

**Edge Security**

# **API Reference**

**Issue**            03  
**Date**             2024-10-31



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

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

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

## **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

---

<b>1 Before You Start.....</b>	<b>1</b>
1.1 Overview.....	1
1.2 API Calling.....	1
1.3 Endpoints.....	1
1.4 Concepts.....	1
<b>2 API Overview.....</b>	<b>3</b>
<b>3 API Calling.....</b>	<b>4</b>
3.1 Making an API Request.....	4
3.2 Authentication.....	7
3.3 Returned Values.....	8
<b>4 API.....</b>	<b>10</b>
4.1 Protected Domain Name Management.....	10
4.1.1 Querying the Protected Domain Name List.....	10
4.1.2 Creating a Domain Name.....	13
4.1.3 Querying Details About a Protected Domain Name.....	15
4.1.4 Updating Protected Domain Names.....	18
4.1.5 Deleting a Protected Domain Name.....	20
<b>A Appendix.....</b>	<b>23</b>
A.1 Status Code.....	23
A.2 Error Codes.....	23
A.3 Troubleshooting.....	37
A.3.1 EdgeSec.00000005 Invalid Parameter.....	37
A.3.2 EdgeSec.00000013 Concurrent Modification Exception.....	37
A.3.3 EdgeSec.00000014 Only Default Enterprise Project Supported (Not support operation in this enterprise project).....	38
A.3.4 EdgeSec.00000015 Write Operation Not Supported When All Enterprise Projects Are Selected (All enterprise projects do not support the write operation).....	39
A.3.5 EdgeSec.00000018 Migration of Resources to Non-Default Enterprise Project Not Supported (This version only supports default enterprise project).....	39
A.3.6 EdgeSec.00000019 Frozen Resources Cannot Be Migrated to or from an Enterprise Project (frozen cannot create eps tag).....	40
A.3.7 EdgeSec.00000023 Operation Not Supported by the Current Specifications.....	40
A.3.8 EdgeSec.00000025 Invalid Block Time (Invalid block time).....	41

A.3.9 EdgeSec.00000026 Invalid Whitelist Rule Type (Invalid rule type).....	41
A.3.10 EdgeSec.00000027 Invalid CC Rule Condition Length (Invalid cc condition length value).....	41
A.3.11 EdgeSec.00010001 Invalid IAM Service Project (Failed to get IAM projects).....	42
A.3.12 EdgeSec.00010005 Insufficient WAF Policy Rule Quota.....	42
A.3.13 EdgeSec.00010006 Blacklist and Whitelist Rules of Edge WAF Exceed the Quota.....	43
A.3.14 EdgeSec.00010007 Insufficient IP Address Group Quota of Edge WAF.....	44
A.3.15 EdgeSec.00010008 Insufficient Edge WAF Certificate Quota.....	44
A.3.16 EdgeSec.00030001 Invalid DDoS Overview Parameters (Illegal Elasticsearch Request).....	45
A.3.17 EdgeSec.00030003 DDoS Overview Query Type Exception (Statistic Type Error).....	46
A.3.18 EdgeSec.00030002 DDoS Overview Query Type Exception (Search Error).....	46
A.3.19 EdgeSec.00040007 No Permission To Operate.....	46
A.3.20 EdgeSec.00040013 Insufficient Top-Level Domain Name Quota.....	47
A.3.21 EdgeSec.00040014 Expansion Resource Quota Has Been Used.....	48
A.3.22 WAF.00022002 Resource Already Exists (Domain Already Exists).....	49
A.3.23 WAF.00014002 Resource Already Exists.....	49
A.3.24 common.01010003 No Purchase Permission.....	50
A.4 Obtaining a Project ID.....	50

# 1 Before You Start

---

## 1.1 Overview

EdgeSec (Edge Security) is a security protection service built on edge nodes.

ESA (Edge Security Acceleration) is a sub-product of EdgeSec. It provides cache acceleration and application security protection and supports multiple security functions, such as web attack defense, DDoS attack defense, and CC attack defense. ESA comprehensively improves the security protection capability of the acceleration network and ensures high-quality user experience and service security.

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, and allows you to make API calls over HTTPS.

For details about how to call APIs, see [API Calling](#).

## 1.3 Endpoints

An endpoint is the **request address** for calling an API.

Endpoints vary depending on services and endpoints. 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.

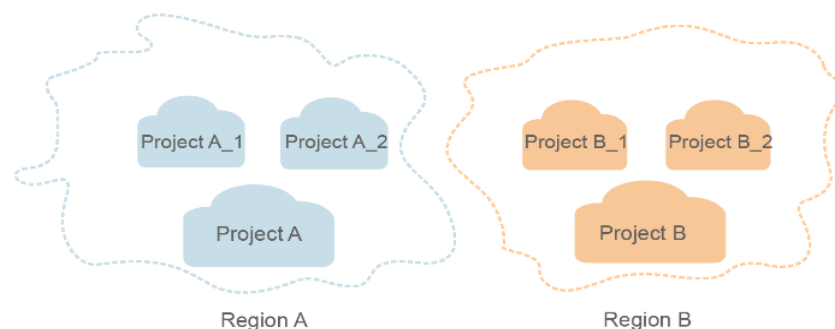
- Availability Zone (AZ)

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

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

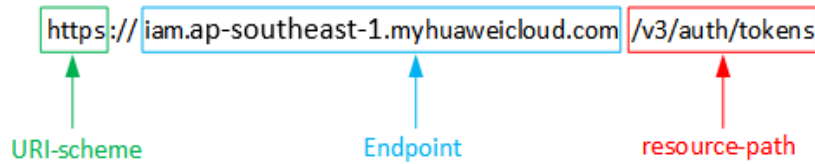
For example, to obtain an IAM token in the **CN-Hong Kong** region, obtain the endpoint of IAM (**iam.ap-southeast-1.myhuaweicloud.com**) for this region and



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 **xxxxxxxxxxxxxxxxxxxx** 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": "xxxxxxxxxxxxxxxxxxxx"
      }
    }
  }
}
```

```
}  
}
```

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": "xxxxxxxxx"  
    }  
  }  
}
```

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

```
connection → keep-alive
content-type → application/json
date → Tue, 12 Feb 2019 06:52:13 GMT
server → Web Server
strict-transport-security → max-age=31536000; includeSubdomains;
transfer-encoding → chunked
via → proxy A
x-content-type-options → nosniff
x-download-options → noopen
x-frame-options → SAMEORIGIN
x-iam-trace-id → 218d45ab-d674-4995-af3a-2d0255ba41b5
x-subject-token → MIIVXQYJKoZIhvcNAQcCoIIYTCCEGoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOensiZXhwaXJlc19hdCI6IjwMTktMDItMTNUMC
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkajACgkIQ01wi4JIGzrpd18LGXK5bdfq4lqHCYb8P4NaYONYeJcAgzVefYtLWT1GSO0zxKZmlQHq82HBqHdgIZO9fuEeL5dMhdavj+33wEI
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jggIFkNPQuFSOU8+uSsttVwRtnfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUUVhVpxk8pxiX1wTEboX-
RzT6MUbvpGw-oPNFYxJECKnoH3HRozv0vN--n5d6Nbxg==
x-xss-protection → 1; mode=block;
```

## (Optional) Response Body

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

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

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

```

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 Protected Domain Name Management

### 4.1.1 Querying the Protected Domain Name List

#### Function

Queries the protection domain name list.

#### URI

GET <https://esa.cn-north-4.myhuaweicloud.com/v1/edgesec/configuration/domains>

**Table 4-1** Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Query offset.
limit	No	Integer	Number of records on each page of the query list.
domain_name	No	String	Domain name.
policy_name	No	String	Policy name.
enterprise_project_id	No	String	Enterprise project ID.

## Request Parameters

**Table 4-2** Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Tenant token.

## Response Parameters

**Status code: 200**

**Table 4-3** Response body parameters

Parameter	Type	Description
total	Long	Total number of protected domain names.
domain_used_quota	Long	Used domain name quota.
domain_list	Array of <a href="#">DomainInfo</a> objects	Details about a protected domain name.

**Table 4-4** DomainInfo

Parameter	Type	Description
id	String	Domain name ID.
domain_name	String	Domain name.
enterprise_project_id	String	Enterprise project ID.
dispatch_statuses	String	Status <ul style="list-style-type: none"><li>• Scheduling exception: dispatch_abnormal</li><li>• Unscheduled: un_dispatch</li><li>• Scheduling: dispatching</li><li>• Scheduled: dispatched</li><li>• Deleting: dispatch_deleting</li></ul>
web_name	String	Website name.
description	String	Description
policy_id	String	Policy ID.

Parameter	Type	Description
protect_status	String	Protection status: <ul style="list-style-type: none"><li>• Protected: on</li><li>• Not protected: off</li></ul>
create_time	Long	Time when the domain name is created.
update_time	Long	Time when the domain name is updated.

**Status code: 400****Table 4-5** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

**Status code: 401****Table 4-6** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

**Status code: 500****Table 4-7** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.



Parameter	Type	Description
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

## Example Requests

None

## Example Responses

None

## Status Codes

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

## Error Codes

See [Error Codes](#).

## 4.1.2 Creating a Domain Name

### Function

This API is used to create a protected domain name.

### URI

POST <https://esa.cn-north-4.myhuaweicloud.com/v1/edgesec/configuration/domains>

### Request Parameters

**Table 4-8** Request header parameters

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

**Table 4-9** Request body parameters

Parameter	Mandatory	Type	Description
domain_name	Yes	String	Protected domain name (port allowed).
enterprise_project_id	Yes	String	Enterprise project ID.
policy_id	No	String	ID of the policy associated with the protected domain name.
description	No	String	Domain name description.

## Response Parameters

**Status code: 400**

**Table 4-10** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

**Status code: 401**

**Table 4-11** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

**Status code: 500**

**Table 4-12** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

## Example Requests

None

## Example Responses

None

## Status Codes

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

## Error Codes

See [Error Codes](#).

## 4.1.3 Querying Details About a Protected Domain Name

### Function

This API is used to query a protected domain name.

### URI

GET [https://esa.cn-north-4.myhuaweicloud.com/v1/edgesec/configuration/domains/{domain\\_id}](https://esa.cn-north-4.myhuaweicloud.com/v1/edgesec/configuration/domains/{domain_id})

**Table 4-13** Path Parameters

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

## Request Parameters

**Table 4-14** Request header parameters

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

## Response Parameters

**Status code: 200**

**Table 4-15** Response body parameters

Parameter	Type	Description
id	String	Domain name ID.
domain_name	String	Domain name.
enterprise_project_id	String	Enterprise project ID.
description	String	Domain name description.
policy_id	String	Policy ID.
protect_status	String	Protection status: <ul style="list-style-type: none"><li>Protected: on</li><li>Not protected: off</li></ul>
create_time	Long	Time when the domain name is created.
update_time	Long	Time when the domain name is updated.

**Status code: 400**

**Table 4-16** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code

Parameter	Type	Description
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

**Status code: 401****Table 4-17** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

**Status code: 500****Table 4-18** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

**Example Requests**

None

**Example Responses**

None

## Status Codes

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

## Error Codes

See [Error Codes](#).

### 4.1.4 Updating Protected Domain Names

#### Function

This API is used to update protected domain names.

#### URI

PUT [https://esa.cn-north-4.myhuaweicloud.com/v1/edgesec/configuration/domains/{domain\\_id}](https://esa.cn-north-4.myhuaweicloud.com/v1/edgesec/configuration/domains/{domain_id})

**Table 4-19** Path Parameters

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Domain name.

#### Request Parameters

**Table 4-20** Request header parameters

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

**Table 4-21** Request body parameters

Parameter	Mandatory	Type	Description
protect_status	No	String	Protection status. The value can be on (protected) or off (unprotected).
description	No	String	Domain name description.

## Response Parameters

### Status code: 400

**Table 4-22** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

### Status code: 401

**Table 4-23** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

### Status code: 500

**Table 4-24** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.

Parameter	Type	Description
encoded_authorized_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

## Example Requests

None

## Example Responses

None

## Status Codes

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

## Error Codes

See [Error Codes](#).

## 4.1.5 Deleting a Protected Domain Name

### Function

This API is used to delete a protected domain name.

### URI

DELETE [https://esa.cn-north-4.myhuaweicloud.com/v1/edgesec/configuration/domains/{domain\\_id}](https://esa.cn-north-4.myhuaweicloud.com/v1/edgesec/configuration/domains/{domain_id})

**Table 4-25** Path Parameters

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



**Table 4-26** Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID.

## Request Parameters

**Table 4-27** Request header parameters

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

## Response Parameters

### Status code: 400

**Table 4-28** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

### Status code: 401

**Table 4-29** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

### Status code: 500

**Table 4-30** Response body parameters

Parameter	Type	Description
error_code	String	Standard error code: service name.8-digit code
error_msg	String	Detailed error information.
encoded_authentication_message	String	If the service is integrated with IAM5.0, an IAM response must be returned when access is denied.

## Example Requests

None

## Example Responses

None

## Status Codes

Status Code	Description
200	No Content
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 <a href="https://support.huaweicloud.com/en-us/usermanual-edgesecc/edgesecc_01_0058.html#section1">https://support.huaweicloud.com/en-us/usermanual-edgesecc/edgesecc_01_0058.html#section1</a> . 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.0003 0003	Statistic Type Error.	An error occurred when querying the protected data type.	Check the protected data type.
400	EdgeSec.0004 0004	The customer has purchased this product.	You have purchased the product.	Cancel purchase or contact technical support.
400	EdgeSec.0004 0007	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.0004 0008	The customer has not purchased this main resource.	You have not purchased EdgeSec.	Purchase EdgeSec or contact technical support.
400	EdgeSec.0004 0009	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.0004 0010	The remaining resources are insufficient.	Insufficient resources.	Expand resources or delete unnecessary resources.
400	EdgeSec.0004 0011	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.protection.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.configuration.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.0001401 2	insufficient.tenant.quota	Insufficient tenant quota	Purchase quota upgrade package
400	WAF.0001401 3	exclusive.ip.config.error	Exclusive IP configuration error	Check exclusive IP configuration
400	WAF.0001401 4	exclusive.ip.config.error	exclusive.ip.config.error	Check exclusive IP configuration
400	WAF.0002100 2	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.0002100 3	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.0002100 4	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.0002100 5	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.0002100 6	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

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

### A.3.3 EdgeSec.0000014 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

Instance Name/ID	Product Type/Specifications	Region	Provisioned/Expires	Status	Validity Period	Operation

----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

### Root Cause

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

### Troubleshooting Methods

Check the operation permissions of each edition.

### 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

### Root Cause

The edge WAF policy rule quota is insufficient.

### Troubleshooting Methods

Check the policy rule quota of each edition.

### 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.

Scenario	Solution
The edition with the largest quota still fails to meet the requirements.	<a href="#">Submit a service ticket.</a>

## 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

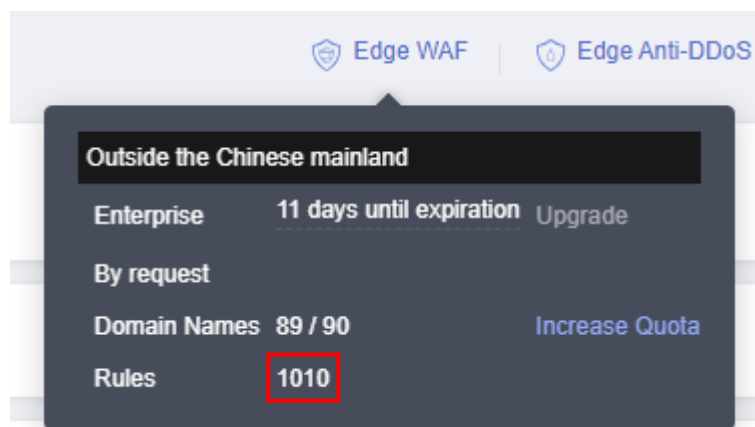
### Viewing Blacklist and Whitelist Rule Quotas

**Step 1** [Log in to the management console.](#)

**Step 2** Click  in the upper left corner of the page and choose **Content Delivery & Edge Computing > CDN and 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).  <b>NOTE</b> 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 **Content Delivery & Edge Computing > CDN and 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	<ul style="list-style-type: none"><li>No edge Anti-DDoS resources are purchased.</li><li>Edge Anti-DDoS resources are frozen.</li></ul>	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

#### 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 **Content Delivery & Edge Computing > CDN and 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. <b>NOTE</b> 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. <b>NOTE</b> Each domain name expansion package contains a top-level domain name.

**A.3.21 EdgeSec.00040014 Expansion Resource 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.
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
<ul style="list-style-type: none"><li>An IAM user attempts to purchase resources.</li><li>An IAM user attempts to change resources.</li></ul>	<ul style="list-style-type: none"><li>Add the IAM user to the admin user group.</li><li>Add the IAM user to the group having the EdgeSec_FullAccess Permission.</li><li>Use the account that is used to create the IAM user.</li></ul>

## A.4 Obtaining a Project ID

### Obtaining a Project ID by Calling an API

You can obtain the project ID by calling the API for [Querying Project Information Based on 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": "xxxxxxx",
      "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

