

**CodeArts**

# **API Reference**

**Issue**            01  
**Date**             2026-05-25



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. 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>
<b>2 API Overview</b>	<b>3</b>
<b>3 Calling APIs</b>	<b>4</b>
3.1 Making an API Request	4
3.2 Authentication	7
3.3 Response	9
<b>4 API</b>	<b>11</b>
4.1 VPC endpoint management	11
4.1.1 Deleting VPC Endpoint Access Control Information	11
4.1.2 Obtaining List of VPC Endpoints Authorized by a Tenant	16
<b>5 Permissions and Supported Actions</b>	<b>24</b>
5.1 Permissions and Supported Actions	24
<b>6 Appendix</b>	<b>25</b>
6.1 Status Codes	25
6.2 Error Codes	28
6.3 Obtaining a Project ID	34
6.3.1 Obtaining an IAM Project ID	34
6.3.2 Obtaining a CodeArts Project ID	35
6.4 Obtaining an Account ID	36
<b>7 Change History</b>	<b>37</b>

# 1 Before You Start

Welcome to CodeArts. CodeArts is a one-stop platform that provides out-of-the-box cloud services for requirement delivery, code commit, check, build, verification, deployment, and release throughout the entire software lifecycle.

This document describes how to use APIs to manage VPCEP information for CodeArts access control. For details, see [API Overview](#).

Before calling an API, you must be familiar with CodeArts concepts. For details, see [Service Overview](#).

## Endpoints

An endpoint is the request address for calling an API. Endpoints vary depending on services and regions.

The following table lists CodeArts endpoints. Select a desired one based on the service requirements.

**Table 1-1** CodeArts endpoints

Region	ID	Endpoint
AF-Cairo	af-north-1	codearts-devuc.af-north-1.myhuaweicloud.com
AF-Johannesburg	af-south-1	codearts-devuc.af-south-1.myhuaweicloud.com
AP-Singapore	ap-southeast-3	codearts-devuc.ap-southeast-3.myhuaweicloud.com
LA-Mexico City2	la-north-2	codearts-devuc.la-north-2.myhuaweicloud.com
LA-Santiago	la-south-2	codearts-devuc.la-south-2.myhuaweicloud.com
ME-Riyadh	me-east-1	codearts-devuc.me-east-1.myhuaweicloud.com

Region	ID	Endpoint
LA-Sao Paulo1	sa-brazil-1	codearts-devuc.sa-brazil-1.myhuaweicloud.com
TR-Istanbul	tr-west-1	codearts-devuc.tr-west-1.myhuaweicloud.com

## Concepts

- Account

The account has full access permissions for all of its cloud services and resources via Huawei Cloud registration. 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 IAM users and grant them permissions for routine management.
- User

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

An IAM user can view the account ID and user ID on the [My Credentials](#) page of the console. The account name, username, and password will be required for API authentication.
- 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 into universal regions and dedicated regions.

  - A universal region provides universal cloud services for common tenants.
  - A dedicated region provides particular services for specific tenants.

For details, see [Region and AZ](#).
- AZ

An availability zone (AZ) contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to support cross-AZ high-availability (HA) systems.

# 2 API Overview

---

**Table 2-1** API Overview

Type	API Description
VpcepManager	APIs for managing VPCEP.

# 3 Calling APIs

## 3.1 Making an API Request

This section describes the structure of a RESTful API request, and uses the IAM API for [creating an IAM user](#) as an example to describe how to call an API.

### Request URI

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

A request URI is in the following format: *{URI-scheme}://{Endpoint}/{resource-path}?{query-string}*

The following table describes the parameters.

Parameter	Description
URI-scheme	Protocol used to transmit requests. All APIs use <b>HTTPS</b> .
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 <a href="#">Regions and Endpoints</a> .  For example, the endpoint of IAM in the <b>AP-Singapore</b> region is <b>iam.ap-southeast-3.myhuaweicloud.com</b> .
resource-path	Access path of an API for performing a specified operation. Obtain the path from the URI module of an API. For example, the value of <b>resource-path</b> for the API used to create an IAM user is <b>/v3.0/OS-USER/users</b> .
query-string	(Optional) Query parameter. Ensure that a question mark (?) is included in front of each query parameter that is in the format of <i>Parameter name=Parameter value</i> . For example, <b>limit=10</b> indicates that a maximum of 10 data records will be queried.

You can use the endpoint of any region to create an IAM user as IAM is a global service. For example, the endpoint (`iam.ap-southeast-3.myhuaweicloud.com`) of AP-Singapore . You can find the resource-path (`/v3.0/OS-USER/users`) in the URI of the API used by referring to [Creating an IAM User by Administrator](#). Then, construct the URI as follows:

```
https://iam.ap-southeast-3.myhuaweicloud.com/v3.0/OS-USER/users
```

**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.

Request Method	Description
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 [create an IAM user](#), the request method is **POST**. The request is as follows:

```
POST https://iam.ap-southeast-3.myhuaweicloud.com/v3.0/OS-USER/users
```

## 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 are provided for specific APIs, if any.
- **Authorization**: provides signature authentication information. This field is optional. When AK/SK authentication is enabled, this field is automatically specified for signing the request with SDK. For more information, see [AK/SK-based Authentication](#).
- **X-Sdk-Date**: specifies the time when a request is sent. This field is optional. When AK/SK authentication is enabled, this field is automatically specified for signing the request with SDK. For more information, see [AK/SK-based Authentication](#).
- **X-Auth-Token**: specifies a user token. This field is mandatory only when token-based API authentication is used. 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.
- **X-Project-ID**: specifies a subproject ID. This parameter is optional. It is used in multi-project scenarios. The **X-Project-ID** field is mandatory in the request header for accessing resources in a sub-project through AK/SK-based authentication.
- **X-Domain-ID**: specifies the account ID, which is optional. When you call APIs of global services using AK/SK-based authentication, **X-Domain-ID** needs to be configured in the request header.

For the API for [creating an IAM user as an administrator](#), if AK/SK-based authentication is enabled, the request with the header is as follows:

```
POST https://iam.ap-southeast-3.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=*****, SignedHeaders=content-type;host;x-sdk-date,
Signature=*****
```

## Request Body

A request body is often sent in a structured format defined by the request header field **Content-Type** and transfers information except the request header. If the request body contains Chinese characters, set **Content-type** to **utf-8**, for example, **Content-Type: application/json; charset=utf-8**.

Request bodies vary with APIs. Some APIs do not require a request body, such as the APIs using **GET** and **DELETE** methods.

For the API used to [create an IAM user](#), you can check the required request parameters and their description in the API request. The following provides an example request with a body included. Replace the bold fields with the actual values.

- **accountid** indicates the ID of the account to which the IAM user belongs.
- **username** indicates the username of the IAM user to be created.
- **email** indicates the email address of the IAM user.
- **\*\*\*\*\*** indicates the login password of the IAM user.

```
POST https://iam.ap-southeast-3.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Sdk-Date: 20240416T095341Z
Authorization: SDK-HMAC-SHA256 Access=*****, SignedHeaders=content-type;host;x-sdk-date,
Signature=*****

{
  "user": {
    "domain_id": "accountid",
    "name": "username",
    "password": "*****",
    "email": "email",
    "description": "IAM User Description"
  }
}
```

If all data required for the API request is available, you can send the request to call the API through curl, Postman, or coding.

## 3.2 Authentication

You can use either of the following authentication methods when calling APIs:

- AK/SK-based authentication: Requests are encrypted using an Access Key ID/ Secret Access Key (AK/SK) pair.
- Token-based authentication. General requests are authenticated using tokens.

### AK/SK-based Authentication

AK/SK-based authentication uses AK/SK to sign requests, and the signature is then added to request headers for authentication.

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

In AK/SK-based authentication, you can sign requests either using an AK/SK pair based on the signature algorithm or using the signing SDK. For details about how to sign requests and use the signing SDK, see [AK/SK Signing and Authentication Guide](#).

---

#### NOTICE

Unlike the SDKs provided by services, the signing SDK is only used for signing requests.

---

#### Constraints

- AK/SK-based authentication supports API requests with a body no larger than 12 MB. For API requests with a larger body, you should use token-based authentication.
- You can use the AK/SK in either a permanent or temporary access key. If you are using a temporary access key, you must configure the **X-Security-Token** field whose value is the **security\_token** of the temporary access key.
- API Gateway checks the time format and compares the request time with the time when API Gateway received the request. If the time difference exceeds 15 minutes, API Gateway will reject the request. Therefore, the local time on the client must be synchronized with the clock server to avoid a large offset in the value of the **X-Sdk-Date** request header.

## Token-based Authentication

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

### NOTE

- The validity period of a token is 24 hours. When using a token for authentication, cache it to prevent frequently calling the API for obtaining a user token.
- Ensure that the token is valid when you use it. Using a token that will soon expire may cause API calling failures.

When calling the API to **obtain a user token**, set **auth.scope** in the request body to **project**.

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

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 **ABCDEFGH....**, add **X-Auth-Token: ABCDEFH....** to a request as follows:

```
GET https://iam.ap-southeast-3.myhuaweicloud.com/v3.0/OS-USER/users
Content-Type: application/json
X-Auth-Token: ABCDEFH....
```

## 3.3 Response

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

### Status Code

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 Codes](#).

If status code 201 is returned for the API for [creating an IAM user as an administrator](#), the request is successful.

### Response Header

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

For the API for [creating an IAM user as an administrator](#), the message header shown in [Figure 3-2](#) is returned.

**Figure 3-2** Response headers

```
"X-Frame-Options": "SAMEORIGIN",
"X-IAM-ETag-id": "2562365939-d8f6f12921974cb097338ac11fcec8a",
"Transfer-Encoding": "chunked",
"Strict-Transport-Security": "max-age=31536000; includeSubdomains;",
"Server": "api-gateway",
"X-Request-Id": "af2953f2bcc67a42325a69a19e6c32a2",
"X-Content-Type-Options": "nosniff",
"Connection": "keep-alive",
"X-Download-Options": "noopen",
"X-XSS-Protection": "1; mode=block;",
"X-IAM-Trace-Id": "token_██████████_null_af2953f2bcc67a42325a69a19e6c32a2",
"Date": "Tue, 21 May 2024 09:03:40 GMT",
"Content-Type": "application/json; charset=utf8"
```

### Response Body

A response body is often returned in a structured format defined by the response header field **Content-Type** and transfers information except the response header.

For the API for [creating an IAM user as an administrator](#), the following message body is returned. The following example is part of the response body for the API used to obtain a user token:

```
{
  "user": {
    "id": "c131886aec...",
    "name": "IAMUser",
    "description": "IAM User Description",
    "areacode": "",
    "phone": "",
    "email": "****@***.com",
    "status": null,
    "enabled": true,
```

```
"pwd_status": false,  
"access_mode": "default",  
"is_domain_owner": false,  
"xuser_id": "",  
"xuser_type": "",  
"password_expires_at": null,  
"create_time": "2024-05-21T09:03:41.000000",  
"domain_id": "d78cbac1.....",  
"xdomain_id": "30086000.....",  
"xdomain_type": "",  
"default_project_id": null  
}  
}
```

If an error occurs during API calling, an error code and a message will be returned. An error response body is shown as follows:

```
{  
  "error_msg": "Request body is invalid.",  
  "error_code": "IAM.0011"  
}
```

In the response body, **error\_code** indicates an error code, and **error\_msg** provides information about the error.

# 4 API

---

## 4.1 VPC endpoint management

### 4.1.1 Deleting VPC Endpoint Access Control Information

#### Function

This API is used to delete a private network security access control policy. Before calling this API, make sure the security access control policy does exist.

#### Calling Method

For details, see [Calling APIs](#).

#### Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions. For details about the required permissions, see [Permissions Policies and Supported Actions](#).

#### URI

DELETE /v2/vpceps

## Request Parameters

**Table 4-1** Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<b>Definition</b> User token. (It is the value obtained from X-Subject-Token in the response header.) It can be obtained by calling the API for <a href="#">obtaining an IAM user token</a> . <b>Constraints</b> Global tenant tokens are not supported. Use a region-level token whose <b>scope</b> is <b>project</b> . <b>Range</b> N/A <b>Default Value</b> N/A
region	Yes	String	<b>Definition</b> Region where the VPC endpoint to be deleted is located. It can be found from the region column in the <a href="#">Endpoint</a> list. <b>Constraints</b> N/A <b>Range</b> Enter 1 to 40 characters. Only digits, letters, and hyphens (-) are allowed. <b>Default Value</b> N/A

**Table 4-2** Request body parameters

Parameter	Mandatory	Type	Description
enterprise_id	No	String	<b>Definition</b> Tenant ID. For details about how to obtain the account ID, see <a href="#">Obtaining an Account ID</a> . <b>Constraints</b> N/A. <b>Range</b> Enter 1 to 40 characters. Only digits, letters, hyphens (-), and underscores (_) are allowed. <b>Default Value</b> N/A.
vpceps	No	Array of <a href="#">VpcepRequestInfo</a> objects	<b>Definition</b> List of authorized VPC endpoint information. <b>Constraints</b> N/A

**Table 4-3** VpcepRequestInfo

Parameter	Mandatory	Type	Description
description	No	String	<b>Definition</b> VPC endpoint description. <b>Constraints</b> N/A <b>Range</b> Enter 0 to 128 characters. Use only letters, digits, spaces, and these special characters: ()[]-_.~.&; <b>Default Value</b> N/A

Parameter	Mandatory	Type	Description
vpcep_id	No	String	<b>Definition</b> VPC endpoint ID. Check it from the <b>All Account Settings &gt; General &gt; Internal Secure Access</b> page. <b>Constraints</b> N/A <b>Range</b> Enter 1 to 40 characters. Only use digits, lower-case letters, and hyphens (-). <b>Default Value</b> N/A

## Response Parameters

**Status code: 200**

**Table 4-4** Response body parameters

Parameter	Type	Description
status	String	<b>Definition</b> Status. <b>Range</b> <ul style="list-style-type: none"><li>• <b>ok</b>: The API is successfully called.</li></ul>
total	Integer	<b>Definition</b> Total count. <b>Range</b> N/A.

**Status code: 401**

**Table 4-5** Response body parameters

Parameter	Type	Description
error_code	String	<b>Definition</b> Error code. <b>Range</b> N/A.

Parameter	Type	Description
error_msg	String	<b>Definition</b> Error message. <b>Range</b> N/A.

**Status code: 404****Table 4-6** Response body parameters

Parameter	Type	Description
error_code	String	<b>Definition</b> Error code. <b>Range</b> N/A.
error_msg	String	<b>Definition</b> Error message. <b>Range</b> N/A.

**Example Requests**

```
DELETE https://{endpoint}/v2/vpceps

{
  "enterprise_id" : "abcdbfa39r7pg09la8msyu8vq004aabcd",
  "vpceps" : [ {
    "vpcep_id" : "1234bfa39r7pg09la8msyu8vq004a1234"
  } ]
}
```

**Example Responses****Status code: 200**

Deleted.

```
{
  "status" : "ok",
  "total" : 1
}
```

## Status Codes

Status Code	Description
200	Deleted.
401	Insufficient permissions.
404	Not found.

## Error Codes

See [Error Codes](#).

## 4.1.2 Obtaining List of VPC Endpoints Authorized by a Tenant

### Function

This API is used to obtain the VPC endpoint access control list authorized by a tenant. Before calling this API, make sure the security access control policy does exist.

### Calling Method

For details, see [Calling APIs](#).

### Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions. For details about the required permissions, see [Permissions Policies and Supported Actions](#).

### URI

GET /v2/vpceps

**Table 4-7** Query Parameters

Parameter	Mandatory	Type	Description
enterprise_id	Yes	String	<b>Definition</b> Tenant ID. For details about how to obtain the account ID, see <a href="#">Obtaining an Account ID</a> . <b>Constraints</b> N/A <b>Range</b> Enter 1 to 40 characters. Only digits, letters, underlines (_), and hyphens (-) are allowed. <b>Default Value</b> N/A
vpcep_ids	No	String	<b>Definition</b> The list of queried VPC endpoint IDs. Check them from the <b>All Account Settings &gt; General &gt; Internal Secure Access</b> page. <b>Constraints</b> N/A <b>Range</b> Enter 1 to 1,229 characters. Only use digits, lower-case letters, and hyphens (-). <b>Default Value</b> N/A
offset	No	Integer	<b>Definition</b> Offset. <b>Constraints</b> N/A <b>Range</b> The value ranges from 0 to 9,999. <b>Default Value</b> N/A

Parameter	Mandatory	Type	Description
limit	No	Integer	<b>Definition</b> Page size. <b>Constraints</b> N/A <b>Range</b> The value ranges from 1 to 100. <b>Default Value</b> N/A
sort	No	String	<b>Definition</b> Sorting by vpcep_id. <b>Constraints</b> N/A <b>Range</b> <ul style="list-style-type: none"><li>• asc ASC: ascending order.</li><li>• desc DESC: descending order.</li></ul> <b>Default Value</b> N/A

## Request Parameters

**Table 4-8** Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	<b>Definition</b> User token. (It is the value obtained from X-Subject-Token in the response header.) It can be obtained by calling the API for <a href="#">obtaining an IAM user token</a> . <b>Constraints</b> Global tenant tokens are not supported. Use a region-level token whose <b>scope</b> is <b>project</b> . <b>Range</b> N/A <b>Default Value</b> N/A

Parameter	Mandatory	Type	Description
region	Yes	String	<b>Definition</b> Region where the VPC endpoint to be queried is located. It can be found from the region column in the <a href="#">Endpoint</a> list. <b>Constraints</b> N/A <b>Range</b> Enter 1 to 40 characters. Only digits, letters, and hyphens (-) are allowed. <b>Default Value</b> N/A

## Response Parameters

Status code: 200

Table 4-9 Response body parameters

Parameter	Type	Description
status	String	<b>Definition</b> Status. <b>Range</b> ● <b>ok</b> : The API is successfully called.
data	<a href="#">TenantVpceInfos</a> object	<b>Definition</b> Tenant and their authorized VPC endpoints. <b>Range</b> N/A
limit	Integer	<b>Definition</b> Page size. <b>Range</b> 0 to 100.
offset	Integer	<b>Definition</b> Offset. <b>Range</b> 0 to 9,999.

Parameter	Type	Description
total	Integer	<b>Definition</b> Total data volume. <b>Range</b> N/A

**Table 4-10** TenantVpceInfos

Parameter	Type	Description
enterprise_id	String	<b>Definition</b> Tenant ID. <b>Range</b> Enter 1 to 40 characters. Only digits, letters, underlines (_), and hyphens (-) are allowed.
vpceps	Array of <b>VpceInfo</b> objects	<b>Definition</b> Information about the authorized VPC endpoints. <b>Range</b> N/A

**Table 4-11** VpceInfo

Parameter	Type	Description
create_time	String	<b>Definition</b> Creation time. <b>Range</b> N/A
creator	String	<b>Definition</b> Creator. <b>Range</b> N/A
description	String	<b>Definition</b> VPC endpoint description. <b>Range</b> N/A

Parameter	Type	Description
modify_time	String	<b>Definition</b> Modification time. <b>Range</b> N/A
region	String	<b>Definition</b> Site. <b>Range</b> Enter 1 to 40 characters. Only use digits, lower-case letters, and hyphens (-).
vpcep_id	String	<b>Definition</b> VPC endpoint ID. <b>Range</b> Enter 1 to 40 characters. Only use digits, lower-case letters, and hyphens (-).

**Status code: 400****Table 4-12** Response body parameters

Parameter	Type	Description
error_code	String	<b>Definition</b> Error code. <b>Range</b> N/A.
error_msg	String	<b>Definition</b> Error message. <b>Range</b> N/A.

**Status code: 401**

**Table 4-13** Response body parameters

Parameter	Type	Description
error_code	String	<b>Definition</b> Error code. <b>Range</b> N/A.
error_msg	String	<b>Definition</b> Error message. <b>Range</b> N/A.

**Status code: 404****Table 4-14** Response body parameters

Parameter	Type	Description
error_code	String	<b>Definition</b> Error code. <b>Range</b> N/A.
error_msg	String	<b>Definition</b> Error message. <b>Range</b> N/A.

**Example Requests**

```
GET https://{endpoint}/v2/vpceps?  
enterprise_id=a8dd901e70f2485cb4f1fa2264eb3add&vpcep_ids=a8dd901e70f2485cb4f1fa2264eb3add,00120  
e895121420aa2c81870d09756b2&sort=asc
```

**Example Responses****Status code: 200**

List of VPC endpoints authorized by the tenant.

```
{  
  "data" : {  
    "enterprise_id" : "a8dd901e70f2485cb4f1fa2264eb3add",  
    "vpceps" : [ {  
      "vpcep_id" : "a8dd901e70f2485cb4f1fa2264eb3add",  
      "description" : "VPCEP1",  
      "creator" : "user001",  
      "create_time" : "2026-05-01T10:30:00Z",  
      "modify_time" : "2026-05-01T10:30:00Z",
```

```
"region" : "cn-north-7"  
}, {  
  "vpcep_id" : "00120e895121420aa2c81870d09756b2",  
  "description" : "VPCEP2",  
  "creator" : "user002",  
  "create_time" : "2026-05-02T14:20:001Z",  
  "modify_time" : "2026-05-03T09:15:001Z",  
  "region" : "cn-east-3"  
}]  
},  
"offset" : 0,  
"limit" : 10,  
"total" : 2  
}
```

## Status Codes

Status Code	Description
200	List of VPC endpoints authorized by the tenant.
400	Invalid parameter.
401	Insufficient permissions.
404	Not found.

## Error Codes

See [Error Codes](#).

# 5 Permissions and Supported Actions

---

## 5.1 Permissions and Supported Actions

This section describes fine-grained permissions management for your CodeArts resources. If your account does not need individual IAM users, you can skip over this section.

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

You can grant users permissions by using [roles](#) and [policies](#). Roles are provided by IAM to define service-based permissions that match users' job responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

### NOTE

If you want to allow or deny the access to an API, use policy-based authorization.

Your account has all the permissions required to call all APIs. If you use IAM users in your account to call an API, the IAM users must be granted the required permissions. To call this API, the user must have the Tenant Administrator permission.

# 6 Appendix

## 6.1 Status Codes

[Table 6-1](#) describes status codes.

**Table 6-1** Status codes

Status Code	Message	Description
100	Continue	The client should continue with its request. This interim response is used to inform the client that the initial part of the request has been received and has not yet been rejected by the server.
101	Switching Protocols	The protocol should be switched only when it is advantageous to do so. For example, the current HTTP protocol is switched to a later version.
201	Created	The request has been fulfilled and resulted in a new resource being created.
202	Accepted	The request has been accepted for processing, but the processing has not been completed.
203	Non-Authoritative Information	The server successfully processed the request, but is returning information that may be from another source.
204	NoContent	The server has successfully processed the request, but does not return any response. The status code is returned in response to an HTTP OPTIONS request.

Status Code	Message	Description
205	Reset Content	The server has fulfilled the request, but the requester is required to reset the content.
206	Partial Content	The server has fulfilled the partial GET request for the resource.
300	Multiple Choices	The response contains a list of resource characteristics and addresses from which a user terminal (such as a browser) can choose the most appropriate one.
301	Moved Permanently	This and all future requests have been permanently moved to the given URI indicated in this response.
302	Found	The requested resource has been temporarily moved.
303	See Other	The response to the request can be found under a different URI and should be retrieved using a GET or POST method.
304	Not Modified	The requested resource has not been modified. When the server returns this status code, no resource is returned.
305	Use Proxy	The requested resource is available only through a proxy.
306	Unused	This HTTP status code is no longer used.
400	BadRequest	Invalid request. The client should modify the request instead of re-initiating it.
401	Unauthorized	The authentication information provided by the client is incorrect or invalid.
402	Payment Required	Reserved request.
403	Forbidden	Request rejected. The server has received the request and understood it, but refuses to respond to it. The client should not repeat the request without modifications.
404	NotFound	The requested resource cannot be found. The client should modify the request instead of re-initiating it.

Status Code	Message	Description
405	MethodNotAllowed	The method specified in the request is not allowed for the requested resource. The client should modify the request instead of re-initiating it.
406	Not Acceptable	The server cannot implement the request based on the content characteristics of the request.
407	Proxy Authentication Required	This code is similar to 401, but indicates that the client must first authenticate itself with the proxy.
408	Request Time-out	The server timed out waiting for the request. The client may re-initiate the request without modifications at any time later.
409	Conflict	The request cannot be processed due to a conflict. This status code indicates that the resource that the client attempts to create already exists, or the request fails to be processed because of the update of the conflict request.
410	Gone	The requested resource cannot be found. This status code indicates that the requested resource has been deleted permanently.
411	Length Required	The server refused to process the request because the request does not specify the length of its content.
412	Precondition Failed	The server does not meet one of the preconditions that the requester puts on the request.
413	Request Entity Too Large	The server refuses to process a request because the request is too large. The server may disable the connection to prevent the client from sending requests consecutively. If the server temporarily cannot process the request, the response will contain a <b>Retry-After</b> header field.
414	Request-URI Too Large	The request URI is too long for the server to process.
415	Unsupported Media Type	The server does not support the media type in the request.
416	Requested range not satisfiable	The requested range is invalid.

Status Code	Message	Description
417	Expectation Failed	The server fails to meet the requirements of the <b>Expect</b> request header field.
422	UnprocessableEntity	The request is well-formed but is unable to respond due to semantic errors.
429	TooManyRequests	The client sends too many requests to the server within a given time, exceeding the client's access frequency limit or beyond the server's processing capability. In this case, the client should repeat requests after the time specified in the <b>Retry-After</b> header of the response expires.
500	InternalServerError	The server is able to receive the request but it cannot understand the request.
501	Not Implemented	The server does not support the requested function, and therefore cannot implement the request.
502	Bad Gateway	The server acting as a gateway or proxy receives an invalid response from a remote server.
503	ServiceUnavailable	The requested service is invalid. The client should modify the request instead of re-initiating it.
504	ServerTimeout	The server could not return a timely response. The response will reach the client only if the request carries a timeout parameter.
505	HTTP Version not supported	The server does not support the HTTP protocol version used in the request.

## 6.2 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	UC.00011001	Bad request.	Bad request.	Check the URL, parameters, and request header.

Status Code	Error Codes	Error Message	Description	Solution
400	UC.00011002	Invalid parameter.	Invalid parameter.	Check the parameter completeness or redundancy, and format.
400	UC.00011011	Invalid resource path.	Invalid resource path.	Check whether the resource path is linked to the service resource list.
400	UC.00011012	User does not exist or already associated with a role.	User does not exist or already associated with a role.	Check whether the user is deleted, disabled, or already added to the project.
400	UC.00011013	Template role cannot be associated with any group or user.	Template role cannot be associated with any group or user.	Check whether the role is a template role.
400	UC.00011014	Invalid permission rule.	Invalid permission rule.	Check the permission rule.
400	UC.00011015	Special roles cannot be associated.	Special roles cannot be associated.	Check whether the associated role is project administrator.
400	UC.00011019	Your free quota is insufficient.	Your free quota is insufficient.	Check your quota.
400	UC.00011020	Insufficient quota in your package.	Insufficient quota in your package.	Check your remaining quota.
400	UC.00011021	IPD projects cannot be managed across tenants.	IPD projects cannot be managed across tenants.	IPD projects cannot be managed across tenants.
400	UC.00011023	The user already has a role in this project.	The user already has a role in this project.	Check your parameter.

Status Code	Error Codes	Error Message	Description	Solution
400	UC.00011025	Only one enterprise account can be invited at a time.	Only one enterprise account can be invited at a time.	Only one enterprise account can be invited at a time.
400	UC.00011032	Invalid enterprise account ID or name.	Invalid enterprise account ID or name.	Check your parameter.
400	UC.00011036	Your VPCEP quota has been used up.	Your VPCEP quota has been used up.	Increase your quota.
400	UC.00011037	Project not found.	Project not found.	Check your parameter.
400	UC.00011038	Permission template not found.	Permission template not found.	Check your parameter.
400	UC.00011039	Template already created with this project.	Template already created with this project.	You can only use a project to create one template.
400	UC.00011040	Too many templates under your tenant.	Too many templates under your tenant.	Too many templates under your tenant.
400	UC.00011041	Project template name already exists.	Project template name already exists.	Use another name.
400	UC.00011042	Project type and template type do not match.	Project type and template type do not match.	Check your parameter.
400	UC.00011044	Template roles cannot be deleted.	Template roles cannot be deleted.	Template roles cannot be deleted.
400	UC.00011045	The user has left or is not in the project.	The user has left or is not in the project.	Join the project first.
400	UC.00011053	Project and role do not match.	Project and role do not match.	Role not found or not included in the project.

Status Code	Error Codes	Error Message	Description	Solution
400	UC.00011054	Role already added to this user.	Role already added to this user.	Do not add the same role again.
400	UC.00011055	You cannot add a user from another enterprise to your project.	You cannot add a user from another enterprise to your project.	Check the user's tenant.
400	UC.00011059	The user is not a member of this project.	The user is not a member of this project.	Add the user to the project first.
400	UC.00011061	Too many users to authorize.	Too many users to authorize.	You cannot add more.
400	UC.00011064	Failed to obtain delegated users from IAM Identity Center.	Failed to obtain delegated users from IAM Identity Center.	Try again later.
400	UC.00011085	Only one agency can be selected at a time.	Only one agency can be selected at a time.	Select one agency.
400	UC.00011176	Team not found.	Team not found.	Check your parameter.
400	UC.00011177	Too many members in the team.	Too many members in the team.	Remove some members.
400	UC.00011178	Team name already exists.	Team name already exists.	Use another name.
400	UC.00011179	This team has already been associated with the project.	This team has already been associated with the project.	Select another project.
400	UC.00011180	Invalid role name.	Invalid role name.	Use another name.
400	UC.00011181	Invalid user.	Invalid user.	The user may not exist in the current tenant.

Status Code	Error Codes	Error Message	Description	Solution
400	UC.00011182	Invalid user-role relationship.	Invalid user-role relationship.	The user-role relationship does not exist.
400	UC.00011189	Role not found.	Role not found.	Check your role parameter.
400	UC.00011191	Too many teams in the project.	Too many teams in the project.	Too many teams in the project.
401	UC.00010002	You do not have permissions.	You do not have permissions.	Check your permissions.
401	UC.00011003	No permission.	No permission.	Check your permissions.
401	UC.00011017	Enterprise account frozen.	Enterprise account frozen.	Unfreeze it first.
401	UC.00011018	Yearly/monthly billing currently disabled.	Yearly/monthly billing currently disabled.	Enable yearly/monthly billing first.
401	UC.00011026	Target enterprise not yet authorized.	Target enterprise not yet authorized.	Authorize it first.
401	UC.00011028	Incorrect user numbers for the target enterprise.	Incorrect user numbers for the target enterprise.	Check the user numbers.
401	UC.00011030	Target tenant not authorized for the region.	Target tenant not authorized for the region.	Check the region.
401	UC.00011031	You cannot invite your own enterprise account.	You cannot invite your own enterprise account.	You cannot invite your own enterprise account.
401	UC.00011034	Not authorized to modify this permission.	Not authorized to modify this permission.	Check your parameter.

Status Code	Error Codes	Error Message	Description	Solution
401	UC.00011043	Not authorized to modify this role.	Not authorized to modify this role.	Check your permissions.
401	UC.00011084	Target tenant not yet authorized.	Target tenant not yet authorized.	Authorize it first.
403	UC.00011004	Data currently in use.	Data currently in use.	The data cannot be deleted. Delete the associated data first.
403	UC.00011016	Too many custom roles.	Too many custom roles.	Max. 500 custom roles. Delete unnecessary ones.
403	UC.00011062	Package frozen.	Package frozen.	Unfreeze it first.
403	UC.00011065	Tenants with private network access enabled cannot be invited.	Tenants with private network access enabled cannot be invited.	Do not invite tenants for which private network access has been enabled.
403	UC.00011070	The project creator cannot be deleted.	The project creator cannot be deleted.	Exclude the project creator.
403	UC.00011071	Not permitted to set project administrator.	Not permitted to set project administrator.	Exclude the project administrator.
404	UC.00010003	File not found.	File not found.	Check the file.
404	UC.00011005	Not found.	Not found.	Data already deleted.
405	UC.00011006	Unavailable method.	Unavailable method.	Contact technical support.
408	UC.00011007	Request timed out.	Request timed out.	Remote connection timed out. Check background logs.

Status Code	Error Codes	Error Message	Description	Solution
409	UC.00011008	Conflict.	Conflict.	Check whether the name matches the ID.
409	UC.00011009	Data already exists.	Data already exists.	Check the input parameter, or delete the data.
409	UC.00011022	Request already submitted.	Request already submitted.	Do not submit another request.
409	UC.00011033	The user is already in this project.	The user is already in this project.	Check your parameter.
409	UC.00011063	Failed to obtain the Redis lock.	Failed to obtain the Redis lock.	Check the Redis health.
424	UC.00011024	An external service returned an error.	An external service returned an error.	Check the external service.
429	UC.00011035	Account locked.	Account locked.	Check your parameter, and try again 15 minutes later.
500	UC.00010005	Internal service error.	Internal service error.	Check the background logs.
500	UC.00011010	Operation failed.	Operation failed.	Check the background logs.

## 6.3 Obtaining a Project ID

### 6.3.1 Obtaining an IAM Project ID

#### Obtaining an IAM Project ID by Calling an API

A project ID can be obtained by calling a specific API. For details, see [Querying Project Information Based on the Specified Criteria](#).

The API used to obtain an IAM project ID is **GET https://{Endpoint}/v3/projects/**, where *{Endpoint}* indicates the IAM endpoint. You can obtain the IAM endpoint from [Regions and Endpoints](#). For details about API authentication, see [Authentication](#).

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

```
{
  "projects": [
    {
      "domain_id": "65382450e8f64ac0870cd180d14e684b",
      "is_domain": false,
      "parent_id": "65382450e8f64ac0870cd180d14e684b",

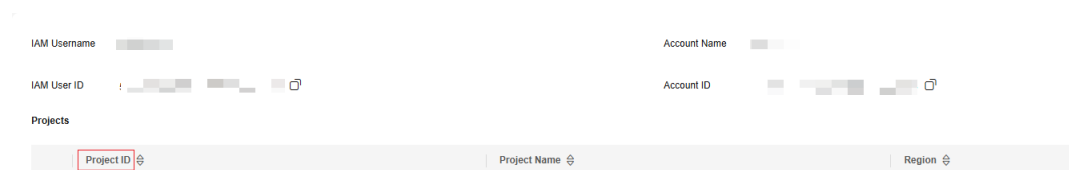
      "name": "ap-southeast-3",
      "description": "",
      "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
      },
      "id": "a4a5d4098fb4474fa22cd05f897d6b99",
      "enabled": true
    }
  ],
  "links": {
    "next": null,
    "previous": null,
    "self": "https://www.example.com/v3/projects"
  }
}
```

## Obtaining an IAM 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:


- Step 1** Log in to the management console.
- Step 2** Hover over the username in the upper right corner and choose **My Credentials** from the drop-down list.
- Step 3** On the displayed **API Credentials** page, check project IDs in the project list.

**Figure 6-1** Viewing an IAM project ID



----End

## 6.3.2 Obtaining a CodeArts Project ID

- Step 1** Go to the CodeArts homepage.
  1. Log in to the [CodeArts console](#), click , and select a region where you have enabled CodeArts.
  2. Click **Go to Workspace**.  
If your account uses the old billing mode (see [Old Billing Modes](#)), click **Access Service**.
- Step 2** Find the target project card on the CodeArts homepage and copy the project ID.

**Figure 6-2** Obtaining a CodeArts Project ID



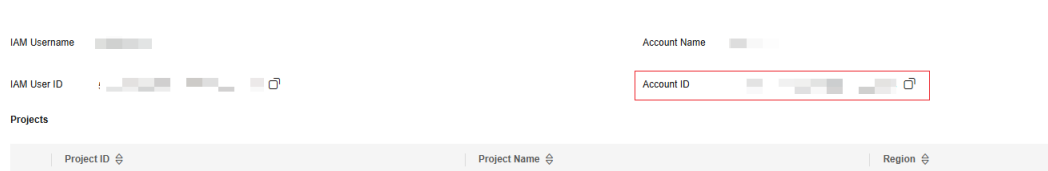
----End

## 6.4 Obtaining an Account ID

An account ID is required for some URLs when an API is called. To obtain an account ID, perform the following operations:

- Step 1** Log in to the management console.
- Step 2** Hover over the username in the upper right corner and choose **My Credentials** from the drop-down list.
- Step 3** On the **API Credentials** page, view **Account ID**.

**Figure 6-3** Obtaining an Account ID



----End

---

# 7 Change History

---

Each document issue builds upon the previous one, with the latest issue incorporating all changes made in earlier versions.

Released On	Change Description
2025-11-21	This is the first official release.