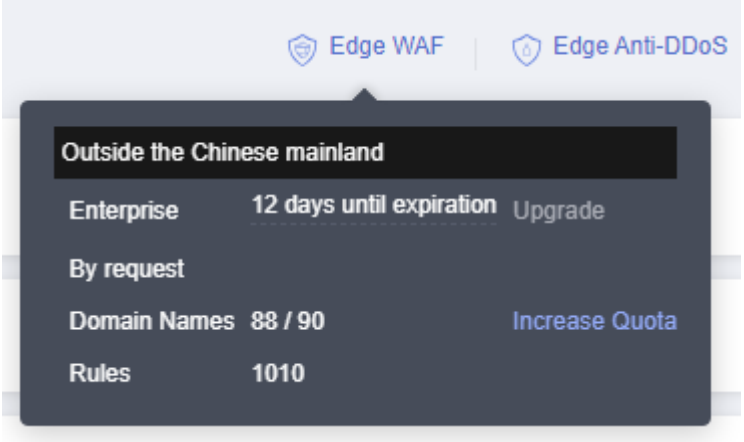
Viewing Domain Quotas

Step 1 **Log in to the management console.**

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

Step 3 Click **Edge WAF** in the upper right corner of the page to view the current domain name quota.

Figure A-3 Domain name quota



NOTE

Certificate quota = Domain name quota. For example, if the domain name quota is 90, the certificate quota is 90, as shown in **Domain name quota**.

----End

Solution

Purchase the domain name expansion package of the edge WAF.

A.3.16 EdgeSec.00030001 Invalid DDoS Overview Parameters (Illegal Elasticsearch Request)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

Check the parameters on the query page.

Solution

Refresh the page. Then, select a proper time range, specify other parameters, and try again.

A.3.17 EdgeSec.00030003 DDoS Overview Query Type Exception (Statistic Type Error)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

Check the parameters on the query page.

Solution

Refresh the page. Then, select a proper time range, specify other parameters, and try again.

A.3.18 EdgeSec.00030002 DDoS Overview Query Type Exception (Search Error)

Root Cause

This error was reported when a user entered an invalid parameter for using some functions on the console.

Troubleshooting Methods

Check the parameters on the query page.

Solution

Refresh the page. Then, select a proper time range, specify other parameters, and try again.

A.3.19 EdgeSec.00040007 No Permission To Operate

Root Cause

This error was reported when the operation permission is insufficient.

Troubleshooting and Solution

Event Scenario	Sub-Scenario	Cause	Solution
Adding, modifying, and deleting operations	Edge WAF	Edge WAF resources are frozen.	Renew the affected resources.
	Edge Anti-DDoS	• No edge Anti-DDoS resources are purchased. • Edge Anti-DDoS resources are frozen.	Buy or renew edge Anti-DDoS resources.
Viewing operation	Edge Anti-DDoS	No edge Anti-DDoS resources are purchased.	Buy edge Anti-DDoS.

A.3.20 EdgeSec.00040013 Insufficient Top-Level Domain Name Quota (The remaining first level domain resources are insufficient)

Root Cause

This error was reported when the top-level domain name quota in edge WAF was insufficient.

Troubleshooting Methods

1. Learn the top-level domain name quota specified in each EdgeSec edition. For details, see **Specification Limitations**.
2. **Viewing Top-Level Domain Name Quotas**

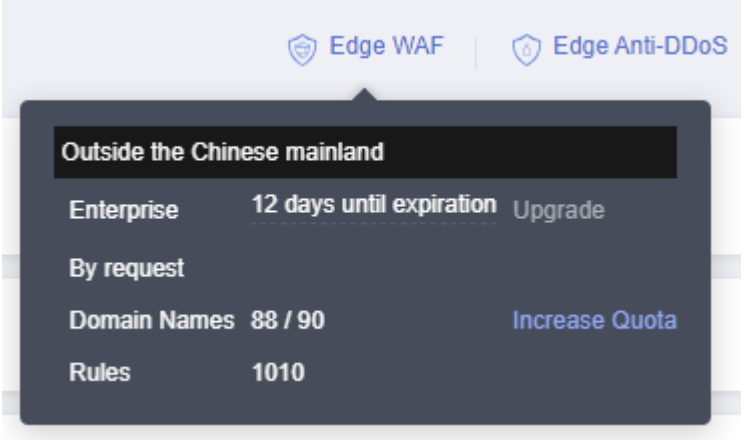
Viewing Top-Level Domain Name Quotas

Step 1 **Log in to the management console.**

Step 2 Click ☰ in the upper left corner of the page and choose **Security & Compliance** > **Edge Security**.

Step 3 Click **Edge WAF** in the upper right corner of the page to view the current domain name quota.

Figure A-4 Domain name quota



NOTE

First-level domain name quota = Domain name quota/10. For example, if the domain name quota is 90, as shown in **Figure A-4**, the top-level domain name quota is 9.

----End

Solution

Scenario	Method
The enterprise edition edge WAF is in use.	Buy a domain name expansion package. **NOTE** Each domain name expansion package contains a top-level domain name.
The basic or professional edition edge WAF is in use.	Upgrade the edition or buy a domain name expansion package. **NOTE** • For details about the top-level domain name quota, see **Edition Description**. • Each domain name expansion package contains a top-level domain name.

A.3.21 EdgeSec.00040014 Expansion Resource Quota Has Been Used (The extended quota has been used)

Root Cause

This error was generated when expansion resource quotas were in use while the user attempt to unsubscribe from expansion packages they have.

Troubleshooting and Solution

Event Scenario	Cause	Solution
A user attempts to unsubscribe from an edge WAF domain name expansion package.	The number of domain names or rules used by the user has exceeded the quota provided by the edition.	Check the used edge WAF domain names or rules, delete the ones not in use, and keep their quantity within the specifications supported by the service edition in use. **NOTE** For details about how to view the policy rule quota of each edition, see **Edition Description**.
A user attempts to unsubscribe from an edge WAF rule expansion package.		

A.3.22 WAF.00022002 Resource Already Exists (Domain Already Exists)

Root Cause

This error was reported when there are edge WAF resources in the system while a user attempted to create the same ones.

Troubleshooting Methods

Scenario	Cause
Adding or modifying an edge WAF blacklist/ whitelist rule	There is a blacklist or whitelist rule with the same name.
	There is a blacklist or whitelist rule with the same IP addresses listed.
Adding or modifying an edge WAF data masking rule	Duplicate combination of the path, masked fields, and masked field name.

Solution

A rule cannot be added repeatedly. Modify the rule parameters.

A.3.23 WAF.00014002 Resource Already Exists

Root Cause

This error was reported when there are edge WAF resources in the system while a user attempted to create the same ones.

Troubleshooting Methods

Scenario	Cause
Adding an address group	There is already an address group with the same name.

Solution

Do not use an existing address group name when adding an address group.

A.3.24 common.01010003 No Purchase Permission

Root Cause

The current account does not have the purchase permission.

Solution

Event Scenario	Solution
• An IAM user attempts to purchase resources. • An IAM user attempts to change resources.	• Add the IAM user to the admin user group. • Add the IAM user to the group having the EdgeSec_FullAccess Permission. • Use the account that is used to create the IAM user.

A.4 Obtaining a Project ID

Obtaining a Project ID by Calling an API

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

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

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

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

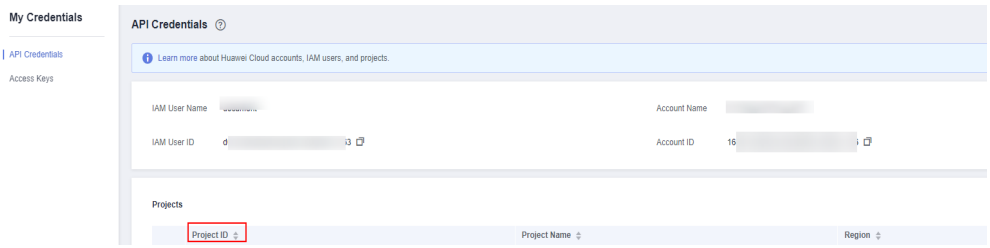
Obtaining a Project ID from the Console

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

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

3. On the page, view the project ID in the project list.

Figure A-5 Viewing project IDs



B Change History

Released On	Description
2023-11-24	This is the second official release. Added: • Certificate management APIs: – Query the certificate list. – Create a certificate. – Query a certificate. – Delete a certificate. – Modify a certificate. • **Troubleshooting**
2023-08-18	This is the first official release.

