

Cloud Certificate Manager

API Reference

Issue	01
Date	2025-11-28



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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.

Contents

1 Before You Start.....	1
2 API Overview.....	3
3 Calling APIs.....	5
3.1 Making an API Request.....	5
3.2 Authentication.....	7
3.3 Response.....	9
4 API.....	11
4.1 Managing SSL Certificates.....	11
4.1.1 Certificate Application Management.....	11
4.1.1.1 Apply for a certificate.....	11
4.1.1.2 Withdrawing a Certificate Application.....	19
4.1.2 Certificate Order Management.....	23
4.1.2.1 Purchasing an SSL Certificate.....	23
4.1.3 Certificate Lifecycle Management.....	30
4.1.3.1 Querying the Certificate List.....	30
4.1.3.2 Importing a Certificate.....	40
4.1.3.3 Obtaining Details of a Certificate.....	46
4.1.3.4 Deleting a Certificate.....	56
4.1.3.5 Exporting a Certificate.....	59
4.1.4 Certificate Deployment Management.....	63
4.1.4.1 Pushing a Certificate.....	63
4.1.4.2 Pushing Certificates in Batches.....	67
4.1.4.3 Deploying Certificates.....	71
4.2 Managing Private Certificates.....	77
4.2.1 Private CA Management.....	77
4.2.1.1 Querying the CA List.....	77
4.2.1.2 Creating a CA.....	88
4.2.1.3 Querying the CA Quota.....	103
4.2.1.4 Querying CA Details.....	108
4.2.1.5 Deleting a Private CA.....	117
4.2.1.6 Activating a CA.....	122
4.2.1.7 Exporting a CSR of a CA.....	134

4.2.1.8 Disabling a Private CA.....	139
4.2.1.9 Enabling a Private CA.....	143
4.2.1.10 Exporting a CA Certificate.....	147
4.2.1.11 Importing a CA Certificate.....	153
4.2.1.12 Restoring a CA.....	157
4.2.1.13 Revoking a Subordinate CA.....	162
4.2.2 Private Certificate Management.....	167
4.2.2.1 Querying the List of Private Certificates.....	168
4.2.2.2 Applying for a Certificate.....	177
4.2.2.3 Issuing a Certificate with a CSR.....	191
4.2.2.4 Parsing a CSR.....	200
4.2.2.5 Querying the Private Certificate Quota.....	206
4.2.2.6 Querying Certificate Details.....	211
4.2.2.7 Deleting a Certificate.....	219
4.2.2.8 Exporting a Certificate.....	223
4.2.2.9 Revoking a Certificate.....	233
4.2.3 Certificate Revocation.....	238
4.2.3.1 Checking the Agency Permission.....	239
4.2.3.2 Creating an Agency.....	243
4.2.3.3 Querying the List of OBS Buckets.....	247
4.2.3.4 Enabling a CRL.....	252
4.2.3.5 Disabling a CRL.....	256
4.2.4 Tag Management.....	261
4.2.4.1 Batch Creating CA Tags.....	261
4.2.4.2 Batch Deleting Tags for a CA.....	266
4.2.4.3 Creating a Tag for a CA.....	271
4.2.4.4 Querying the Tag List for a CA.....	276
4.2.4.5 Querying the Tag List for All CAs.....	282
4.2.4.6 Querying the CA List by Tags.....	286
4.2.4.7 Querying the CA Quantity by Tag.....	295
4.2.4.8 Batch Creating Tags for a Certificate.....	301
4.2.4.9 Batch Deleting Tags for a Certificate.....	307
4.2.4.10 Creating a Tag for a Certificate.....	312
4.2.4.11 Querying the Tag List for a Certificate.....	316
4.2.4.12 Querying the Tag List for All Certificates.....	321
4.2.4.13 Querying the Certificate List by Tag.....	326
4.2.4.14 Querying the Certificate Quantity by Tags.....	335
4.2.5 Order Management.....	341
4.2.5.1 Purchasing a CA.....	342
4.2.6 Querying Supported Features of a Site.....	348
4.2.6.1 Querying Supported Features in a Site.....	348
5 Permissions and Supported Actions.....	353

5.1 Introduction to Permissions Policies and Supported Actions..... 353

5.2 Private Certificate Authority (PCA)..... 354

A Appendix..... 357

A.1 Status Codes..... 357

A.2 Error Codes..... 357

A.2.1 SCM Error Codes..... 358

A.2.2 PCA Error Codes..... 369

A.3 Obtaining a Project ID..... 377

1 Before You Start

Welcome to use Cloud Certificate Manager (CCM). Cloud Certificate Manager (CCM) issues cloud certificates and manages the entire lifecycle of the certificates. It can be used in many scenarios, such as cloud platform, Internet of Vehicles (IoV), and Internet of Things (IoT). CCM includes the SSL Certificate Manager (SCM) and Private Certificate Authority (PCA) services.

Before calling CCM APIs, ensure that you have understood the concepts related to CCM. For more information, see [What Is CCM?](#)

Endpoints

An endpoint is the **request address** for calling an API. CCM is a global service deployed for all physical regions. [Table 1-1](#) lists all CCM endpoints.

Table 1-1 CCM endpoints

Region	Endpoint Region	Endpoint	Protocol	Microservice Included
All	ALL	ccm.eu-west-101.myhuaweicloud.eu	HTTPS	PCA
All	ALL	scm.eu-west-101.myhuaweicloud.eu	HTTPS	SCM

Concepts

- 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.

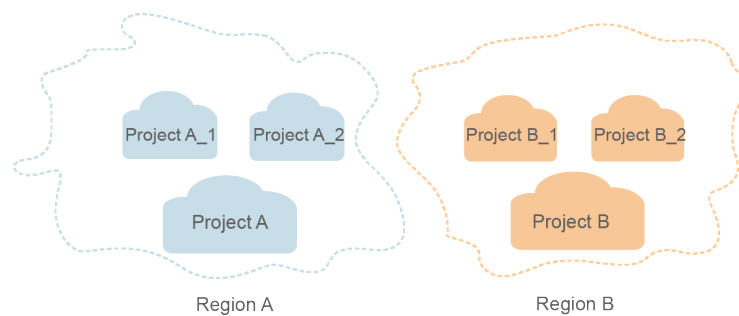
- Availability Zone (AZ)

An 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, compute, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

- Project

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

Figure 1-1 Project isolating model



2 API Overview

By using the APIs provided by CCM, you can use all functions of CCM.

Managing SSL Certificates

API		Description
Certificate lifecycle management	Querying the Certificate List	Query the SSL certificate list.
	Importing a Certificate	Import a certificate to SCM.
	Obtaining Details of a Certificate	Query details of an SSL certificate.
	Deleting a Certificate	Delete an SSL certificate.
	Exporting a Certificate	Export an SSL certificate.
Certificate application management	Apply for a certificate.	Apply for an SSL certificate.
	Withdrawing a Certificate Application	Withdraw an SSL certificate application.
Certificate order management	Purchasing an SSL Certificate	Purchase an SSL certificate.
Certificate deployment management	Pushing a Certificate	Push an SSL certificate to other Huawei Cloud services.
	Pushing Certificates in Batches	Push an SSL certificate to other Huawei Cloud services in batches.

API		Description
	Deploying Certificates	Deploy SSL certificates to other Huawei Cloud services, such as CDN, WAF, and ELB.

Managing Private Certificates

API	Description
Private CA Management	Manage private CAs, including creating, querying, and deleting private CAs.
Private Certificate Management	Manage private certificates, including creating, querying, and deleting private certificates.
Certificate Revocation	Revoke certificates, including creating an agency, querying an agency, and querying the OBS bucket list.
Tag Management	Manage private certificates and private CA tags, including creating and deleting private CAs and private CA tags, and querying the CA list and number of CAs by tag.
Order Management	Purchase a private CA.
Querying Supported Features of a Site	Querying Supported Features in a Site

3 Calling APIs

3.1 Making an API Request

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

Request URI

A request URI is in the following format:

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

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

- **URI-scheme:**
Protocol used to transmit requests. All APIs use HTTPS.
- **Endpoint:**
Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from the administrator.
- **resource-path:**
Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.
- **query-string:**
Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

NOTE

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

Request Methods

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

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

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

```
POST https://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 the administrator.

NOTE

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

```
POST https://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": "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: ABCDEFGH....** to a request as follows:

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

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.

NOTICE

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

3.3 Response

Status Code

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

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

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

Response Header

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

Figure 3-1 shows the response header for the API of obtaining a user token, in which **x-subject-token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

Figure 3-1 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 → MIIYXQYJKoZIhvcNAQcCoIIYtjCCGEOCAQExDTALBgIghkgB8ZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOansiZXhwaXJlc19hdCI6IjIwMTktMDItMTNUMC
fj3KJs6YgKnPvNRbW2eZ5eb78SZOkqjACgklqO1wi4JIGzrpd18LGXK5bdfq4lqHCYb8P4NaY0NYejcAgz/VeFYtLWT1GSO0zxKZmlQHq82HBqHdglZO9fuEbL5dMhdavj+33wEI
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXI1jipPEGA270g1FrUooL6jggIFkNPQuFSOU8+uSsttVwRtNfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUUVhVpxk8pxiX1wTEboX-
RzT6MUbpvGw-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. The following describes part of the response body.

```
{
  "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 Managing SSL Certificates

4.1.1 Certificate Application Management

4.1.1.1 Apply for a certificate.

Function

This API is used to apply for a certificate.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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

POST /v3/scm/certificates/{certificate_id}/apply

Table 4-1 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Certificate ID. Minimum: 16 Maximum: 16

Request Parameters

Table 4-2 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Table 4-3 Request body parameters

Parameter	Mandatory	Type	Description
domain	Yes	String	Domain name bound to a certificate. • If you purchase a single-domain or wildcard-domain certificate, enter a single domain name or wildcard domain name. • If you purchase a multi-domain certificate, you need to select a domain name as the primary domain name. Example: www.example.com Minimum: 0 Maximum: 255

Parameter	Mandatory	Type	Description
sans	No	String	Additional domain name associated with a multi-domain certificate. This value is required only when the purchased certificate is a multi-domain certificate and the quota of additional domain names can be increased. Use semicolons (;) to separate multiple domain names. Example: www.example.com;www.example1.com;www.example2.com Minimum: 0 Maximum: 4096
csr	No	String	Certificate CSR string, which must match the domain name. Minimum: 0 Maximum: 5120
company_name	No	String	Company name. This parameter is mandatory for OV and EV certificates. The value contains 0 to 63 characters. Minimum: 0 Maximum: 63
company_unit	No	String	Department name. The value contains 0 to 63 characters. Minimum: 0 Maximum: 63
company_province	No	String	Province where the company is located. This parameter is mandatory for OV and EV certificates. The value contains 0 to 63 characters. Minimum: 0 Maximum: 63

Parameter	Mandatory	Type	Description
company_city	No	String	City where the company is located. This parameter is mandatory for OV and EV certificates. The value contains 0 to 63 characters. Minimum: 0 Maximum: 63
country	No	String	Country code, which is mandatory for OV and EV certificates. The value must comply with the regular expression [A-Za-z]{2} . Minimum: 2 Maximum: 2
applicant_name	Yes	String	Applicant name. Enter 4 to 100 characters. Only letters, digits, underscores (_), hyphens (-), periods (.), brackets, spaces, and commas (,) are allowed. Minimum: 0 Maximum: 63
applicant_phone	Yes	String	Phone number of an applicant. Example: 13212345678 Minimum: 0 Maximum: 63
applicant_email	Yes	String	Email of an applicant. Example: example@huawei.com Minimum: 0 Maximum: 256
contact_name	No	String	Technical contact name. The value contains 0 to 63 characters. Minimum: 0 Maximum: 63
contact_phone	No	String	Phone number of the technical contact. Example: 13212345678 Minimum: 0 Maximum: 63

Parameter	Mandatory	Type	Description
contact_email	No	String	Email of a technical contact. Example: example@huawei.com Minimum: 0 Maximum: 256
auto_dns_auth	No	Boolean	Whether to push DNS authentication information to Huawei Cloud DNS. • true: Push • false: No push
agree_privacy_protection	Yes	Boolean	Whether to agree with the privacy agreement. You can submit your certificate application only when this parameter is set to true. • true: Agree to the privacy agreement. • false: Disagree with the privacy agreement.

Parameter	Mandatory	Type	Description
domain_method	Yes	String	Domain name verification method. • DNS: You need to verify the domain ownership by resolving a specific DNS record on the domain name management platform. • File: You need to create a specified file on the server to verify your ownership of the domain. • Email: You can click the link and follow the directions in the email to verify ownership of the domain. For DV and basic DV certificates (GeoTrust entry-level SSL certificates and DigiCert free SSL certificates), DNS is supported for verification by default. IP address (public IP address) certificates can be verified only by files. File verification is supported by only IP address certificates. Minimum: 0 Maximum: 32
key_algorithm	No	String	Key algorithm. The default value is RSA_2048. Minimum: 0 Maximum: 32
ca_hash_algorithm	No	String	Signature algorithm. Mandatory for the Geo OV certificate. • DEFAULT • SHA-256 Minimum: 0 Maximum: 32

Response Parameters

Status code: 200

Table 4-4 Response body parameters

Parameter	Type	Description
request_info	String	Request result. Minimum: 0 Maximum: 63

Status code: 401**Table 4-5** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403**Table 4-6** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500

Table 4-7 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

```
{
  "domain" : "www.test.com",
  "company_name" : "Company XX",
  "company_province" : "Sichuan",
  "company_city" : "Chengdu",
  "applicant_name" : "xx",
  "applicant_phone" : "12312345678",
  "applicant_email" : "example@test.com",
  "csr" : "",
  "sans" : "",
  "country" : "CN",
  "company_unit" : "IT",
  "contact_name" : "test",
  "contact_phone" : "12312345678",
  "contact_email" : "example@test.com",
  "auto_dns_auth" : false,
  "agree_privacy_protection" : true,
  "domain_method" : "DNS"
}
```

Example Responses

Status code: 200

Normal response.

```
{
  "request_info" : "success"
}
```

Status code: 401

Authentication failed.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Access denied.

```
{
  "error_code" : "SCM.XXX",
}
```

```
{  
  "error_msg" : "XXX"  
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{  
  "error_code" : "SCM.XXX",  
  "error_msg" : "XXX"  
}
```

Status Codes

Status Code	Description
200	Normal response.
401	Authentication failed.
403	Access denied.
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.1.1.2 Withdrawing a Certificate Application

Function

Withdraw the certificate application.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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

POST /v3/scm/certificates/{certificate_id}/cancel-cert

Table 4-8 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Certificate ID. Minimum: 16 Maximum: 16

Request Parameters

Table 4-9 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Response Parameters

Status code: 200

Table 4-10 Response body parameters

Parameter	Type	Description
cert_id	String	Certificate ID. Minimum: 16 Maximum: 16
message	String	Execution result. The value can be: success Minimum: 0 Maximum: 16

Status code: 401

Table 4-11 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403**Table 4-12** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500**Table 4-13** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

None

Example Responses

Status code: 200

Normal response.

```
{
  "cert_id" : "scsxxxx",
  "message" : "success"
}
```

Status code: 401

Authentication failed.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Access denied.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Normal response.
401	Authentication failed.
403	Access denied.
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.1.2 Certificate Order Management

4.1.2.1 Purchasing an SSL Certificate

Function

This API is used to purchase an SSL certificate.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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

POST /v3/scm/certificates/buy

Request Parameters

Table 4-14 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Table 4-15 Request body parameters

Parameter	Mandatory	Type	Description
cert_brand	Yes	String	Certificate authority. The options are as follows: • GEOTRUST • GLOBALSIGN • SYMANTEC • CFCA • TRUSTASIA • VTRUS Minimum: 0 Maximum: 32
cert_type	Yes	String	Certificate type. The options are as follows: • DV_SSL_CERT • DV_SSL_CERT_BASIC • EV_SSL_CERT • EV_SSL_CERT_PRO • OV_SSL_CERT • OV_SSL_CERT_PRO Minimum: 0 Maximum: 32
domain_type	Yes	String	Domain name type. The options are as follows: • SINGLE_DOMAIN: single domain name. • MULTI_DOMAIN: multi-domain name type. • WILDCARD: wildcard domain name. Minimum: 0 Maximum: 32
effective_time	Yes	Integer	Certificate validity period, in years. Minimum: 1 Maximum: 3

Parameter	Mandatory	Type	Description
domain_numbers	Yes	Integer	Number of domain names. - If domain_type is set to SINGLE_DOMAIN or WILDCARD, the value is 1. - If domain_type is set to MULTI_DOMAIN, the value ranges from 2 to 100. Minimum: 1 Maximum: 100
order_number	Yes	Integer	Number of purchased certificates. The value ranges from 1 to 100. Minimum: 1 Maximum: 100
agree_privacy_protection	Yes	Boolean	Whether to agree to the privacy agreement. The value can only be true. - true: agree - false: disagree
primary_domain_type	No	String	Primary domain name type in multiple domain names. The value can be: SINGLE_DOMAIN: primary single domain name WILDCARD_DOMAIN: primary wildcard domain name Minimum: 0 Maximum: 63
single_domain_number	No	Integer	Number of additional single domain names. Minimum: 1 Maximum: 100
wildcard_domain_number	No	Integer	Number of additional wildcard domain names. Minimum: 1 Maximum: 100
is_auto_pay	No	Boolean	Whether to enable auto payment. - true: enable - false: disable

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. If the enterprise project function is not enabled, you do not need to set this parameter. If the enterprise project function is enabled, you can set this parameter when querying a resource. If this parameter is not specified, the system searches for the required resource in all the enterprise projects that you have permissions for. In this case, the value of enterprise_project_id is all . The parameter value must meet one of the following requirements: • The value is all. • The value is 0. • The value matches the <code>^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}\$</code> regular expression. Minimum: 0 Maximum: 36
order_id	No	String	Order ID. Used only in combined purchase scenarios. Minimum: 0 Maximum: 63
tags	No	Array of ScsResourceTag objects	Tags. Array Length: 0 - 10

Table 4-16 ScsResourceTag

Parameter	Mandatory	Type	Description
key	No	String	Tag key. Minimum: 0 Maximum: 128

Parameter	Mandatory	Type	Description
value	No	String	Tag value. Minimum: 0 Maximum: 255

Response Parameters

Status code: 200

Table 4-17 Response body parameters

Parameter	Type	Description
order_id	String	Order ID. Minimum: 0 Maximum: 63
cert	Array of CertDetail objects	For details, see parameter description of the CertDetail field. Array Length: 0 - 1000

Table 4-18 CertDetail

Parameter	Type	Description
cert_id	String	Certificate ID. Minimum: 16 Maximum: 16

Status code: 401

Table 4-19 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403**Table 4-20** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500**Table 4-21** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

```
{  
  "cert_brand" : "GLOBALSIGN",  
  "cert_type" : "OV_SSL_CERT",  
  "domain_type" : "MULTI_DOMAIN",  
  "effective_time" : 1,  
  "domain_numbers" : 5,  
}
```

```
"order_number" : 1,  
"agree_privacy_protection" : true  
}
```

Example Responses

Status code: 200

Normal return.

```
{  
  "order_id" : "CS1803192259ROA8U",  
  "cert" : [ {  
    "cert_id" : "scs1481110651012"  
  } ]  
}
```

Status code: 401

Authentication failed.

```
{  
  "error_code" : "SCM.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 403

Access denied.

```
{  
  "error_code" : "SCM.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{  
  "error_code" : "SCM.XXX",  
  "error_msg" : "XXX"  
}
```

Status Codes

Status Code	Description
200	Normal return.
401	Authentication failed.
403	Access denied.
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.1.3 Certificate Lifecycle Management

4.1.3.1 Querying the Certificate List

Function

This API is used to query the certificate list by certificate name or bound domain name.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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 /v3/scm/certificates

Table 4-22 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	Number of certificate records on each page. The options are as follows: • 10: 10 certificate records can be displayed on each page. • 20: 20 certificate records can be displayed on each page. • 50: 50 certificate records can be displayed on each page. Minimum: 10 Maximum: 50 Default: 10
offset	No	Integer	Query offset. Minimum: 0 Maximum: 100 Default: 0

Parameter	Mandatory	Type	Description
sort_dir	No	String	Sorting order. The returned certificates are listed by parameter sort_key. The options are as follows: • ASC: ascending order • DESC: descending order Default: DESC Minimum: 0 Maximum: 32
sort_key	No	String	Sorting criteria. The options are as follows: • certExpiredTime: Certificate expiration time. • certStatus: certificate status • certUpdateTime: Certificate update time. Default: certUpdateTime Minimum: 0 Maximum: 64

Parameter	Mandatory	Type	Description
status	No	String	Certificate status. The options are as follows: -ALL: All certificate statuses. • PAID: The certificate has been paid and needs to be applied for from the CA. • ISSUED: The certificate has been issued. • CHECKING: The certificate application is being reviewed. • CANCELCHECKING: The certificate application cancellation is being reviewed. • UNPASSED: The certificate application fails. • EXPIRED: The certificate has expired. • REVOKING: The certificate revocation application is being reviewed. • REVOKED: The certificate has been revoked. • UPLOAD: The certificate is being managed. • CHECKING_ORG: The organization verification is to be completed. • ISSUING: The certificate is to be issued. • SUPPLEMENTCHECKING: Additional domain names to be added for a multi-domain certificate are being reviewed. Default: ALL Minimum: 0 Maximum: 64

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. If the enterprise project function is not enabled, you do not need to set this parameter. If the enterprise project function is enabled, you can set this parameter when querying a resource. If this parameter is not specified, the system searches for the required resource in all the enterprise projects that you have permissions for. In this case, the value of enterprise_project_id is all. The parameter value must meet one of the following requirements: • The value is all. • The value is 0. • The value matches the <code>^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}\$</code> regular expression. Default: all Minimum: 0 Maximum: 64
deploy_support	No	Boolean	Whether to filter only certificates that can be deployed. Default: false
owned_by_self	No	Boolean	Whether the resource belongs to the current tenant. The options are as follows: • true: Only resources that belong to the current tenant are queried, excluding shared resources. • false: Query the current tenant and the resources shared with the tenant. Default: true

Parameter	Mandatory	Type	Description
expired_days_since	No	Integer	The certificate is within the validity period and expires in a maximum of xx days. Minimum: 0 Maximum: 1095 Default: 0

Request Parameters

Table 4-23 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Response Parameters

Status code: 200

Table 4-24 Response body parameters

Parameter	Type	Description
certificates	Array of CertificateDetail objects	For details, see data structure description of the CertificateDetail field. Array Length: 0 - 1000
total_count	Integer	Number of certificates. Minimum: 0 Maximum: 10000

Table 4-25 CertificateDetail

Parameter	Type	Description
id	String	Certificate ID. Minimum: 16 Maximum: 16
name	String	Certificate name. Maximum: 63 Minimum: 3
domain	String	Domain name bound to a certificate. Minimum: 1 Maximum: 255
sans	String	Additional domain name bound to a multi-domain certificate. Minimum: 1 Maximum: 4096
signature_algorithm	String	Signature algorithm. Minimum: 0 Maximum: 64
deploy_support	Boolean	Whether deployment is supported.
type	String	Certificate type. The options are: DV_SSL_CERT, DV_SSL_CERT_BASIC, EV_SSL_CERT, EV_SSL_CERT_PRO, OV_SSL_CERT, or OV_SSL_CERT_PRO Minimum: 1 Maximum: 128
brand	String	Certificate authority. The value can be GLOBALSIGN, SYMANTEC, GEOTRUST or CFCA. Minimum: 1 Maximum: 255
expire_time	String	Certificate expiration time. Minimum: 1 Maximum: 32

Parameter	Type	Description
domain_type	String	Zone type. The options are: • SINGLE_DOMAIN: Single domain names • WILDCARD: Wildcard domain names • MULTI_DOMAIN: Multiple domain names Minimum: 1 Maximum: 128
validity_period	Integer	Certificate validity period, in months. [CCM provides a solution for purchasing certificates with a multi-year validity period. This multi-year certificate takes effect by adding multiple SSL certificates with a validity period of one year. For example, a certificate with three years' validity period contains three SSL certificates with one-year validity period and the same specifications. The system automatically applies for a second certificate based on the information about the first certificate 30 days before the first certificate expires.] (tag:hws) Minimum: 12 Maximum: 12

Parameter	Type	Description
status	String	Certificate status. The options are as follows: • PAID: The certificate has been paid and needs to be applied for from the CA. • ISSUED: The certificate has been issued. • CHECKING: The certificate application is being reviewed. • CANCELCHECKING: The certificate application cancellation is being reviewed. • UNPASSED: The certificate application fails. • EXPIRED: The certificate has expired. • REVOKING: The certificate revocation application is being reviewed. • CANCLEREVOKING: The cancellation on certificate revocation is being reviewed. • REVOKED: The certificate has been revoked. • UPLOAD: The certificate is being managed. • SUPPLEMENTCHECKING: Additional domain names to be added for a multi-domain certificate are being reviewed. • CANCELSUPPLEMENTING: The cancellation on additional domain names to be added is being reviewed. Minimum: 0 Maximum: 64
domain_count	Integer	Number of domain names can be bound to a certificate. Minimum: 1 Maximum: 100

Parameter	Type	Description
wildcard_count	Integer	Number of wildcard domain names can be bound to a certificate. Minimum: 0 Maximum: 100
description	String	Certificate description Minimum: 0 Maximum: 255
domain_id	String	Account ID. Minimum: 0 Maximum: 100
enterprise_project_id	String	Enterprise project ID. The default value is 0 . For users who have enabled the enterprise project function, this value indicates that resources are in the default enterprise project. For users who have not enabled the enterprise project function, this value indicates that resources are not in the default enterprise project. Minimum: 0 Maximum: 36

Status code: 401**Table 4-26** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403

Table 4-27 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500**Table 4-28** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

None

Example Responses

Status code: 200

Normal return.

```
{
  "certificates" : [ {
    "id" : "scs1554192131150",
    "name" : "test",
    "domain" : "www.zx.com",
    "sans" : "a.zx.com;b.zx.com",
    "type" : "OV_SSL_CERT",
    "deploy_support" : true,
    "signature_algorithm" : "SHA256WITHRSA",
    "brand" : "GEOTRUST",
    "expire_time" : "2021-05-27 16:46:25.0",
    "domain_type" : "MULTI_DOMAIN",
```

```
"validity_period" : 12,  
"status" : "ISSUED",  
"domain_count" : 2,  
"wildcard_count" : 0,  
"description" : null  
}],  
"total_count" : 1  
}
```

Status code: 401

Authentication failed.

```
{  
  "error_code" : "SCM.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 403

Access denied.

```
{  
  "error_code" : "SCM.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{  
  "error_code" : "SCM.XXX",  
  "error_msg" : "XXX"  
}
```

Status Codes

Status Code	Description
200	Normal return.
401	Authentication failed.
403	Access denied.
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.1.3.2 Importing a Certificate

Function

Import a certificate to CCM.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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

POST /v3/scm/certificates/import

Request Parameters

Table 4-29 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Table 4-30 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Certificate name. Enter a string of 3 to 63 characters. Only letters, numbers, underscores (_), hyphens (-), and periods (.) are allowed. Minimum: 3 Maximum: 63

Parameter	Mandatory	Type	Description
certificate	Yes	String	Certificate content, which can be an intermediate certificate or a root certificate. If the certificate_chain field is transferred to the certificate chain, this field is set to the certificate. Use the escape character \n or \r\n to replace carriage return and line feed characters. Minimum: 0 Maximum: 4096
certificate_chain	No	String	Certificate chain, which is optional and can be transferred through the certificate field. Use the escape character \n or \r\n to replace carriage return and line feed characters. Minimum: 0 Maximum: 8192
private_key	Yes	String	Private key of a certificate. The private key protected by password cannot be uploaded. The carriage return character must be replaced with the escape character \n or \r\n. Minimum: 0 Maximum: 4096
duplicate_check	No	Boolean	Whether the same certificate can be uploaded. • true: The same certificate can be uploaded. • false: disagree

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. If the enterprise project function is not enabled, you do not need to set this parameter. If the enterprise project function is enabled, you can set this parameter when querying a resource. If this parameter is not specified, the system searches for the required resource in all the enterprise projects that you have permissions for. In this case, the value of enterprise_project_id is all. The parameter value must meet one of the following requirements: • The value is all. • The value is 0. • The value matches the <code>^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}\$</code> regular expression. Minimum: 0 Maximum: 64
enc_certificate	No	String	(Optional) The content of an SM encryption certificate. Use the escape character <code>\n</code> or <code>\r</code> to replace carriage return and line feed characters. Minimum: 0 Maximum: 4096
enc_private_key	No	String	(Optional) Private key of an SM encryption certificate. The private key protected by password cannot be uploaded. The carriage return character must be replaced with the escape character <code>\n</code> or <code>\r</code>. Minimum: 0 Maximum: 4096

Response Parameters

Status code: 200

Table 4-31 Response body parameters

Parameter	Type	Description
certificate_id	String	Certificate ID. Minimum: 16 Maximum: 16

Status code: 401

Table 4-32 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403

Table 4-33 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500

Table 4-34 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

```
{
  "name" : "test_cert",
  "certificate" : "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----BEGIN CERTIFICATE-----
*****-----END CERTIFICATE-----",
  "private_key" : "-----BEGIN RSA PRIVATE KEY-----*****-----END RSA PRIVATE KEY-----"
}
```

Example Responses

Status code: 200

Normal return.

```
{
  "certificate_id" : "scs1600313391074"
}
```

Status code: 401

Authentication failed.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Access denied.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Normal return.
401	Authentication failed.
403	Access denied.
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.1.3.3 Obtaining Details of a Certificate

Function

This API is used to query details about a certificate.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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 /v3/scm/certificates/{certificate_id}

Table 4-35 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Certificate ID. Minimum: 16 Maximum: 16

Request Parameters

Table 4-36 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Response Parameters

Status code: 200

Table 4-37 Response body parameters

Parameter	Type	Description
id	String	Certificate ID. Minimum: 16 Maximum: 16

Parameter	Type	Description
status	String	Certificate status. The options are: • PAID: The certificate has been paid and needs to be applied for from the CA. • ISSUED: The certificate has been issued. • CHECKING: The certificate application is being reviewed. • CANCELCHECKING: The certificate application cancellation is being reviewed. • UNPASSED: The certificate application fails. • EXPIRED: The certificate has expired. • REVOKING: The certificate revocation application is being reviewed. • REVOKED: The certificate has been revoked. • UPLOAD: The certificate is being managed. • SUPPLEMENTCHECKING: Additional domain names to be added for a multi-domain certificate are being reviewed. • CANCELSUPPLEMENTING: The cancellation on additional domain names to be added is being reviewed. Minimum: 0 Maximum: 32
order_id	String	Order ID. Minimum: 0 Maximum: 63
name	String	Certificate name. Minimum: 3 Maximum: 63

Parameter	Type	Description
type	String	Certificate type. The options are: DV_SSL_CERT , DV_SSL_CERT_BASIC , EV_SSL_CERT , EV_SSL_CERT_PRO , OV_SSL_CERT , or OV_SSL_CERT_PRO Minimum: 0 Maximum: 32
brand	String	Certificate authority. The options are: GLOBALSIGN , SYMANTEC , GEOTRUST , or CFCA Minimum: 0 Maximum: 32
push_support	String	Whether a certificate can be pushed. Minimum: 0 Maximum: 32
revoke_reason	String	Reason for certificate revocation. Minimum: 0 Maximum: 255
signature_algorithm	String	Signature algorithm. Minimum: 0 Maximum: 64
issue_time	String	Time when the certificate was issued. If no valid value is obtained, this parameter is left blank. Minimum: 0 Maximum: 32
not_before	String	Time when the certificate takes effect. If no valid value is obtained, this parameter is left blank. Minimum: 0 Maximum: 32
not_after	String	Time when the certificate becomes invalid. If no valid value is obtained, this parameter is left blank. Minimum: 0 Maximum: 32

Parameter	Type	Description
validity_period	Integer	Certificate validity period, in months. [CCM provides a solution for purchasing certificates with a multi-year validity period. This multi-year certificate takes effect by adding multiple SSL certificates with a validity period of one year. For example, a certificate with three years' validity period contains three SSL certificates with one-year validity period and the same specifications. The system automatically applies for a second certificate based on the information about the first certificate 30 days before the first certificate expires.] (tag:hws) Minimum: 12 Maximum: 12
validation_method	String	Domain ownership verification method. The value can be DNS, FILE, or EMAIL. Minimum: 0 Maximum: 32
domain_type	String	Domain name type. The options are as follows: • SINGLE_DOMAIN: Single domain names • WILDCARD: Wildcard domain names • MULTI_DOMAIN: Multiple domain names Minimum: 0 Maximum: 32
multi_domain_type	String	Multi-domain name type. The options are as follows: • primary_single: primary single domain name • primary_wildcard: primary wildcard domain name Minimum: 0 Maximum: 32

Parameter	Type	Description
domain	String	Domain name bound to a certificate. Minimum: 0 Maximum: 255
sans	String	Additional domain name associated with the certificate Minimum: 0 Maximum: 4096
domain_count	Integer	Number of domain names can be bound to a certificate. Minimum: 1 Maximum: 100
wildcard_count	Integer	Number of additional domain names can be bound to a certificate. Minimum: 0 Maximum: 99
fingerprint	String	SHA-1 certificate fingerprint Minimum: 40 Maximum: 40
shared	Boolean	Shared resource or not
application_info	application_info object	Certificate application information.
description	String	Certificate description. Minimum: 0 Maximum: 255
enterprise_project_id	String	Enterprise project ID. The default value is 0 . For users who have enabled the enterprise project function, this value indicates that resources are in the default enterprise project. For users who have not enabled the enterprise project function, this value indicates that resources are not in the default enterprise project. Minimum: 0 Maximum: 36

Parameter	Type	Description
authentication	Array of Authentication objects	Domain ownership verification information. For details, see data structure of the Authentication field. Array Length: 0 - 100

Table 4-38 application_info

Parameter	Type	Description
country	String	Country or region. Minimum: 0 Maximum: 255
company_name	String	Company name. Minimum: 0 Maximum: 255
company_province	String	State/Province Minimum: 0 Maximum: 255
company_city	String	City where a company is located. Minimum: 0 Maximum: 255
applicant_name	String	Applicant name. Minimum: 0 Maximum: 255
applicant_phone	String	Phone number of an applicant. Minimum: 0 Maximum: 255
applicant_email	String	Email of an applicant. Minimum: 0 Maximum: 255
contact_name	String	Name of a technical contact. Minimum: 0 Maximum: 255
contact_phone	String	Phone number of the technical contact. Minimum: 0 Maximum: 255

Parameter	Type	Description
contact_email	String	Email of a technical contact. Minimum: 0 Maximum: 255

Table 4-39 Authentication

Parameter	Type	Description
record_name	String	Name of a domain ownership verification value. Minimum: 0 Maximum: 255
record_type	String	Type of the domain name verification value. Minimum: 0 Maximum: 255
record_value	String	Domain verification value. Minimum: 0 Maximum: 255
domain	String	Domain name mapping to the verification value Minimum: 0 Maximum: 255

Status code: 401**Table 4-40** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403**Table 4-41** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500**Table 4-42** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

None

Example Responses**Status code: 200**

Normal return.

```
{
  "id" : "scs1590053258704",
  "order_id" : "CS20052117270N7V9",
  "name" : "scm-testing",
  "type" : "DV_SSL_CERT",
  "brand" : "SYMANTEC",
  "push_support" : "OFF",
  "revoke_reason" : null,
  "status" : "CHECKING_DOMAIN",
```

```
"signature_algorithm" : null,
"issue_time" : null,
"not_before" : null,
"not_after" : null,
"validity_period" : 12,
"validation_method" : "DNS",
"domain_type" : "SINGLE_DOMAIN",
"multi_domain_type" : null,
"domain" : "hosting-*****.test.cn",
"sans" : null,
"domain_count" : 1,
"wildcard_count" : 0,
"fingerprint" : "185d687de3f44f2249d0e0f084efccb56b7c2cbe",
"enterprise_project_id" : "0",
"authentication" : [ {
  "record_name" : "_dnsauth.hosting-****.test.cn",
  "record_type" : "TXT",
  "record_value" : "201801040000001ytm4q*****cd8p7eg9ktlwfsord",
  "domain" : "hosting-*****.test.cn"
} ]
}
```

Status code: 401

Authentication failed.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Access denied.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Normal return.
401	Authentication failed.
403	Access denied.
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.1.3.4 Deleting a Certificate

Function

This API is used to delete a certificate from Huawei Cloud.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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 /v3/scm/certificates/{certificate_id}

Table 4-43 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Certificate ID. Minimum: 16 Maximum: 16

Request Parameters

Table 4-44 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Response Parameters

Status code: 204

Normal return.

Status code: 401

Table 4-45 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403

Table 4-46 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500

Table 4-47 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

None

Example Responses

Status code: 401

Authentication failed.

```
{  
  "error_code" : "SCM.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 403

Access denied.

```
{  
  "error_code" : "SCM.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{  
  "error_code" : "SCM.XXX",  
  "error_msg" : "XXX"  
}
```

Status Codes

Status Code	Description
204	Normal return.
401	Authentication failed.
403	Access denied.

Status Code	Description
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.1.3.5 Exporting a Certificate

Function

This API is used to export a certificate.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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

POST /v3/scm/certificates/{certificate_id}/export

Table 4-48 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Certificate ID. Minimum: 16 Maximum: 16

Request Parameters

Table 4-49 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Response Parameters

Status code: 200**Table 4-50** Response body parameters

Parameter	Type	Description
entire_certificate	String	Certificate and certificate chain. Minimum: 1 Maximum: 12288
certificate	String	Certificate content, excluding the certificate chain. Minimum: 1 Maximum: 4096
certificate_chain	String	Certificate chain Minimum: 1 Maximum: 8192
private_key	String	Private key of a certificate Minimum: 1 Maximum: 4096
enc_certificate	String	Encryption certificate content Minimum: 1 Maximum: 4096

Parameter	Type	Description
enc_private_key	String	Encryption certificate private key. • Method of self-generating CSR files: This field is encrypted and needs to be decrypted. • Method of Non-self-generated CSR files: This field does not need to be decrypted. The decryption process is as follows: 1. Obtain the symmetric key ciphertext and encrypted private key ciphertext from digital envelope. 2. Use the signature private key to decrypt the symmetric key ciphertext to obtain the symmetric key plaintext. 3. Use the symmetric key to decrypt the encrypted private key ciphertext to obtain the encrypted private key plaintext. Minimum: 1 Maximum: 4096

Status code: 401**Table 4-51** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403

Table 4-52 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500**Table 4-53** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

None

Example Responses

Status code: 200

Normal return.

```
{
  "entire_certificate" : "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----BEGIN CERTIFICATE-----
*****-----END CERTIFICATE-----",
  "certificate" : "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----",
  "certificate_chain" : "-----BEGIN CERTIFICATE-----*****-----END CERTIFICATE-----",
  "private_key" : "-----BEGIN RSA PRIVATE KEY-----*****-----END RSA PRIVATE KEY-----"
}
```

Status code: 401

Authentication failed.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Access denied.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Normal return.
401	Authentication failed.
403	Access denied.
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.1.4 Certificate Deployment Management

4.1.4.1 Pushing a Certificate

Function

This API is used to push an SSL certificate to another HUAWEI CLOUD service, such as Elastic Load Balance (ELB), Web Application Firewall (WAF), and Content Delivery Network (CDN).

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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

POST /v3/scm/certificates/{certificate_id}/push

Table 4-54 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Certificate ID. Minimum: 16 Maximum: 16

Request Parameters

Table 4-55 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Table 4-56 Request body parameters

Parameter	Mandatory	Type	Description
target_project	Yes	String	Region where the service you want to push a certificate to is deployed. Minimum: 1 Maximum: 255

Parameter	Mandatory	Type	Description
target_service	Yes	String	Service to which the certificate is pushed. Currently, certificates can only be pushed to CDN, WAF, and ELB. Minimum: 1 Maximum: 64

Response Parameters

Status code: 204

Normal return.

Status code: 401

Table 4-57 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403

Table 4-58 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500**Table 4-59** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

```
{
  "target_service" : "waf",
  "target_project" : "cn-north-7"
}
```

Example Responses**Status code: 401**

Authentication failed.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Access denied.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Normal return.
401	Authentication failed.
403	Access denied.
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.1.4.2 Pushing Certificates in Batches

Function

This API is used to push an SSL certificate to another Huawei Cloud service in batches, such as Elastic Load Balance (ELB), Web Application Firewall (WAF), and Content Delivery Network (CDN).

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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

POST /v3/scm/certificates/{certificate_id}/batch-push

Table 4-60 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Certificate ID. Minimum: 16 Maximum: 16

Request Parameters

Table 4-61 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Table 4-62 Request body parameters

Parameter	Mandatory	Type	Description
target_projects	Yes	Array of strings	Region where the service you want to push a certificate to is deployed, for example, CDN, ELB, or WAF. Minimum: 1 Maximum: 32 Array Length: 1 - 10
target_service	Yes	String	Service to which the certificate is pushed. Currently, certificates can only be pushed to CDN, WAF, and ELB. Minimum: 1 Maximum: 64

Response Parameters

Status code: 200

Table 4-63 Response body parameters

Parameter	Type	Description
results	Array of results objects	Deployment result Array Length: 1 - 10

Table 4-64 results

Parameter	Type	Description
project_name	String	Region name, for example, cn-north-7. Minimum: 0 Maximum: 63
cert_id	String	Certificate ID. Minimum: 0 Maximum: 255
message	String	Push result. Minimum: 0 Maximum: 255

Status code: 401**Table 4-65** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403**Table 4-66** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500

Table 4-67 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

```
{
  "target_service": "waf",
  "target_projects": [ "cn-north-7" ]
}
```

Example Responses

Status code: 200

Normal response.

```
{
  "results": [ {
    "project_name": "cn-north-7",
    "cert_id": "scs16751254852691",
    "message": "success"
  } ]
}
```

Status code: 401

Authentication failed.

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

Status code: 403

Access denied.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{
  "error_code" : "SCM.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Normal response.
401	Authentication failed.
403	Access denied.
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.1.4.3 Deploying Certificates

Function

This API is used to deploy an SSL certificate to another Huawei Cloud service, such as Elastic Load Balance (ELB), Web Application Firewall (WAF), and Content Delivery Network (CDN).

Constraints

- Upload a certificate and a test certificate with a validity period of three months. For other cloud services, the deployment fee is CNY30/domain.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

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

POST /v3/scm/certificates/{certificate_id}/deploy

Table 4-68 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	Certificate ID. Minimum: 16 Maximum: 16

Request Parameters

Table 4-69 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It can be obtained by calling the IAM API. The value of X-Subject-Token in the response header is the user token. Minimum: 32 Maximum: 2097152

Table 4-70 Request body parameters

Parameter	Mandatory	Type	Description
project_name	No	String	Name of the project where the resource to be deployed is located. If the resource is deployed in the main project, the value is the region ID. Minimum: 1 Maximum: 255

Parameter	Mandatory	Type	Description
service_name	Yes	String	Service to which the certificate is pushed. Currently, certificates can only be pushed to CDN, WAF, and ELB. Minimum: 1 Maximum: 64
resources	Yes	Array of DeployedResource objects	List of resources to be deployed. Array Length: 1 - 20

Table 4-71 DeployedResource

Parameter	Mandatory	Type	Description
id	No	String	Resource ID. This parameter is mandatory when WAF or ELB is deployed. Minimum: 0 Maximum: 63
type	No	String	Resource type. Currently, this parameter is required only when WAF resources are deployed. The value can be cloud for cloud mode or premium for dedicated mode. Minimum: 0 Maximum: 63
domain_name	No	String	Domain name to be deployed. Currently, this parameter is required only when CDN is deployed, that is, the domain name to be accelerated. The domain name must match the certificate. Minimum: 0 Maximum: 63

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	ID of the enterprise project to which the resource to be deployed belongs. This parameter is mandatory only when WAF resources are deployed. Minimum: 0 Maximum: 63

Response Parameters

Status code: 200

Table 4-72 Response body parameters

Parameter	Type	Description
failure_list	Array of FailureResource objects	List of resources that fail to be deployed. Array Length: 1 - 20

Table 4-73 FailureResource

Parameter	Type	Description
resource	String	Information about the resource that fails to be deployed. When WAF or ELB is deployed, this field is the resource ID. When CDN is deployed, this field is the acceleration domain name. Minimum: 0 Maximum: 63
failure_info	String	Failure cause, which is generally the error code returned by the target service. Minimum: 0 Maximum: 255

Status code: 401

Table 4-74 Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 403**Table 4-75** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Status code: 500**Table 4-76** Response body parameters

Parameter	Type	Description
error_code	String	Error code returned for an error request. Minimum: 3 Maximum: 36
error_msg	String	Error information returned for an error request. Minimum: 0 Maximum: 1024

Example Requests

```
{
  "service_name": "ELB",
  "project_name": "cn-north-7",
  "resources": [ {
    "id": "982b8a6a6ebc43809d82a46ca99aaeb7"
  } ]
}
```

Example Responses

Status code: 200

Normal response.

```
{
  "failure_list": [ {
    "resource": "982b8a6a6ebc43809d82a46ca99aaeb7",
    "failure_info": "ELB.8904:certificate 982b8a6a6ebc43809d82a46ca99aaeb7 does not exist"
  } ]
}
```

Status code: 401

Authentication failed.

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

Status code: 403

Access denied.

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

Status code: 500

Failed to complete the request because of an internal server error.

```
{
  "error_code": "SCM.XXX",
  "error_msg": "XXX"
}
```

Status Codes

Status Code	Description
200	Normal response.
401	Authentication failed.
403	Access denied.
404	Access page not found.
500	Failed to complete the request because of an internal server error.

Error Codes

See [Error Codes](#).

4.2 Managing Private Certificates

4.2.1 Private CA Management

4.2.1.1 Querying the CA List

Function

This API is used to query the CA list.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:list	List	ca *	-	-	-
		-	g:EnterpriseProjectId		

URI

GET /v1/private-certificate-authorities

Table 4-77 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	The number of returned records. The default value is 10 . Minimum: 0 Maximum: 1000
name	No	String	The CA certificate name (CN) filter. This parameter is used to obtain the set of CA certificates whose names contain a specific value. Minimum: 1 Maximum: 64
offset	No	Integer	Index position. The query starts from the next record indexed by this parameter. The default value is 0 . Minimum: 0
status	No	String	The CA certificate status. You can search CA certificates by status. ● PENDING: The CA certificate is not activated. The CA cannot issue certificates. ● ACTIVED: The CA certificate has been activated. You can use the CA to issue certificates. ● DISABLED: The CA certificate is disabled. The CA cannot issue certificates. ● DELETED: The CA certificate is to be deleted as scheduled. In this state, the CA cannot issue certificates. ● EXPIRED: The CA certificate has expired. An expired CA cannot issue certificates.
type	No	String	CA certificate types: ● ROOT: root CA certificate ● SUBORDINATE: subordinate CA certificate

Parameter	Mandatory	Type	Description
sort_key	No	String	Sorting attribute. The following attributes are available now: • create_time: certificate creation time (default) • common_name: certificate name • type: CA certificate type • not_after: certificate expiration time
sort_dir	No	String	Sorting sequence. The options are as follows: • DESC: descending order (default) • ASC: ascending order
owned_by_self	No	Boolean	Whether the resource belongs to the current tenant. The options are as follows: • true: Only the resources that belong to the current tenant are queried, excluding shared resources. • false: Resources of the current tenant and resources shared to the tenant are queried. Default: true Minimum: 0 Maximum: 64

Request Parameters

Table 4-78 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-79 Response body parameters

Parameter	Type	Description
total	Integer	Total number of CA certificates
certificate_authorities	Array of CertificateAuthorities objects	The CA list. For details, see data structure for the CertificateAuthorities field.

Table 4-80 CertificateAuthorities

Parameter	Type	Description
ca_id	String	ID of the CA certificate Minimum: 36 Maximum: 36
type	String	The CA type can be: • ROOT: root CA • SUBORDINATE: subordinate CA
status	String	CA certificate status: • PENDING: The CA certificate is not activated. The CA cannot issue certificates. • ACTIVED: The CA certificate has been activated. You can use the CA to issue certificates. • DISABLED: The CA certificate is disabled. The CA cannot issue certificates. • DELETED: The CA certificate is to be deleted as scheduled. In this state, the CA cannot issue certificates. • EXPIRED: The CA certificate has expired. An expired CA cannot issue certificates.

Parameter	Type	Description
path_length	Integer	CA path length. NOTE Note: The path length of the generated root CA certificate is not limited, but this field is set to 7 in the database. The path length of a subordinate CA is specified by you when you create subordinate CA. The default value is 0 . Minimum: 0 Maximum: 6
issuer_id	String	The ID of the CA certificate that issues the certificate. For a root CA, the value of this parameter is null . Minimum: 36 Maximum: 36
issuer_name	String	The name of the parent CA certificate. For a root CA, the value of this parameter is null . Minimum: 1 Maximum: 64
key_algorithm	String	Key algorithm
signature_algorithm	String	Signature hash algorithm.
freeze_flag	Integer	Freezing tag: • 0: non-frozen • Other values: frozen state. This is currently reserved.
gen_mode	String	Certificate generation method. • GENERATE: generated by the PCA system. • IMPORT: imported externally. • CSR: issued by an internal CA with CSRs imported externally. This means the private key is not managed by PCA.
serial_number	String	Serial number of the certificate. Minimum: 1 Maximum: 64
create_time	Long	Time the certificate was created. The value is a timestamp in milliseconds.

Parameter	Type	Description
delete_time	Long	Time the certificate was deleted. The value is a timestamp in milliseconds.
not_before	Long	Time the certificate was created. The value is a timestamp in milliseconds.
not_after	Long	Time the certificate expires. The value is a timestamp in milliseconds.
distinguished_name	DistinguishedName object	Certificate name. For details, see data structure for the DistinguishedName field.
crl_configuration	ListCrlConfiguration object	Certificate CRL. For details, see data structure for the ListCrlConfiguration field.
enterprise_project_id	String	Enterprise project ID. The default value is 0 . For users who have enabled the enterprise project function, this value indicates that resources are in the default enterprise project. For users who have not enabled the enterprise project function, this value indicates that resources are not in the default enterprise project.
free_quota	Integer	Free certificate quota.
charging_mode	Integer	Billing mode. The value can be: • 0: yearly/monthly • 1: pay-per-use
cluster_id	String	DHSM cluster ID. Minimum: 1 Maximum: 64
domain_id	String	Account ID. Minimum: 0 Maximum: 100

Table 4-81 DistinguishedName

Parameter	Type	Description
common_name	String	Common name (CN) of a certificate. The value can contain a maximum of 64 characters, including only letters, digits, spaces, Chinese characters, hyphens (-), underscores (_), periods (.), commas (,), and asterisks (*). Minimum: 1 Maximum: 64
country	String	Country code. The value is a string of two characters and can contain only letters. Minimum: 2 Maximum: 2
state	String	Name of a province or city. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
locality	String	Region name. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
organization	String	Organization name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64

Parameter	Type	Description
organizational_unit	String	Organization unit name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64

Table 4-82 ListCrlConfiguration

Parameter	Type	Description
enabled	Boolean	Whether to enable the gray release function of CRL. • true • false
crl_name	String	Name of the certificate revocation list. NOTE If you do not specify this parameter, the system uses the ID of the parent CA that issues the current certificate by default.
obs_bucket_name	String	OBS bucket name.
valid_days	Integer	CRL update interval, in days. This parameter is mandatory when the CRL release function is enabled. Minimum: 7 Maximum: 30
crl_dis_point	String	The address of the CRL file in the OBS bucket. NOTE This parameter is composed of crl_name , ** obs_bucket_name** , and OBS address.

Status code: 400

Table 4-83 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-84** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-85** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-86 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-87** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you use this API to query the CA certificate list, a token is required in the **X-Auth-Token** field in the request header. The token must have the permission to access the API.

```
GET https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 2,
  "certificate_authorities" : [ {
    "signature_algorithm" : "SHA384",
    "issuer_id" : null,
    "issuer_name" : null,
    "not_after" : 1678159435000,
    "not_before" : 1646623375000,
    "status" : "ACTIVED",
    "freeze_flag" : 0,
    "gen_mode" : "GENERATE",
    "serial_number" : "202203070322544291829058",
```

```
"distinguished_name" : {
  "country" : "cn",
  "state" : "shanghai",
  "locality" : "shanghai",
  "organization" : "shanghai",
  "organizational_unit" : "shanghai",
  "common_name" : "CSR_123"
},
"key_algorithm" : "EC384",
"create_time" : 1646623375000,
"delete_time" : null,
"ca_id" : "a6bbf0be-79f3-4f66-858a-0fdb96dfcbe",
"type" : "ROOT",
"path_length" : 7,
"crl_configuration" : {
  "enabled" : false,
  "obs_bucket_name" : null,
  "valid_days" : null,
  "crl_name" : null,
  "crl_dis_point" : null
}
}, {
  "signature_algorithm" : "SHA256",
  "issuer_id" : null,
  "issuer_name" : null,
  "not_after" : 1727492412000,
  "not_before" : 1632797952000,
  "status" : "ACTIVED",
  "freeze_flag" : 0,
  "gen_mode" : "GENERATE",
  "serial_number" : "202109280259122080649087",
  "distinguished_name" : {
    "country" : "CN",
    "state" : "Sichuan",
    "locality" : "Chengdu",
    "organization" : "Huawei",
    "organizational_unit" : "CloudBU",
    "common_name" : "pca-ca"
  },
  "key_algorithm" : "RSA2048",
  "create_time" : 1632797953000,
  "delete_time" : null,
  "ca_id" : "fb7bd6a6-6a11-4a58-8710-a3c0a620aedc",
  "type" : "ROOT",
  "path_length" : 7,
  "crl_configuration" : {
    "enabled" : false,
    "obs_bucket_name" : null,
    "valid_days" : null,
    "crl_name" : null,
    "crl_dis_point" : null
  }
}
}]
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
```

```
"error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.2 Creating a CA

Function

There are three methods to create CAs.

- Creating a root CA: All mandatory parameters must be specified.
- Creating a subordinate CA and activating the certificate: All mandatory parameters must be specified.

- Creating a subordinate CA without activating it: The request body contains only **issuer_id**, **signature_algorithm**, or **validity**.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:create	Write	ca *	-	-	-
		-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v1/private-certificate-authorities

Request Parameters

Table 4-88 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-89 Request body parameters

Parameter	Mandatory	Type	Description
type	Yes	String	Type of the CA you want to create: • ROOT: root CA • SUBORDINATE: subordinate CA
distinguished_name	Yes	DistinguishedName object	Certificate name. For details, see data structure for the DistinguishedName field.
key_algorithm	Yes	String	Key algorithm. The options are as follows: • RSA2048: RSA algorithm. The key length is 2048 bits. • RSA4096: RSA algorithm. The key length is 4096 bits. • EC256: Elliptic Curve Digital Signature Algorithm (ECDSA). The key length is 256 bits. • EC384: Elliptic Curve Digital Signature Algorithm (ECDSA). The key length is 384 bits. • SM2: Elliptic curve algorithm (signature hash algorithm SM3) issued by the China State Cryptography Administration. The key length is 256 bits. (Huawei Cloud Chinese Mainland website)

Parameter	Mandatory	Type	Description
validity	No	Validity object	Validity period of a certificate. The options are as follows: • This parameter is mandatory when you create a root CA. • This parameter is mandatory when you create and activate a subordinate CA. • This parameter can be ignored when you create a subordinate CA but do not activate it. However, you still need to specify this parameter when you activate the subordinate CA later. NOTE For details, see data structure description of the Validity field.
hsm_cluster_info	No	HsmClusterInfo object	HSM cluster information. This method can be used to encrypt CA only for users in the whitelist. For details, see HsmClusterInfo field description.

Parameter	Mandatory	Type	Description
issuer_id	No	String	ID of the parent CA. The options are as follows: • If you want to create a root CA, this parameter can be ignored. This is because a root CA is a self-signed certificate and has no parent CA. • If you want to create and activate a subordinate CA, this parameter is mandatory. • If you want to create a subordinate CA but do not activate it, this parameter can be ignored. However, you still need to specify this parameter when you activate the subordinate CA later. Minimum: 36 Maximum: 36

Parameter	Mandatory	Type	Description
path_length	No	Integer	Length of the CA certificate path. The options are as follows: • If you want to create a root CA, this parameter is not required by default. This means CA path length is not limited and you can expand the CA hierarchies. You can limit the CA hierarchy levels by subordinate CAs • If you want to create and activate a subordinate CA, this parameter is customizable. If you do not specify this parameter, 0 is used by default. • If you want to create a subordinate CA but do not activate it, this parameter can be ignored. You still need to specify this parameter when you activate the subordinate CA later. Minimum: 0 Maximum: 6

Parameter	Mandatory	Type	Description
signature_algorithm	No	String	Signature hash algorithm. • There are three cases: – If you want to create a root CA, this parameter is mandatory. – If you want to create a subordinate CA and activate it, this parameter is mandatory. – If you want to create a subordinate CA but not activate it immediately, this parameter is not required. You can specify this parameter when activating the subordinate CA. • The options are as follows: – SHA256 – SHA384 – SHA512 – SM3 (Chinese mainland website, SM2)

Parameter	Mandatory	Type	Description
key_usages	No	Array of strings	Key usage. For details, see [4.2.1.3] in RFC 5280 (https://datatracker.ietf.org/doc/html/rfc5280#section-4.2.1.3) • digitalSignature: used as digital signatures. • nonRepudiation: used for non-repudiation • keyEncipherment: used to encrypt key data. • dataEncipherment: used to encrypt data. • keyAgreement: used for key negotiation • keyCertSign: used to issue a certificate. • cRLSign: used to issue the revocation list. • encipherOnly: used only for encryption. • decipherOnly: used only for decryption. • The default values are as follows: NOTE • Root CA certificate: The default value is [digitalSignature, keyCertSign, cRLSign]. The value you specified will be ignored. • Subordinate CA certificate: The default value is [digitalSignature, keyCertSign, cRLSign]. You can customize the value.
crl_configuration	No	CrlConfiguration object	Certificate CRL. For details, see data structure for the CrlConfiguration field.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. If the enterprise project function is not enabled, you do not need to set this parameter. If the enterprise project function is enabled, you can set this parameter when querying a resource. If this parameter is not specified, the system searches for the required resource in all the enterprise projects that you have permissions for. In this case, the value of enterprise_project_id is all . The parameter value must meet one of the following requirements: Is all Is 0 Matches the regular expression <code>^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}\$</code> .
ca_id	No	String	ID of the CA certificate. If the value is empty, a pay-per-use CA is created. If the value is not empty, the yearly/monthly CA information is saved. Minimum: 36 Maximum: 36

Table 4-90 DistinguishedName

Parameter	Mandatory	Type	Description
common_name	Yes	String	Common name (CN) of a certificate. The value can contain a maximum of 64 characters, including only letters, digits, spaces, Chinese characters, hyphens (-), underscores (_), periods (.), commas (,), and asterisks (*). Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
country	Yes	String	Country code. The value is a string of two characters and can contain only letters. Minimum: 2 Maximum: 2
state	Yes	String	Name of a province or city. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
locality	Yes	String	Region name. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
organization	Yes	String	Organization name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64
organizational_unit	Yes	String	Organization unit name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64

Table 4-91 Validity

Parameter	Mandatory	Type	Description
type	Yes	String	Validity period type, which is mandatory. The options are as follows: • YEAR: by the year (12 months) • MONTH:by the month (31 days) • DAY: by the day • HOURL: by the hour
value	Yes	Integer	The certificate validity period. The value of this parameter varies depending on the value of type : • Root CAs: The validity period is less than or equal to 30 years. • Subordinate CAs and private certificates: The validity period is less than or equal to 20 years.
start_from	No	Integer	Start time. The options are as follows: • The format is a timestamp in milliseconds. For example, 1645146939688 indicates 2022-02-18 09:15:39. • The start time can begin no more than five minutes earlier than the current time. It means the value of start_from must be larger than the value of current_time minus 5 minutes.

Table 4-92 HsmClusterInfo

Parameter	Mandatory	Type	Description
hsm_project	Yes	String	Project information. For example, cn-north-7

Parameter	Mandatory	Type	Description
hsm_cluster_id	Yes	String	HSM cluster identifier. For example, 54d8301b-b859-4c55-a628-21cf90e609e
hsm_ca_cert	Yes	String	String following base64 of the certificate in PEM format • MXXXXX

Table 4-93 CrlConfiguration

Parameter	Mandatory	Type	Description
enabled	Yes	Boolean	Whether to enable the gray release function of CRL. • true • false
crl_name	No	String	Name of the certificate revocation list. NOTE If you do not specify this parameter, the system uses the ID of the parent CA that issues the current certificate by default.
obs_bucket_name	No	String	Specifies the OBS bucket name. NOTE To enable the CRL release function: • This parameter is mandatory. You must have created an agency and assigned PCA permissions on OBS to it. For details, see ** Certificate Revocation > Checking Permissions of an Agency ** and ** Certificate Revocation > Creating an Agency **. • The specified OBS bucket must exist. Otherwise, an error will be reported.
valid_days	No	Integer	CRL update interval, in days. This parameter is mandatory when the CRL release function is enabled. Minimum: 7 Maximum: 30

Response Parameters

Status code: 200

Table 4-94 Response body parameters

Parameter	Type	Description
ca_id	String	ID of the CA certificate being issued. Minimum: 36 Maximum: 36

Status code: 400

Table 4-95 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-96 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403

Table 4-97 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-98** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-99** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you use this API to create a CA certificate, a token is required in the **X-Auth-Token** field in the request header. The token must have the permission to access the API.

POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities

```
{
  "type": "ROOT",
  "key_algorithm": "RSA4096",
  "signature_algorithm": "SHA512",
  "distinguished_name": {
    "common_name": "demoRootRSA",
    "country": "CN",
    "locality": "chengdu",
    "organization": "HW",
    "organizational_unit": "dew",
    "state": "sichuan"
  },
  "validity": {
    "type": "YEAR",
    "value": 3
  },
  "crl_configuration": {
    "enabled": false,
    "obs_bucket_name": "demoBucket",
    "valid_days": 8
  }
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "ca_id": "66504812-fedc-414a-9b7c-4c1836398524"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code": "PCA.XXX",
}
```

```
"error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.3 Querying the CA Quota

Function

This API is used to query the CA quota.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:quota	Read	-	-	-	-

URI

GET /v1/private-certificate-authorities/quotas

Request Parameters

Table 4-100 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-101 Response body parameters

Parameter	Type	Description
quotas	Quotas object	Certificate quota. For details, see data structure for the Quotas field.

Table 4-102 Quotas

Parameter	Type	Description
resources	Array of Resources objects	Resource quota list. For details, see data structure for the Resources field. Array Length: 0 - 10

Table 4-103 Resources

Parameter	Type	Description
type	String	Certificate type. • CERTIFICATE_AUTHORITY: CA certificate. • CERTIFICATE: private certificate.
used	Integer	Used quota
quota	Integer	Total quota. • CERTIFICATE_AUTHORITY: 100 is specified in the current system. • CERTIFICATE: 100000 is specified in the current system.

Status code: 400**Table 4-104** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-105** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403

Table 4-106 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-107** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-108** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

GET <https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/quotas>

Example Responses

Status code: 200

Request succeeded.

```
{
  "quotas" : {
    "resources" : [ {
      "type" : "CERTIFICATE_AUTHORITY",
      "used" : 25,
      "quota" : 100
    } ]
  }
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```


Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.4 Querying CA Details

Function

This API is used to query details about a CA.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:get	Read	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

GET /v1/private-certificate-authorities/{ca_id}

Table 4-109 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the CA certificate Minimum: 36 Maximum: 36

Request Parameters

Table 4-110 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-111 Response body parameters

Parameter	Type	Description
ca_id	String	ID of the CA certificate Minimum: 36 Maximum: 36
type	String	The CA type can be: • ROOT: root CA • SUBORDINATE: subordinate CA

Parameter	Type	Description
status	String	CA certificate status: • PENDING: The CA certificate is not activated. The CA cannot issue certificates. • ACTIVED: The CA certificate has been activated. You can use the CA to issue certificates. • DISABLED: The CA certificate is disabled. The CA cannot issue certificates. • DELETED: The CA certificate is to be deleted as scheduled. In this state, the CA cannot issue certificates. • EXPIRED: The CA certificate has expired. An expired CA cannot issue certificates.
path_length	Integer	CA path length. NOTE Note: The path length of the generated root CA certificate is not limited, but this field is set to 7 in the database. The path length of a subordinate CA is specified by you when you create subordinate CA. The default value is 0 . Minimum: 0 Maximum: 6
issuer_id	String	The ID of the CA certificate that issues the certificate. For a root CA, the value of this parameter is null . Minimum: 36 Maximum: 36
issuer_name	String	The name of the parent CA certificate. For a root CA, the value of this parameter is null . Minimum: 1 Maximum: 64
key_algorithm	String	Key algorithm
signature_algorithm	String	Signature hash algorithm.

Parameter	Type	Description
freeze_flag	Integer	Freezing tag: • 0: non-frozen • Other values: frozen state. This is currently reserved.
gen_mode	String	Certificate generation method. • GENERATE: generated by the PCA system. • IMPORT: imported externally. • CSR: issued by an internal CA with CSRs imported externally. This means the private key is not managed by PCA.
serial_number	String	Serial number of the certificate. Minimum: 1 Maximum: 64
create_time	Long	Time the certificate was created. The value is a timestamp in milliseconds.
delete_time	Long	Time the certificate was deleted. The value is a timestamp in milliseconds.
not_before	Long	Time the certificate was created. The value is a timestamp in milliseconds.
not_after	Long	Time the certificate expires. The value is a timestamp in milliseconds.
distinguished_name	DistinguishedName object	Certificate name. For details, see data structure for the DistinguishedName field.
crl_configuration	ListCrlConfiguration object	Certificate CRL. For details, see data structure for the ListCrlConfiguration field.
enterprise_project_id	String	Enterprise project ID. The default value is 0 . For users who have enabled the enterprise project function, this value indicates that resources are in the default enterprise project. For users who have not enabled the enterprise project function, this value indicates that resources are not in the default enterprise project.
free_quota	Integer	Free certificate quota.

Parameter	Type	Description
charging_mode	Integer	Billing mode. The value can be: • 0: yearly/monthly • 1: pay-per-use
cluster_id	String	DHSM cluster ID. Minimum: 1 Maximum: 64
domain_id	String	Account ID. Minimum: 0 Maximum: 100

Table 4-112 DistinguishedName

Parameter	Type	Description
common_name	String	Common name (CN) of a certificate. The value can contain a maximum of 64 characters, including only letters, digits, spaces, Chinese characters, hyphens (-), underscores (_), periods (.), commas (,), and asterisks (*). Minimum: 1 Maximum: 64
country	String	Country code. The value is a string of two characters and can contain only letters. Minimum: 2 Maximum: 2
state	String	Name of a province or city. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128

Parameter	Type	Description
locality	String	Region name. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
organization	String	Organization name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64
organizational_unit	String	Organization unit name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64

Table 4-113 ListCrlConfiguration

Parameter	Type	Description
enabled	Boolean	Whether to enable the gray release function of CRL. • true • false
crl_name	String	Name of the certificate revocation list. NOTE If you do not specify this parameter, the system uses the ID of the parent CA that issues the current certificate by default.
obs_bucket_name	String	OBS bucket name.

Parameter	Type	Description
valid_days	Integer	CRL update interval, in days. This parameter is mandatory when the CRL release function is enabled. Minimum: 7 Maximum: 30
crl_dis_point	String	The address of the CRL file in the OBS bucket. NOTE This parameter is composed of crl_name , ** obs_bucket_name** , and OBS address.

Status code: 400**Table 4-114** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-115** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403

Table 4-116 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-117** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-118** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.


```
GET https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "signature_algorithm": "SHA384",
  "issuer_id": "928bd666-e879-448a-ab54-82f6ae3d81e0",
  "issuer_name": "Huawei IT Root CA",
  "not_after": 1647567892000,
  "not_before": 1645148632000,
  "status": "ACTIVED",
  "freeze_flag": 0,
  "gen_mode": "CSR",
  "serial_number": "202202180143522338893611",
  "distinguished_name": {
    "country": "CN",
    "state": "guangdong",
    "locality": "shenzhen",
    "organization": "Huawei",
    "organizational_unit": "IT",
    "common_name": "Huawei IT Root CA"
  },
  "key_algorithm": "RSA",
  "create_time": 1645148633000,
  "delete_time": null,
  "ca_id": "4c0e772e-a30c-4029-b929-b7acb04143f7",
  "type": "SUBORDINATE",
  "path_length": 0,
  "crl_configuration": {
    "enabled": false,
    "obs_bucket_name": null,
    "valid_days": null,
    "crl_name": null,
    "crl_dis_point": null
  },
  "cluster_id": "54d8301b-b859-4c55-a628-21cf90e609e"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.5 Deleting a Private CA

Function

This API is used to delete a CA as scheduled. The scheduled time range can be 7 to 30 days.

** NOTE**

Only the CAs in the **Pending activation** or **Disabled** status can be deleted. If the CA certificate is in the **Pending activation** status, the CA certificate will be deleted immediately. Scheduled deletion is not supported.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:delete	Write	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

DELETE /v1/private-certificate-authorities/{ca_id}

Table 4-119 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the CA certificate you plan to delete. Minimum: 36 Maximum: 36

Table 4-120 Query Parameters

Parameter	Mandatory	Type	Description
pending_days	No	String	Delayed deletion time, in days. If this parameter is not specified, the default value is 30. Minimum: 1 Maximum: 2

Request Parameters

Table 4-121 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400**Table 4-122** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-123** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-124** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-125** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-126** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
DELETE https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7?pending_days=7
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.

Status Code	Description
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.6 Activating a CA

Function

This API is used to activate a CA.

NOTE

You can activate a certificate only when it is in the **Pending activation** status.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:activate	Write	ca *	g:ResourceTag/<tag-key>	• pca:ca:active	-
		-	g:EnterpriseProjectId		

URI

POST /v1/private-certificate-authorities/{ca_id}/activate

Table 4-127 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the subordinate CA you want to activate. Minimum: 36 Maximum: 36

Request Parameters

Table 4-128 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-129 Request body parameters

Parameter	Mandatory	Type	Description
issuer_id	Yes	String	ID of the parent CA. Minimum: 1 Maximum: 64
path_length	No	Integer	Path length. Minimum: 0 Maximum: 6
signature_algorithm	Yes	String	Signature hash algorithm. The options are as follows: • SHA256 • SHA384 • SHA512 • SM3 (Huawei Cloud Chinese Mainland website)

Parameter	Mandatory	Type	Description
validity	Yes	Validity object	Certificate validity. For details, see data structure for the Validity field.
hsm_cluster_info	No	HsmClusterInfo object	HSM cluster information. This method can be used to encrypt CA only for users in the whitelist. For details, see HsmClusterInfo field description.
type	No	String	Type of the CA you want to create: (This parameter is mandatory if a yearly/monthly CA is activated.) • ROOT: root CA • SUBORDINATE: subordinate CA
distinguished_name	No	DistinguishedName object	Certificate name. For details, see data structure of the DistinguishedName field. (This parameter is mandatory if a yearly/monthly CA is activated.)

Parameter	Mandatory	Type	Description
key_algorithm	No	String	Key algorithm. This parameter is mandatory if a yearly/monthly CA is activated. The options are as follows: • RSA2048: RSA algorithm with the key length of 2048 bits • RSA4096: RSA algorithm with the key length of 4096 bits • EC256: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 256 bits • EC384: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 384 bits • SM2: An Elliptic Curve Digital Signature Algorithm (ECDSA) (signature hash algorithm SM3) issued by China State Cryptography Administration. The key length is 256 bits. (Chinese mainland website)

Parameter	Mandatory	Type	Description
key_usages	No	Array of strings	Key usage. For details, see [4.2.1.3] in RFC 5280 (https://datatracker.ietf.org/doc/html/rfc5280#section-4.2.1.3) • digitalSignature: The key can be used as a digital signature. • nonRepudiation: The key can be used for non-repudiation. • keyEncipherment: The key is used to encrypt key data. • dataEncipherment: The key is used to encrypt data. • keyAgreement: The key is used for key negotiation. • keyCertSign: The key can issue a certificate. • cRLSign: The key can issue a certificate revocation list (CRL). • encipherOnly: The key is used only for encryption. • decipherOnly: The key is used only for decryption. NOTE The default values are as follows: • Root CA certificates: [digitalSignature, keyCertSign, cRLSign], which cannot be changed. The value you specified is ignored. • Subordinate CA certificates: [digitalSignature, keyCertSign, cRLSign], which can be customized.
crl_configuration	No	CrlConfiguration object	Certificate CRL. For details, see data structure of the CrlConfiguration field.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. If the enterprise project function is not enabled, you do not need to set this parameter. If the enterprise project function is enabled, you can set this parameter when querying a resource. If this parameter is not specified, the system searches for the required resource in all the enterprise projects that you have permissions for. In this case, the value of enterprise_project_id is all. The parameter value must meet one of the following requirements: Is all Is 0 Matches the regular expression <code>^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}\$</code>.

Table 4-130 Validity

Parameter	Mandatory	Type	Description
type	Yes	String	Validity period type, which is mandatory. The options are as follows: ● YEAR: by the year (12 months) ● MONTH: by the month (31 days) ● DAY: by the day ● HOUR: by the hour

Parameter	Mandatory	Type	Description
value	Yes	Integer	The certificate validity period. The value of this parameter varies depending on the value of type : • Root CAs: The validity period is less than or equal to 30 years. • Subordinate CAs and private certificates: The validity period is less than or equal to 20 years.
start_from	No	Integer	Start time. The options are as follows: • The format is a timestamp in milliseconds. For example, 1645146939688 indicates 2022-02-18 09:15:39. • The start time can begin no more than five minutes earlier than the current time. It means the value of start_from must be larger than the value of current_time minus 5 minutes.

Table 4-131 HsmClusterInfo

Parameter	Mandatory	Type	Description
hsm_project	Yes	String	Project information. For example, cn-north-7
hsm_cluster_id	Yes	String	HSM cluster identifier. For example, 54d8301b-b859-4c55-a628-21fc90e609e
hsm_ca_cert	Yes	String	String following base64 of the certificate in PEM format • MXXXXX

Table 4-132 DistinguishedName

Parameter	Mandatory	Type	Description
common_name	Yes	String	Common name (CN) of a certificate. The value can contain a maximum of 64 characters, including only letters, digits, spaces, Chinese characters, hyphens (-), underscores (_), periods (.), commas (,), and asterisks (*). Minimum: 1 Maximum: 64
country	Yes	String	Country code. The value is a string of two characters and can contain only letters. Minimum: 2 Maximum: 2
state	Yes	String	Name of a province or city. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
locality	Yes	String	Region name. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
organization	Yes	String	Organization name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
organizational_unit	Yes	String	Organization unit name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64

Table 4-133 CrlConfiguration

Parameter	Mandatory	Type	Description
enabled	Yes	Boolean	Whether to enable the gray release function of CRL. • true • false
crl_name	No	String	Name of the certificate revocation list. NOTE If you do not specify this parameter, the system uses the ID of the parent CA that issues the current certificate by default.
obs_bucket_name	No	String	Specifies the OBS bucket name. NOTE To enable the CRL release function: • This parameter is mandatory. You must have created an agency and assigned PCA permissions on OBS to it. For details, see ** Certificate Revocation > Checking Permissions of an Agency ** and ** Certificate Revocation > Creating an Agency **. • The specified OBS bucket must exist. Otherwise, an error will be reported.

Parameter	Mandatory	Type	Description
valid_days	No	Integer	CRL update interval, in days. This parameter is mandatory when the CRL release function is enabled. Minimum: 7 Maximum: 30

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400

Table 4-134 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-135 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403

Table 4-136 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-137** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-138** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/activate
```

```
{
  "signature_algorithm" : "SHA256",
  "validity" : {
    "type" : "YEAR",
    "value" : 1
  },
  "path_length" : 3,
  "issuer_id" : "c718fe5f-d44a-467f-80f1-948348ff4132"
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.

Status Code	Description
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.7 Exporting a CSR of a CA

Function

This API is used to export a Certificate Signing Request (CSR) of a CA.

NOTE

A CSR can be exported only when the corresponding CA is in the **Pending activation** status.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:getCsr	Read	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

GET /v1/private-certificate-authorities/{ca_id}/csr

Table 4-139 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the subordinate CA that has not been activated. Minimum: 36 Maximum: 36

Request Parameters

Table 4-140 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-141 Response body parameters

Parameter	Type	Description
csr	String	Content of the CSR. The content varies depending on how you obtain the CSR: - If you use this API, newline characters in the exported CSR have been replaced by <code>\r\n</code>. - If you export the CSR through the console, the exported CSR is in PEM format. Minimum: 1 Maximum: 4096

Status code: 400

Table 4-142 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-143** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-144** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-145 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-146** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
GET https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/csr
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "csr" : "-----BEGIN CERTIFICATE REQUEST-----\r
\nMIIBUDCB2AIBADBZMRAwDgYDVQQDDADU1IsMTIzMQswCQYDVQQGEWJjbjERMA8G\r
\nA1UECAwlc2hhbmdoYWxkETAPBgNVBACMCHNoYW5naGFpMRIwEAYDVQQKDAZaGFu\r
\nZyxoYWkwZjAQBgcqhkJOPQIBBgUrgQQAIGNiAAQI9M7bK+vys5x9mnfG3783aPRh\r
\nP/xqLPKVsRsQniC3vPZvlz9E7SasMfZLrXVK37QWhtAETgNG7NrQnwiOye0/8VZL\r
\nVX7ildM6CZY4SUYSa6TBUsXyGjOs514fjxbuT6gADAKBggqhkJOPQQDAgNnADBk\r
\nr\nAjbIQiPXU7TDDDwxrh\r
\n+JfZEYgmr61clQdE5GMozPDYime30zcuMnVrb9i3o/2BW+\r
\nr\n0IECMG0QWbAYh0LoqnmAYqlgTKK8nKsxm0xFuTryfxynWi8BpCvAGx803Qpa8EJV\r
\nr\nJTJcw==\r\n\r\n-----\r
\nEND CERTIFICATE REQUEST-----"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.8 Disabling a Private CA

Function

This API is used to disable a private CA.

NOTE

You can disable a certificate only when it is in the **Activated** or **Expired** state.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:disable	Write	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

POST /v1/private-certificate-authorities/{ca_id}/disable

Table 4-147 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the CA certificate you want to disable. Minimum: 36 Maximum: 36

Request Parameters

Table 4-148 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400**Table 4-149** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-150** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-151** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-152** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-153** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/disable
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.

Status Code	Description
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.9 Enabling a Private CA

Function

This API is used to enable a private CA.

NOTE

Note: This operation is allowed only when the CA is in the **Disabled** status.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:enable	Write	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

POST /v1/private-certificate-authorities/{ca_id}/enable

Table 4-154 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the CA you want to enable. Minimum: 36 Maximum: 36

Request Parameters

Table 4-155 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400

Table 4-156 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-157 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-158** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-159** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-160 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/enable
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.10 Exporting a CA Certificate

Function

This API is used to export the CA certificate.

NOTE

Note: You can export a certificate only when it is in the **Activated** or **Expired** state.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:export	Read	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

POST /v1/private-certificate-authorities/{ca_id}/export

Table 4-161 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the CA certificate you want to export. Minimum: 36 Maximum: 36

Request Parameters

Table 4-162 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-163 Response body parameters

Parameter	Type	Description
certificate	String	Certificate content NOTE - If you use this API, newline characters in the exported certificate have been replaced by <code>\r\n</code>. - If you export the certificate through the console, the exported certificate is in PEM format. Minimum: 1 Maximum: 4096
certificate_chain	String	The content of the certificate chain. The sequence of the certificate chain (from top to bottom) is as follows: intermediate certificate >... > root certificate. NOTE - If you use this API, newline characters in the exported certificate chain have been replaced by <code>\r\n</code>. - If you export the certificate chain through the console, the exported certificate chain is in PEM format. Minimum: 1 Maximum: 2097152

Status code: 400**Table 4-164** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-165 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-166** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-167** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-168 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/export
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "certificate" : "-----BEGIN CERTIFICATE-----\r
\nMIIDCzCCAlugAwIBAgIKKsxpff9kUcq6dDANBgkqhkiG9w0BAQsFADBOMQowCAYD\r
\nVQQDDAE3MQswCQYDVQQGEwJDTjEQMA4GA1UECAwHU2ljaHVhbjEQMA4GA1UEBwwwH\r
\nQ2h1bmdkdTEPMA0GA1UECgwGSHVhd2VpMB4XDTEwMTAxNDA4NDMxMVoXDTIyMTAx\r
\nNDA4NDQxMVowPjELMAkGA1UEAwwCWVUxZCZAJBgNVBAYTAjEwMTAxMVoXDTIyMTAx\r
\nMQowCAYDVQQQHDAE0MQowCAYDVQQKDAE1MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8A\r
\nMIIBBgKCAQEANZy9vqhA711c/99INO80/uSXjoL1kEj1BtjVB7vqkDf0Ejs20A\r
\nnfQoHEVTuHams9XLvrlu\r
+YTw4QQ08hjbLl9mmerRRJK0pp+tBmCS3ZFoC23c5vz\r\nny+l0t+Yc2JYhvaO\r
Fr823Yo0WC2+NB065nIKH6/\r
duoONfD+3c5Ynkib0nBNyDV+DB\r\n\r\nhdKM0nrlqI07cNpYDWpfX5iDL+4Oh+kY1xGLZCO\r
bgsXl34zTf6E7bxJ1/\r
iDZjwJ\r\n\r\nndpf6OUQONmIcT49993YCrMDisjJ2OwW9e41S7D2xy/1xmPwWwnid1\r
WHOKTfK4cyl\r\n\r
2PhaHh3FTXIGYjVSg3yKfujauVOFpZ9bTwIDAQABo2MwYTAfBgNVHSMEGDAWgBTu\r
\r\nY36JXjwX7iLcwKtUto8RZa52DAdbgNVHQ4EFgQUyuAS2HonxOWDIPOgPIMFQ9rr\r
\r\nGiMwEgYDVROTAQH/BAgwBgEB/wIBADALBgNVHQ8EBAMCAYYwDQYJKoZIhvcNAQEL\r
\r\nBQADggEBALEa9Hf5iGcFKLpjf30KCBelEgJ3ZxLSBOgsn8UkulB62FyUgnne4AmY\r
\r\nnuWHY0xjbamls8Dgt1GtQrfh3kKq2rfjdasFvrQnAQkjin61O16nbCbWS2H+sqy7Ae\r
\r\nTJZWefx1elAv8XH7g491C5Rb5TGykk/bFm7RvGhr35ri+nIcqiDmjO44zHr1aPvm\r
\r\nns4vA06UQFvLWfY2wiynZ6f+PuvsPraL7kQVJqsel8TYpZjMWL/hc3VvKEX6gqPm\r
\r\nnbzTypaxa63FCETXtXNlsdid/QWX7L/pUtQ2U57mHi+xJNkA8/Spf1y4zH1rAnk\r
mw\r\n\r\nBjeKGRphA4LKir3wsbdXRYbBe7POZo=\r\n\r\n-----END CERTIFICATE-----",
  "certificate_chain" : "-----BEGIN CERTIFICATE-----\r
\nMIIDCzCCAlugAwIBAgIKKsxpOVE4imyq4zANBgkqhkiG9w0BAQsFADBOMQowCAYD\r
\nVQQDDAE3MQswCQYDVQQGEwJDTjEQMA4GA1UECAwHU2ljaHVhbjEQMA4GA1UEBwwwH\r
\nQ2h1bmdkdTEPMA0GA1UECgwGSHVhd2VpMB4XDTEwMTAxNDA4NDMxMVoXDTIyMTAx\r
\nMTAyNTMzMVowTjEKMAGGA1UEAwwBNzELMAkGA1UEBhMCQ04xEDAQBgNVBAGMB1Np\r
\nY2h1YW4xEDAQBgNVBACMB0NoZW5nZHUxZCZANBgNVBAoMBkh1YXdlTCCASlwdQYJ\r
\n\r\nKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMH7+ovgt/xbBfLAG0yBs9QERnfgdLL\r
\n\r\n5BFlgjJNP0Aashw2k5EaWq1qDfY6o4AqGfJHjPd2kLy5ZW7Cq6vuqTD3Uj3tX98N2\r
\r\n\r\n6T2Na/\r
s1JGmIExX7Udsikv6hsoKmAjrgdDBEs2Jl/2FRnxO8uFnOuSLqvPUvLR7c\r
\r\n\r\nldoDq4WqVyl4sXAOuq7xB8GoTsGLANn8eYHVNsZcSZ9E0qEiWx3WqhPh9Ncto949\r
\r\n\r\nvDuDVqkQ9QjFo/\r
yEO6+KhxqyVDWQwdl3UsyzjGtFzKQksLUQ0AUec4IsK/VWypG\r\n\r\nnu34jEkaWGv72CmFGGjEK/K/\r
WoXyzKyCmnS3Wcz4ETliRG5f7aqP56sCAwEAANT\r\n\r\nr\nMFewHwYDVR0jBBgwFoAU7mN+iV48F\r
+14i3MCRvLaPEWWudgwhQYDVR0OBBYEFO5j\r\n\r\nrfnolePBfteltzAq1S2jxFlrnYMA8GA1UdEwEB/\r
wQFMAMBAF8wDQYJKoZIhvcNAQEL\r
\r\nBQADggEBAACHJruSBkb8gA0VajKTZWN7QOvUoJPA2TdOmlnKzxyR5sXkOmslHLP\r
\r\n\r\nnjze9LBKbkMI4/
```

```
ZfWvLUde7wKJzV208E1c3mf0iZFqRJ0Ms+o/DStVw/ap+98ML\r\n4oevJk2y/bn7IQL2bvnEi/  
+iSzmz1CllnRUyfEWBW2aVFgJrm/ZaFTiEb5jldzm\r\ns75YNCvln3eKp+yOQ8fyG7mKvvn3nlRKfMTv+  
+bLLUh9or/e/phWkUj0gtSyDn\r\n\r\nnyOnVuhxyveLwoag27U8THe5E4Ygrrg98v2eGNFyGMmtsXXKNgFSf5FBqvED9d61\r\nnZ86vYp/  
N2dbauF7uUUaX5RbtFANYFU0=\r\nn-----END CERTIFICATE-----"  
}
```

Status code: 400

Invalid request parameters.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 401

Token required for the requested page.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 403

Authentication failed.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 404

No resources available or found.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 500

Internal service error.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.

Status Code	Description
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.11 Importing a CA Certificate

Function

This API is used to import a CA certificate. To use this API, the following conditions must be met:

- (1) A subordinate CA must be in the "PENDING" state.
- (2) The imported certificate body must meet the following requirements:
 - a. The certificate signing request must be exported from the PCA system when the certificate is issued.
 - b. The completed certificate chain must be imported if you need to export a complete certificate chain later.
 - c. The certificate body and chain must be in PEM format.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:import	Write	ca *	-	-	-
		-	g:EnterpriseProjectId		

URI

POST /v1/private-certificate-authorities/{ca_id}/import

Table 4-169 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the CA certificate you want to import. Minimum: 36 Maximum: 36

Request Parameters

Table 4-170 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-171 Request body parameters

Parameter	Mandatory	Type	Description
certificate	Yes	String	Certificate content Minimum: 1 Maximum: 32768
certificate_chain	No	String	Certificate chain content Minimum: 0 Maximum: 2097152

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400

Table 4-172 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-173** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-174** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-175 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-176** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/import
```

```
{
  "certificate" : "-----BEGIN CERTIFICATE-----",
  "certificate_chain" : "-----BEGIN CERTIFICATE-----"
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.12 Restoring a CA

Function

This API is used to restore a CA status from **Schedule deletion** to **Disabled**.

 NOTE

Note: Only a CA in the **Pending deletion** status can be restored.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:restore	Write	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

POST /v1/private-certificate-authorities/{ca_id}/restore

Table 4-177 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the CA certificate you want to restore. Minimum: 36 Maximum: 36

Request Parameters

Table 4-178 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400**Table 4-179** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-180** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-181** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-182** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-183** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/restore
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.

Status Code	Description
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.1.13 Revoking a Subordinate CA

Function

This API is used to revoke a subordinate CA.

NOTE

If you do not want to provide the revocation reason, set the request body to `{}`. Otherwise, an error will be reported.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:revoke	Write	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

POST /v1/private-certificate-authorities/{ca_id}/revoke

Table 4-184 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the sub-CA you want to revoke. Minimum: 36 Maximum: 36

Request Parameters

Table 4-185 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-186 Request body parameters

Parameter	Mandatory	Type	Description
reason	No	String	Reason for revocation. The options are as follows: • UNSPECIFIED: No revocation reason is specified during revocation. The default value is used. • KEY_COMPROMISE: The certificate key material is disclosed. • CERTIFICATE_AUTHORITY_COMPROMISE: CA key materials may be disclosed on the issuing path. • AFFILIATION_CHANGED: The subject or other information in the certificate has been changed. • SUPERSEDED: This certificate has been replaced. • CESSATION_OF_OPERATION: The entity in this certificate or issuing path has ceased to operate • CERTIFICATE_HOLD: The certificate is invalid at present and may take effect in the future. • PRIVILEGE_WITHDRAWN: The certificate no longer has the permission on the attributes it declares. • ATTRIBUTE_AUTHORITY_COMPROMISE: The certificate authority that warrants this certificate attribute may have been compromised. NOTE Note: If you do not want to provide the revocation reason, set the request body to "{}". Otherwise, an error will be reported. UNSPECIFIED is the default value.

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400

Table 4-187 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-188 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403

Table 4-189 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-190** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-191** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/6434f74f-2d13-4e6a-89eb-93ee313f1a43/revoke
{
  "reason": "KEY_COMPROMISE"
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.2 Private Certificate Management

4.2.2.1 Querying the List of Private Certificates

Function

This API is used to query the private certificate list.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:list	List	-	g:EnterpriseProjectId	-	-

URI

GET /v1/private-certificates

Table 4-192 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	The number of returned records. The default value is 10 . Minimum: 0 Maximum: 1000
name	No	String	The name of the private certificate. The set of certificates whose names contain the name field is returned. Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
offset	No	Integer	Index position. The query starts from the next data record indexed by this parameter. Minimum: 0
status	No	String	The private certificate status. You can query private certificates by status. • ISSUED: The certificate has been issued. • REVOKED: The certificate has been revoked. • EXPIRED: The certificate has expired.
sort_key	No	String	Sorting attribute. The following attributes are available now: • create_time: certificate creation time (default) • common_name: certificate name • issuer_name CA name. • not_after: certificate expiration time
sort_dir	No	String	Sorting sequence. The options are as follows: • DESC: descending order (default) • ASC: ascending order

Request Parameters

Table 4-193 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-194 Response body parameters

Parameter	Type	Description
total	Integer	Total number of private certificates. Minimum: 0 Maximum: 1000000
certificates	Array of Certificates objects	For details, see data structure for the Certificates field. Array Length: 0 - 1000

Table 4-195 Certificates

Parameter	Type	Description
certificate_id	String	ID of the private certificate. Minimum: 36 Maximum: 36
status	String	Certificate status: • ISSUED: The certificate has been issued. • EXPIRED: The certificate has expired. • REVOKED: The certificate has been revoked.
issuer_id	String	ID of the parent CA. Minimum: 36 Maximum: 36
issuer_name	String	The name of the parent CA certificate. Minimum: 1 Maximum: 64
key_algorithm	String	Key algorithm.
signature_algorithm	String	Signature algorithm.
freeze_flag	Integer	Freezing tag: • 0: non-frozen • Other values: frozen state. This is currently reserved.

Parameter	Type	Description
gen_mode	String	Certificate generation method. • GENERATE: generated by the PCA system. • IMPORT: imported externally. • CSR: issued by an internal CA with CSRs imported externally. This means the private key is not managed by PCA.
serial_number	String	Serial number. Minimum: 1 Maximum: 64
create_time	Long	Time the certificate was created. The value is a timestamp in milliseconds.
delete_time	Long	Time the certificate was deleted. The value is a timestamp in milliseconds.
not_before	Long	Time the certificate was created. The value is a timestamp in milliseconds.
not_after	Long	Time the certificate expires. The value is a timestamp in milliseconds.
distinguished_name	DistinguishedName object	Certificate name. For details, see data structure for the DistinguishedName field.
enterprise_project_id	String	Enterprise project ID. The default value is 0 . For users who have enabled the enterprise project function, this value indicates that resources are in the default enterprise project. For users who have not enabled the enterprise project function, this value indicates that resources are not in the default enterprise project.

Table 4-196 DistinguishedName

Parameter	Type	Description
common_name	String	Common name (CN) of a certificate. The value can contain a maximum of 64 characters, including only letters, digits, spaces, Chinese characters, hyphens (-), underscores (_), periods (.), commas (,), and asterisks (*). Minimum: 1 Maximum: 64
country	String	Country code. The value is a string of two characters and can contain only letters. Minimum: 2 Maximum: 2
state	String	Name of a province or city. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
locality	String	Region name. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
organization	String	Organization name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64

Parameter	Type	Description
organizational_unit	String	Organization unit name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64

Table 4-197 EncCertInfo

Parameter	Type	Description
enc_serial_number	String	Encryption certificate serial number. Minimum: 1 Maximum: 64

Status code: 400**Table 4-198** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-199** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-200** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-201** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-202** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

GET https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates

Example Responses

Status code: 200

Request succeeded.

```
{
  "total": 2,
  "certificates": [ {
    "signature_algorithm": "SHA256",
    "issuer_id": "ef5d84d1-4f52-47d2-b1c8-a91a672487a0",
    "issuer_name": "12",
    "not_after": 1665539214000,
    "not_before": 1634295475000,
    "status": "ISSUED",
    "freeze_flag": 0,
    "gen_mode": "GENERATE",
    "serial_number": "202110151057541266081861",
    "distinguished_name": {
      "country": "cn",
      "state": "guizhou",
      "locality": "guiyang",
      "organization": "hw",
      "organizational_unit": "IT",
      "common_name": "test.huawei.com"
    },
    "key_algorithm": "RSA4096",
    "create_time": 1634295475000,
    "delete_time": null,
    "certificate_id": "6434f74f-2d13-4e6a-89eb-93ee313f1a43",
    "enc_cert_info": {
      "enc_serial_number": "2ad6c3e393a95bf13f95"
    }
  }, {
    "signature_algorithm": "SHA256",
    "issuer_id": "ef5d84d1-4f52-47d2-b1c8-a91a672487a0",
    "issuer_name": "12",
    "not_after": 1665539214000,
    "not_before": 1634110315000,
    "status": "ISSUED",
    "freeze_flag": 0,
    "gen_mode": "GENERATE",
    "serial_number": "202110130731541908887138",
    "distinguished_name": {
      "country": "cn",
      "state": "sichuan",
      "locality": "chengdu",
      "organization": "hw",
      "organizational_unit": "HR",
```

```
{
  "common_name": "hr.huawei.com"
},
"key_algorithm": "RSA4096",
"create_time": 1634110316000,
"delete_time": null,
"certificate_id": "1cbb5a52-806b-469c-b182-7446e1851a1c",
"enc_cert_info": {
  "enc_serial_number": "448ad305b90e0a266e9"
}
}]
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.

Status Code	Description
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.2.2 Applying for a Certificate

Function

This API is used to apply for a certificate.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:issue Cert	Write	ca *	-	-	-

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
		-	- g:EnterpriseProjectId - g:RequestTag/<tag-key> - g:TagKeys - pca:CommonName		

URI

POST /v1/private-certificates

Request Parameters

Table 4-203 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-204 Request body parameters

Parameter	Mandatory	Type	Description
issuer_id	Yes	String	ID of the parent CA. Minimum: 36 Maximum: 36

Parameter	Mandatory	Type	Description
key_algorithm	No	String	Key algorithm. If this parameter is not specified, the key algorithm of the CA is used by default. The options are as follows: • RSA2048: RSA algorithm with the key length of 2048 bits • RSA4096: RSA algorithm with the key length of 4096 bits • EC256: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 256 bits • EC384: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 384 bits • SM2: Elliptic curve algorithm (signature hash algorithm SM3) issued by China State Cryptography Administration, with the key length of 256 bits (Chinese mainland website)
signature_algorithm	No	String	Signature hash algorithm. If this parameter is not specified, the signature hash algorithm of the CA is used by default. The options are as follows: • SHA256 • SHA384 • SHA512 • SM3 (Chinese mainland website)
distinguished_name	Yes	CertDistinguishedName object	Certificate name. For details, see data structure for the CertDistinguishedName field.
validity	Yes	Validity object	Certificate validity. For details, see data structure for the Validity field.

Parameter	Mandatory	Type	Description
key_usages	No	Array of strings	Key usage. For details, see [4.2.1.3] in RFC 5280 (https://datatracker.ietf.org/doc/html/rfc5280#section-4.2.1.3) • digitalSignature: used as digital signatures. • nonRepudiation: used for non-repudiation • keyEncipherment: used to encrypt key data. • dataEncipherment: used to encrypt data. • keyAgreement: used for key negotiation • keyCertSign: used to issue a certificate. • cRLSign: used to issue the revocation list. • encipherOnly: used only for encryption. • decipherOnly: used only for decryption.
subject_alternative_names	No	Array of SubjectAlternativeName objects	Alternative name for the subject. For details, see data structure of the SubjectAlternativeName field. • Array size: [0, 20] Array Length: 0 - 20
extended_key_usage	No	ExtendedKeyUsage object	Extended key usage. For details, see data structure for the ExtendedKeyUsage field.
customized_extension	No	CustomizedExtension object	Customized extension information. For details, see data structure for the CustomizedExtension field.

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. If the enterprise project function is not enabled, you do not need to set this parameter. If the enterprise project function is enabled, you can set this parameter when querying a resource. If this parameter is not specified, the system searches for the required resource in all the enterprise projects that you have permissions for. In this case, the value of enterprise_project_id is all. The parameter value must meet one of the following requirements: Is all Is 0 Matches the regular expression <code>^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}\$</code>.

Table 4-205 CertDistinguishedName

Parameter	Mandatory	Type	Description
common_name	Yes	String	Common name (CN) of a certificate. The value can contain a maximum of 64 characters, including only letters, digits, spaces, Chinese characters, hyphens (-), underscores (_), periods (.), commas (,), and asterisks (*). Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
country	No	String	Country code. The value is a string of two characters and can contain only letters. If this parameter is not specified, the value of the parent CA is inherited by default. Minimum: 2 Maximum: 2
state	No	String	Name of a province or city. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). If this parameter is not specified, the value of the parent CA is inherited by default. Minimum: 1 Maximum: 128
locality	No	String	Region name. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). If this parameter is not specified, the value of the parent CA is inherited by default. Minimum: 1 Maximum: 128
organization	No	String	Organization name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). If this parameter is not specified, the value of the parent CA is inherited by default. Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
organizational_unit	No	String	Organization unit name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). If this parameter is not specified, the value of the parent CA is inherited by default. Minimum: 1 Maximum: 64

Table 4-206 Validity

Parameter	Mandatory	Type	Description
type	Yes	String	Validity period type, which is mandatory. The options are as follows: • YEAR: by the year (12 months) • MONTH: by the month (31 days) • DAY: by the day • HOURL: by the hour
value	Yes	Integer	The certificate validity period. The value of this parameter varies depending on the value of type : • Root CAs: The validity period is less than or equal to 30 years. • Subordinate CAs and private certificates: The validity period is less than or equal to 20 years.

Parameter	Mandatory	Type	Description
start_from	No	Integer	Start time. The options are as follows: • The format is a timestamp in milliseconds. For example, 1645146939688 indicates 2022-02-18 09:15:39. • The start time can begin no more than five minutes earlier than the current time. It means the value of start_from must be larger than the value of current_time minus 5 minutes.

Table 4-207 SubjectAlternativeName

Parameter	Mandatory	Type	Description
type	Yes	String	Type of the alternative name. Currently, only DNS, IP, EMAIL, URI, and UPN are allowed. • DNS • IP • EMAIL • URI • UPN

Parameter	Mandatory	Type	Description
value	Yes	String	Value of the corresponding alternative name type. • DNS type. The length cannot exceed 253 characters. • IP type. The length cannot exceed 39 characters. IPv4 and IPv6 are supported. • EMAIL type. The length cannot exceed 256 characters. • URI type. The length cannot exceed 253 characters. • UPN type. The length cannot exceed 256 characters.

Table 4-208 ExtendedKeyUsage

Parameter	Mandatory	Type	Description
server_auth	No	Boolean	Server authentication. The OID is 1.3.6.1.5.5.7.3.1. • true • false NOTE Enable this enhanced key usage for the server certificate. The default value is false. Default: false
client_auth	No	Boolean	Client authentication. The OID is 1.3.6.1.5.5.7.3.2 • true • false NOTE Enable this enhanced key usage for the client certificate. The default value is false. Default: false

Parameter	Mandatory	Type	Description
code_signing	No	Boolean	Signing of downloadable executable code client authentication. The OID is 1.3.6.1.5.5.7.3.3. • true • false NOTE The default value is false. Default: false
email_protection	No	Boolean	Email protection. The OID is 1.3.6.1.5.5.7.3.4. • true • false NOTE The default value is false. Default: false
time_stamping	No	Boolean	Binding the hash of an object to a time. The OID is 1.3.6.1.5.5.7.3.8 • true • false NOTE The default value is false. Default: false
smart_card_login	No	Boolean	Smart card login. The OID is 1.3.6.1.4.1.311.20.2.2. • true • false Active Directory login. The default value is false. Default: false

Table 4-209 CustomizedExtension

Parameter	Mandatory	Type	Description
object_identifier	No	String	Object identifier NOTE The value of this parameter must be a dot-decimal notation string that complies with the ASN1 specifications, for example, 1.3.6.1.4.1.2011.4.99. Minimum: 1 Maximum: 64
value	No	String	Custom attribute content. Minimum: 1 Maximum: 64

Response Parameters

Status code: 200

Table 4-210 Response body parameters

Parameter	Type	Description
certificate_id	String	ID of the certificate being issued. Minimum: 36 Maximum: 36

Status code: 400

Table 4-211 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-212 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-213** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-214** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-215 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates

```
{
  "key_algorithm" : "RSA2048",
  "distinguished_name" : {
    "country" : "CN",
    "state" : "Sichuan",
    "locality" : "Chengdu",
    "organization" : "Huawei",
    "organizational_unit" : "CloudBU",
    "common_name" : "TestCert"
  },
  "subject_alternative_names" : [ {
    "type" : "IP",
    "value" : "156.127.116.38"
  } ],
  "signature_algorithm" : "SHA256",
  "validity" : {
    "type" : "YEAR",
    "value" : 3
  },
  "issuer_id" : "2cb2878b-6cd1-460d-bd25-afe655159bdc",
  "key_usages" : [ "digitalSignature", "nonRepudiation" ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "certificate_id" : "ae9a326a-b61e-4446-854d-cda30ffe31f5"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.2.3 Issuing a Certificate with a CSR

Function

This API is used to issue a certificate with a CSR. The constraints are as follows:

1. The default parameters are as follows:
2. When **type** is set to **INTERMEDIATE_CA**, the created subordinate CA certificate has the following restrictions:
 - Default CA parameters:
 - **keyUsage**: can be set to **digitalSignature**, **keyCertSign**, or **cRLSign**. The parameters in the CSR are preferentially used.
 - **SignatureHashAlgorithm**: SHA384
 - **PathLength**: 0 (customizable)
 - Private certificate parameters:
 - **keyUsage**: can be set to **digitalSignature** **keyAgreement**. The parameter in the CSR is preferentially used.
 - **SignatureHashAlgorithm**: SHA384
 - It does not use the CA quota. The certificate is not returned when the CA list is queried.
 - Only the following two APIs can be used to obtain the information:
 - Cannot be used to issue a certificate. The key is kept by the user.
 - It uses the private certificate quota. When the private certificate list is queried, the certificate is returned.
 - The usage of other private certificates is the same as that of other private certificates, except that the key information is not exported (the key information is kept by the user.).

Obtaining certificate details: GET /v1/private-certificate-authorities/{ca_id}

Exporting a certificate: POST /v1/private-certificate-authorities/{ca_id}/export

certificate_id returned by this API indicates **ca_id** of the subordinate CA.

1. If **type** is set to **ENTITY_CERT**, the created private certificate has the following features:

NOTE

Note: Use `\r\n` or `\n` to replace the newline characters to convert the CSR into a string. For details, see the example request. Note: The organization information, public key algorithm, and public key content of a certificate are included in the CSR file and cannot be obtained through APIs.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:issueCertByCsr	Write	ca *	-	• pca:ca:issueCertThroughCSR	-
		-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • pca:CommonName		

URI

POST /v1/private-certificates/csr

Request Parameters

Table 4-216 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-217 Request body parameters

Parameter	Mandatory	Type	Description
issuer_id	Yes	String	ID of the parent CA. Minimum: 36 Maximum: 36
csr	Yes	String	Certificate signature request. Use <code>\r\n</code> or <code>\n</code> to replace the newline characters in the CSR. The replacement is not required if this API is requested through the console. Maximum: 5120
validity	Yes	Validity object	Certificate validity. For details, see data structure for the Validity field.
type	No	String	Certificate type. This parameter is used to distinguish subordinate CA certificates from private certificates. • ENTITY_CERT: indicates private certificates. The default value is used. • INTERMEDIATE_CA: indicates subordinate CAs.
path_length	No	Integer	Path length. This parameter is valid only when a subordinate CA is issued. Minimum: 0 Maximum: 6
subject_alternative_names	No	Array of SubjectAlternativeName objects	The alternative name for the subject (This parameter is reserved and ignored at the backend). For details, see data structure for the SubjectAlternativeName field. Array Length: 0 - 20

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Enterprise project ID. If the enterprise project function is not enabled, you do not need to set this parameter. If the enterprise project function is enabled, you can set this parameter when querying a resource. If this parameter is not specified, the system searches for the required resource in all the enterprise projects that you have permissions for. In this case, the value of enterprise_project_id is all. The parameter value must meet one of the following requirements: Is all Is 0 Matches the regular expression <code>^[0-9a-z]{8}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{4}-[0-9a-z]{12}\$</code>.

Table 4-218 Validity

Parameter	Mandatory	Type	Description
type	Yes	String	Validity period type, which is mandatory. The options are as follows: ● YEAR: by the year (12 months) ● MONTH: by the month (31 days) ● DAY: by the day ● HOUR: by the hour

Parameter	Mandatory	Type	Description
value	Yes	Integer	The certificate validity period. The value of this parameter varies depending on the value of type : • Root CAs: The validity period is less than or equal to 30 years. • Subordinate CAs and private certificates: The validity period is less than or equal to 20 years.
start_from	No	Integer	Start time. The options are as follows: • The format is a timestamp in milliseconds. For example, 1645146939688 indicates 2022-02-18 09:15:39. • The start time can begin no more than five minutes earlier than the current time. It means the value of start_from must be larger than the value of current_time minus 5 minutes.

Table 4-219 SubjectAlternativeName

Parameter	Mandatory	Type	Description
type	Yes	String	Type of the alternative name. Currently, only DNS , IP , EMAIL , URI , and UPN are allowed. • DNS • IP • EMAIL • URI • UPN

Parameter	Mandatory	Type	Description
value	Yes	String	Value of the corresponding alternative name type. • DNS type. The length cannot exceed 253 characters. • IP type. The length cannot exceed 39 characters. IPv4 and IPv6 are supported. • EMAIL type. The length cannot exceed 256 characters. • URI type. The length cannot exceed 253 characters. • UPN type. The length cannot exceed 256 characters.

Response Parameters

Status code: 200

Table 4-220 Response body parameters

Parameter	Type	Description
certificate_id	String	ID of the certificate being issued. Minimum: 36 Maximum: 36

Status code: 400

Table 4-221 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-222** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-223** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-224** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-225 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you use this API to issue a certificate via CSR, a token is required in the **X-Auth-Token** field in the request header. The token must have the permission to access the API.

POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/csr

```
{
  "csr" : "-----BEGIN CERTIFICATE REQUEST-----\n
  \nMIICTCCABECAQAwXjELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB3NpY2hhdW4xEDAO\n
  \nBgNVBAcTB2NoZW5nZHUxZzAjbGVBaTAKXMQswCQYDVQQLZW5nZHUxZzAjbGVB\n
  \nAUMIdGVzdC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQcz4q5z\n
  \nFC9x2jESeUW5GB6zS5rVxT0WLTCTv9d1LtWBLsRiinATYTYiP1pNo4/pBq\n
  \nHIM3IiUDkc896CJerYINzOljTaV4GjCZvPrxSHU5toJvIDfIBsY+gnzbT1ol/y0r\n
  \n3yb9dx7eeF5rPR+U8RTw+Ov/\n
  \nNRb+0CY30hrXMdrWjp5dtLGTlr5EFYxIKNOPCkR\n
  \n+6BGyJnC9PWSuqwsykFbgMRkcBaNAxa59dRhMF50pvx2Vs929vFrMi+ofDELUOqz\n
  \n1vyjaEA3pn3AGJGXZgrGNbSfz12ixgGLes4cQD21GCIAWgnBQ7b1ru2V8ImUfyh0\n
  \nnyvTEyHJTufbQ\n
  \n+257AgMBAAGgJjAkBgkqhkiG9w0BCQ4xZzAVMBMGA1UdEQQMMMAqC\n
  \nCHRLc3QuY29tMA0GCSqGSIb3DQEBCwUAA4IBAQKfjZuYsz4s0wb1POIWn41eiAB\n
  \nnp53qb63QKWILN9z8dLktcdSI3IPfcPZpXv++QPtn3LR9rJKBawusk6SPXbvOGgS\n
  \n5J\n
  \n+6eM8kVW2O3gHFgoaMcPYvtiO7ekG6o25qx6+Rj84wbFdmPoiCc8AwrLEBwzYV\n
  \nnp1zaprWQu6PxBulkYPa3FLcntDdi7B67r0YtpxVvo1K7vHYFboDvPz7xG57QIFIM\n
  \nnwGd1OegariMT3N8gBOzLZc+jqLpxgo4xoNqBHM06DEmKLDwDzU4ljpuGK9had99k\n
  \nnvQ5vft/\n
  \nQra3v1uq2lOm/G92b0uA9Y1t2bMHobTAnuXLOHmY9XclDzpC3f8h8\n
  \nn-----END CERTIFICATE REQUEST-----",
  "validity" : {
    "type" : "YEAR",
    "value" : 3
  },
  "issuer_id" : "2cb2878b-6cd1-460d-bd25-afe655159bdc"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "certificate_id" : "e3e10fc6-5dff-4a70-9cb5-320d258a6215"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
}
```

```
{
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.2.4 Parsing a CSR

Function

This API is used to parse a CSR.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/private-certificates/csr/parse

Request Parameters

Table 4-226 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-227 Request body parameters

Parameter	Mandatory	Type	Description
csr	Yes	String	Certificate signature request. Use <code>\r\n</code> or <code>\n</code> to replace the newline characters in the CSR. The replacement is not required if this API is requested through the console. Maximum: 5120

Response Parameters

Status code: 200

Table 4-228 Response body parameters

Parameter	Type	Description
key_algorithm	String	Key algorithm.
key_algorithm_length	Integer	Length of the key algorithm, in bits.
signature_algorithm	String	Signature algorithm with a specific signature and hash algorithm, for example, SHA256withRSA .
public_key	String	Public key content. NOTE The newline characters have been replaced with \r\n. Minimum: 0 Maximum: 4096
distinguished_name	DistinguishedName object	Certificate name. For details, see data structure for the DistinguishedName field.

Table 4-229 DistinguishedName

Parameter	Type	Description
common_name	String	Common name (CN) of a certificate. The value can contain a maximum of 64 characters, including only letters, digits, spaces, Chinese characters, hyphens (-), underscores (_), periods (.), commas (,), and asterisks (*). Minimum: 1 Maximum: 64
country	String	Country code. The value is a string of two characters and can contain only letters. Minimum: 2 Maximum: 2

Parameter	Type	Description
state	String	Name of a province or city. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
locality	String	Region name. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
organization	String	Organization name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64
organizational_unit	String	Organization unit name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64

Status code: 400

Table 4-230 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-231** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-232** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-233** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-234 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/csr/parse

```
{
  "csr" : "-----BEGIN CERTIFICATE REQUEST-----\n
MIICyTCCAbECAQAwXjELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB3NpY2hhdW4xEDAO\n
BgNVBACTB2NoZW5nZHUxCzAJBgNVBAoTAkhXMQswCQYDVQQLLEwJJVDERMA8GA1UE\n
AxMldGVzdC5jb20wggiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCZ4q5z\\nxqK/L/\n
FC9x2jESeUW5GB6zS5rVxT0WLTCTv9d1LtWBLsRlinATYTYiP1pNo4/pBq\n
\\nHlM3liUDkc896CJerYINzOljTaV4GjCZvPrxSHU5toJvDfBsY+gnzbT1ol/y0r\\n3yb9dx7eeF5rPR+U8RTw+Ov/\n
ZNRb+0CY30hrXMDrWjp5dtLGTlr5EFYxIKNOPCkr\\n\n
+6BGyJnC9PWSuqwsykFbgMRkcBaNAxa59dRhMF50pvx2Vs929vFrMi+ofDELUOqz\n
\\n1vyjaEA3pn3AGJGXZgrGNbSfz12ixgGLes4cQD21GCIAWgnBQ7b1ru2V8lmUfyh0\\nyvTEyHJTufbQ\n
+257AgMBAAAgJjAkBgqhkiG9w0BCQ4xFzAVMBMGAlUdEQQMMAqC\n
\\nCHRLc3QuY29tMA0GCSqGSIb3DQEBCwUAA4IBAQBKfjZuYsz4s0wb1POIWn41eiAB\n
\\np53qb63QKWILN9z8dLktcdSL3IPfcfPZpXv++QPtn3LR9rJKBawusk6SPXbvOGgS\\n5J\n
+6eM8kVW2O3gHFgoaMcPYvtiO7ekG6o25qx6+Rj84wbFdmPOiCc8AwrLEBwzYV\n
\\np1zaprWQu6PxBulkYPa3FLcntDdi7B67r0YtpxVvo1K7vHYFboDvPz7xG57QIFIM\n
\\nwGd1OegariMT3N8gBOzLZc+jqLpxgo4xoNqBHM06DEmKLdWdzU4ljpuGK9had99K\\nvQ5vft/\n
Qra3v1uq2lOm/G92b0uA9Y1t2bMHobTAnuXLOHmY9XcLdzc3f8h8\\n-----END CERTIFICATE REQUEST-----"
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "distinguished_name" : {
```

```
"country" : "CN",
"state" : "sichuan",
"locality" : "chengdu",
"organization" : "HW",
"organizational_unit" : "IT",
"common_name" : "test.com"
},
"public_key" : "-----BEGIN PUBLIC KEY-----\r
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAx1EX1JfOXquoFDjVi67T\r
\npF4kFwetNnLwC0ZQTOk3fftX4/rkHwdGdsYAalzLz2ltlgbtLJHeKaNnjlqTL8bn\r
\n0DVIxww6ZP6VaxpfKXaj76GxDdvb5kp8yRFUAK8N2YQ0UicsFoXn2CAx1dOtAaNf\r
\nO+HwooRnp6GekZaRSYS2bk4olkQ83/2WkkTGC+tAmjSFG7AIY8jaO5RgX40YGANh\r
\nU9UGOo8xCux8k2dsXRnY+fxRiLWphiT2ij4CYURagETbKuRI9WOI+HFVkmIU/Op\r
\nn3FWqB0RdrRTEcAC+55fmW75E85rAMh9f65wa/6eWcM6vlnby4Bbm1mclDr3olgKJ\r
\nnUQIDAQAB\r\n-----END PUBLIC KEY-----\r
\n",
"key_algorithm" : "RSA",
"key_algorithm_length" : 2048,
"signature_algorithm" : "SHA256withRSA"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.2.5 Querying the Private Certificate Quota

Function

This API is used to query the private certificate quota.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:quota	Read	-	-	-	-

URI

GET /v1/private-certificates/quotas

Request Parameters

Table 4-235 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-236 Response body parameters

Parameter	Type	Description
quotas	Quotas object	Certificate quota. For details, see data structure for the Quotas field.

Table 4-237 Quotas

Parameter	Type	Description
resources	Array of Resources objects	Resource quota list. For details, see data structure for the Resources field. Array Length: 0 - 10

Table 4-238 Resources

Parameter	Type	Description
type	String	Certificate type. CERTIFICATE_AUTHORITY: CA certificate. CERTIFICATE: private certificate.
used	Integer	Used quota

Parameter	Type	Description
quota	Integer	Total quota. • CERTIFICATE_AUTHORITY: 100 is specified in the current system. • CERTIFICATE: 100000 is specified in the current system.

Status code: 400**Table 4-239** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-240** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403

Table 4-241 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-242** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-243** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

GET <https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/quotas>

Example Responses

Status code: 200

Request succeeded.

```
{
  "quotas" : {
    "resources" : [ {
      "type" : "CERTIFICATE",
      "used" : 25,
      "quota" : 100000
    } ]
  }
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.2.6 Querying Certificate Details

Function

This API is used to query details about a certificate.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:get	Read	-	g:EnterpriseProjectId	-	-

URI

GET /v1/private-certificates/{certificate_id}

Table 4-244 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	ID of the private certificate you want to query. Minimum: 36 Maximum: 36

Request Parameters

Table 4-245 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-246 Response body parameters

Parameter	Type	Description
certificate_id	String	ID of the private certificate. Minimum: 36 Maximum: 36
status	String	Certificate status: • ISSUED: The certificate has been issued. • EXPIRED: The certificate has expired. • REVOKED: The certificate has been revoked.

Parameter	Type	Description
issuer_id	String	ID of the parent CA. Minimum: 36 Maximum: 36
issuer_name	String	The name of the parent CA certificate. Minimum: 1 Maximum: 64
key_algorithm	String	Key algorithm.
signature_algorithm	String	Signature algorithm.
freeze_flag	Integer	Freezing tag: • 0: non-frozen • Other values: frozen state. This is currently reserved.
gen_mode	String	Certificate generation method. • GENERATE: generated by the PCA system. • IMPORT: imported externally. • CSR: issued by an internal CA with CSRs imported externally. This means the private key is not managed by PCA.
serial_number	String	Serial number. Minimum: 1 Maximum: 64
create_time	Long	Time the certificate was created. The value is a timestamp in milliseconds.
delete_time	Long	Time the certificate was deleted. The value is a timestamp in milliseconds.
not_before	Long	Time the certificate was created. The value is a timestamp in milliseconds.
not_after	Long	Time the certificate expires. The value is a timestamp in milliseconds.
distinguished_name	DistinguishedName object	Certificate name. For details, see data structure for the DistinguishedName field.

Parameter	Type	Description
enterprise_project_id	String	Enterprise project ID. The default value is 0 . For users who have enabled the enterprise project function, this value indicates that resources are in the default enterprise project. For users who have not enabled the enterprise project function, this value indicates that resources are not in the default enterprise project.

Table 4-247 DistinguishedName

Parameter	Type	Description
common_name	String	Common name (CN) of a certificate. The value can contain a maximum of 64 characters, including only letters, digits, spaces, Chinese characters, hyphens (-), underscores (_), periods (.), commas (,), and asterisks (*). Minimum: 1 Maximum: 64
country	String	Country code. The value is a string of two characters and can contain only letters. Minimum: 2 Maximum: 2
state	String	Name of a province or city. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128
locality	String	Region name. The value can contain a maximum of 128 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 128

Parameter	Type	Description
organization	String	Organization name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64
organizational_unit	String	Organization unit name. The value can contain a maximum of 64 characters, including only letters, digits, Chinese characters, spaces, hyphens (-), underscores (_), periods (.), and commas (,). Minimum: 1 Maximum: 64

Table 4-248 EncCertInfo

Parameter	Type	Description
enc_serial_number	String	Encryption certificate serial number. Minimum: 1 Maximum: 64

Status code: 400**Table 4-249** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-250 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-251** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-252** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-253 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
GET https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/  
6434f74f-2d13-4e6a-89eb-93ee313f1a43
```

Example Responses

Status code: 200

Request succeeded.

```
{  
  "signature_algorithm" : "SHA256",  
  "issuer_id" : "ef5d84d1-4f52-47d2-b1c8-a91a672487a0",  
  "issuer_name" : "HW CA",  
  "not_after" : 1665539214000,  
  "not_before" : 1634295475000,  
  "status" : "ISSUED",  
  "freeze_flag" : 0,  
  "gen_mode" : "GENERATE",  
  "serial_number" : "202110151057541266081861",  
  "distinguished_name" : {  
    "country" : "cn",  
    "state" : "guizhou",  
    "locality" : "guiyang",  
    "organization" : "hw",  
    "organizational_unit" : "IT",  
    "common_name" : "test.huawei.com"  
  },  
  "key_algorithm" : "RSA4096",  
  "create_time" : 1634295475000,  
  "delete_time" : null,  
  "certificate_id" : "6434f74f-2d13-4e6a-89eb-93ee313f1a43",  
  "enc_cert_info" : {  
    "enc_serial_number" : "2ad6c3e393a95bf13f95"  
  }  
}
```

Status code: 400

Invalid request parameters.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.2.7 Deleting a Certificate

Function

This API is used to delete a certificate.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:delete	Write	-	g:EnterpriseProjectId	-	-

URI

DELETE /v1/private-certificates/{certificate_id}

Table 4-254 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	ID of the private certificate you want to delete. Minimum: 36 Maximum: 36

Request Parameters

Table 4-255 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400**Table 4-256** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-257** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-258** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-259** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-260** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
DELETE https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/  
6434f74f-2d13-4e6a-89eb-93ee313f1a43
```

Example Responses

Status code: 400

Invalid request parameters.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 401

Token required for the requested page.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 403

Authentication failed.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 404

No resources available or found.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 500

Internal service error.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.

Status Code	Description
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.2.8 Exporting a Certificate

Function

Export the certificates.

- International algorithm
 - There are two methods for different compression statuses:
 - If **is_compressed** is set to **true**, a compressed file package is returned. The package name is in the format of *Certificate name_Lowercase letters of the type field.zip*, for example, **test_apache.zip**.
 - The system generates a key issuing certificate.
 - If type is set to **APACHE**, the compressed package contains three files: **server.key** (key file in PEM format. If a password is set during certificate export, the encrypted private key is used.), **chain.crt** (certificate chain in PEM format), and **server.crt** (certificate in PEM format).
 - If type is set to **IIS**, the compressed package contains two files: **keystorePass.txt** (keystore password. If the password is set during certificate export, the password file does not exist.) and **server.pfx** (PFX certificate, which is contained in the same file as the certificate chain)
 - If type is set to **NGINX**, the compressed package contains two files: **server.key** (key file in PEM format. If a password is set during certificate export, the encrypted private key is used.) and **server.crt** (The content is in PEM format. The certificate and certificate chain are contained in the same file.)
 - If **type** is set to **TOMCAT**, the package contains two files: **keystorePass.txt** (keystore password, if the password is set during certificate export, the password file does not exist.) and **server.jks** (JKX certificate, which is contained in the same file as the certificate chain).

- If **type** is set to **OTHER**, the compressed package contains three files: **server.key** (key file in PEM format. If a password is set during certificate export, the encrypted private key is used.), **chain.pem** (certificate chain), and **server.pem** (certificate)
 - Import the CSR certificate.
 - If **type** is set to **APACHE**, **IIS**, or **TOMCAT**, the package contains two files: **chain.crt** (certificate chain in PEM format) and **server.crt** (certificate in PEM format).
 - If **type** is set to **NGINX**, the compressed package contains the **server.crt** file (certificate in PEM format).
 - If **type** is set to **OTHER**, the compressed package contains two files: **chain.pem** (certificate chain in PEM format) and **cert.pem** (certificate in PEM format).
- If **is_compressed** is set to **false**, a certificate in JSON format is returned, including the following parameters:
 - The system generates a key issuing certificate.
 - If **type** is set to **APACHE**, **NGINX**, or **OTHER**, the following parameters are returned:
 - **certificate**: indicates the certificate content in PEM format.
 - **certificate_chain**: indicates the certificate chain in PEM format.
 - **private_key** (certificate private key in PEM format. If a password is set when the certificate is exported, the encrypted private key is used.)
 - If **type** is set to "IIS" or "TOMCAT", it is not defined currently.
 - Import the CSR certificate.
 - If **type** is set to **APACHE**, **NGINX**, **IIS**, **TOMCAT**, or **OTHER**, the following parameters are returned:
 - **certificate**: indicates the certificate content in PEM format.
 - **certificate_chain**: indicates the certificate chain in PEM format.
- SM algorithm (Chinese mainland website)
 - Set whether to compress and whether to use the SM algorithm, depending on the following situations:
 - If **is_compressed** is set to **true** and **is_sm_standard** is set to **true**, a compressed file package is returned. The package name is in the format of *Certificate name_Lowercase letters of the type field.zip*, for example, **test_apache.zip**.
 - The system generates a key issuing certificate.
 - If **type** is set to **APACHE**, **IIS**, **NGINX**, or **TOMCAT**, the value is not defined.

- If **type** is set to **OTHER**, the package contains five files: **chain.pem** (certificate chain in PEM format), **signCert.key** (signature certificate key file in PEM format. If a password is set during certificate export, the encrypted private key is used.), **signCert.pem** (signature certificate in PEM format), **encSm2EnvelopedKey.key** (digital envelope file in the SM algorithm GMT0009 standard specification of the encryption certificate, encoded using Base64), **signedAndEnvelopedData.key** (digital envelope file in the SM algorithm GMT0010 standard specification of the encryption certificate, encoded using Base64), and **encCert.pem** (encryption certificate in PEM format).
- Import the CSR certificate.
 - If **type** is set to **APACHE**, **IIS**, **NGINX**, or **TOMCAT**, the value is not defined.
 - If **type** is set to **OTHER**, the compressed package contains four files: **chain.pem** (certificate chain in PEM format), **signCert.pem** (signature certificate in PEM format), **encSm2EnvelopedKey.key** (digital envelope file in the SM algorithm GMT0009 standard specification of the encryption certificate, encoded using Base64), **signedAndEnvelopedData.key** (digital envelope file in the SM algorithm GMT0010 standard specification of the encryption certificate, encoded using Base64), and **encCert.pem** (encryption certificate in PEM format).
- If **is_compressed** is set to **true** and **is_sm_standard** is set to **false**, a compressed file package is returned. The package name is in the format of *Certificate name_Lowercase letters of the type field.zip*, for example, **test_apache.zip**.
 - The system generates a key issuing certificate.
 - If **type** is set to **APACHE**, **IIS**, **NGINX**, or **TOMCAT**, the value is not defined.
 - If **type** is set to **OTHER**, the package contains five files: **chain.pem** (certificate chain in PEM format), **signCert.key** (signature certificate key file in PEM format. If a password is set during certificate export, the encrypted private key is used.), **signCert.pem** (signature certificate in PEM format), **encCert.key** (encryption certificate key file in PEM format. If a password is set when the certificate is exported, the encrypted private key is used.), and **encCert.pem** (encryption certificate in PEM format).
 - Import the CSR certificate.
 - If **type** is set to **APACHE**, **IIS**, **NGINX**, or **TOMCAT**, the value is not defined.
 - If **type** is set to **OTHER**, the compressed package contains four files: **chain.pem** (certificate chain in PEM format), **signCert.pem** (signature certificate in PEM format), **encCert.key** (encryption certificate key file in PEM format), and **encCert.pem** (encryption certificate in PEM format).

- If **is_compressed** is set to **false** and **is_sm_standard** is set to **true**, a certificate in JSON format is returned, including the following parameters:
 - The system generates a key issuing certificate.
 - If **type** is set to **APACHE**, **IIS**, **NGINX**, or **TOMCAT**, the value is not defined.
 - If **type** is set to **OTHER**, the following parameters are returned:
 - **certificate_chain**: indicates the certificate chain in PEM format.
 - **certificate**: indicates the signature certificate content in PEM format.
 - **private_key**: indicates the private key of the signature certificate in PEM format. If a password is set when the certificate is exported, the private key is encrypted.
 - **enc_certificate**: indicates the encryption certificate content in PEM format.
 - **enc_sm2_enveloped_key**: indicates the SM algorithm GMT0009 standard digital envelope file of the encryption certificate, encoded using Base64.
 - **signed_and_enveloped_data**: indicates the SM series cryptographic algorithm GMT0010 standard digital envelope file of the encryption certificate, encoded using Base64.
 - Import the CSR certificate.
 - If **type** is set to **APACHE**, **IIS**, **NGINX**, or **TOMCAT**, the value is not defined.
 - If **type** is set to **OTHER**, the following parameters are returned:
 - **certificate_chain**: indicates the certificate chain in PEM format.
 - **certificate**: indicates the signature certificate content in PEM format.
 - **enc_certificate**: indicates the encryption certificate content in PEM format.
 - **enc_sm2_enveloped_key**: indicates the SM algorithm GMT0009 standard digital envelope file of the encryption certificate, encoded using Base64.
 - **signed_and_enveloped_data**: indicates the SM algorithm GMT0010 standard digital envelope file of the encryption certificate, encoded using Base64.
- If **is_compressed** is set to **false** and **is_sm_standard** is set to **false**, a certificate in JSON format is returned, including the following parameters:
 - The system generates a key issuing certificate.

- If **type** is set to **APACHE**, **IIS**, **NGINX**, or **TOMCAT**, the value is not defined.
- If **type** is set to **OTHER**, the following parameters are returned:
 - **certificate_chain**: indicates the certificate chain in PEM format.
 - **certificate**: indicates the signature certificate content in PEM format.
 - **private_key**: indicates the private key of the signature certificate in PEM format. If a password is set when the certificate is exported, the private key is encrypted.
 - **enc_certificate**: indicates the encryption certificate content in PEM format.
 - **enc_private_key**: indicates the private key of the encryption certificate in PEM format. If a password is set when the certificate is exported, the private key is encrypted.
- Import the CSR certificate.
 - If **type** is set to **APACHE**, **IIS**, **NGINX**, or **TOMCAT**, the value is not defined.
 - If **type** is set to **OTHER**, the following parameters are returned:
 - **certificate_chain**: indicates the certificate chain in PEM format.
 - **certificate**: indicates the signature certificate content in PEM format.
 - **enc_certificate**: indicates the encryption certificate content in PEM format.
 - **enc_private_key**: indicates the private key of the encryption certificate in PEM format.

 NOTE

Only certificates in the **Issued** status can be exported.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:export	Read	-	g:EnterpriseProjectId	-	-

URI

POST /v1/private-certificates/{certificate_id}/export

Table 4-261 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	ID of the private certificate you want to export. Minimum: 36 Maximum: 36

Request Parameters

Table 4-262 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-263 Request body parameters

Parameter	Mandatory	Type	Description
is_compressed	Yes	String	Whether to compress. • true • false

Parameter	Mandatory	Type	Description
type	Yes	String	Type of the server on which the certificate is installed. The options are as follows: • APACHE: This parameter is recommended for Apache servers. • NGINX: This parameter is recommended for Nginx servers. - IIS: This parameter is recommended for Windows servers. - TOMCAT: This parameter is recommended for Tomcat servers. • ** OTHER**: This parameter is recommended when you expect to download a certificate in PEM format.
password	No	String	The password used to encrypt private keys. It can contain letters, digits, and some special characters (.,+_-#.). It can contain a maximum of 32 characters. If you do not specify it, private keys will not be encrypted when you export them.

Response Parameters

Status code: 200

Table 4-264 Response body parameters

Parameter	Type	Description
private_key	String	Private key content.
certificate	String	Certificate content.
certificate_chain	String	Certificate chain content.

Status code: 400

Table 4-265 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-266** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-267** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-268 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-269** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/  
6434f74f-2d13-4e6a-89eb-93ee313f1a43/export
```

```
{  
  "type" : "other",  
  "is_compressed" : false,  
  "password" : "test"  
}
```

Example Responses

Status code: 200

Request succeeded.

```
{  
  "certificate" : "-----BEGIN CERTIFICATE-----\r\n*****\r\n-----END CERTIFICATE-----",  
  "certificate_chain" : "-----BEGIN CERTIFICATE-----\r\n*****\r\n-----END CERTIFICATE-----\r\n-----BEGIN  
CERTIFICATE-----\r\n*****\r\n-----END CERTIFICATE-----",  
  "private_key" : "-----BEGIN RSA PRIVATE KEY-----\r\n*****\r\n-----END RSA PRIVATE KEY-----\r\n"  
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.2.9 Revoking a Certificate

Function

This API is used to revoke a certificate.

NOTE

Note: If you do not want to provide the revocation reason, set the request body to `{}`. Otherwise, an error will be reported.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:revokeCert	Write	ca *	g:ResourceTag/<tag-key>	• pca:cert:revoke	-
		-	g:EnterpriseProjectId		

URI

POST /v1/private-certificates/{certificate_id}/revoke

Table 4-270 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	ID of the private certificate you want to revoke. Minimum: 36 Maximum: 36

Request Parameters

Table 4-271 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-272 Request body parameters

Parameter	Mandatory	Type	Description
reason	No	String	Reason for revocation. The options are as follows: • UNSPECIFIED: No revocation reason is specified during revocation. The default value is used. • KEY_COMPROMISE: The certificate key material is disclosed. • CERTIFICATE_AUTHORITY_COMPROMISE: CA key materials may be disclosed on the issuing path. • AFFILIATION_CHANGED: The subject or other information in the certificate has been changed. • SUPERSEDED: This certificate has been replaced. • CESSATION_OF_OPERATION: The entity in this certificate or issuing path has ceased to operate • CERTIFICATE_HOLD: The certificate is invalid at present and may take effect in the future. • PRIVILEGE_WITHDRAWN: The certificate no longer has the permission on the attributes it declares. • ATTRIBUTE_AUTHORITY_COMPROMISE: The certificate authority that warrants this certificate attribute may have been compromised. NOTE Note: If you do not want to provide the revocation reason, set the request body to "{}". Otherwise, an error will be reported. UNSPECIFIED is the default value.

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400

Table 4-273 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-274 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403

Table 4-275 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-276** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-277** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/6434f74f-2d13-4e6a-89eb-93ee313f1a43/revoke
{
  "reason": "KEY_COMPROMISE"
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.3 Certificate Revocation

4.2.3.1 Checking the Agency Permission

Function

This API is used to check whether you have the agency permission.

NOTE

Your token must have the **secu_admin** role assigned.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

GET /v1/private-certificate-authorities/obs/agencies

Request Parameters

Table 4-278 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-279 Response body parameters

Parameter	Type	Description
agency_granted	String	OBS agency status. • true • false

Status code: 400**Table 4-280** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-281** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403

Table 4-282 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-283** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-284** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you use this API to check whether PCA has the OBS agency permission (for accessing OBS buckets and updating the CRL), a token is required in the **X-Auth-Token** field in the request header, and the token must have the permission to access the API and the **secu_admin** permission.

GET https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/obs/agencies

Example Responses

Status code: 200

Request succeeded.

```
{
  "agency_granted" : "true"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.

Status Code	Description
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.3.2 Creating an Agency

Function

This API is used to create an OBS agency for PCA to access OBS buckets and update the CRL.

NOTE

Your token must have the **secu_admin** role assigned.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/private-certificate-authorities/obs/agencies

Request Parameters

Table 4-285 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200**Table 4-286** Response body parameters

Parameter	Type	Description
agency_id	String	Authorization ID returned by IAM when an OBS agency is created.

Status code: 400**Table 4-287** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-288 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-289** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-290** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-291 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you use this API to create an OBS agency (for accessing OBS buckets and updating the CRL) for PCA, a token is required in the **X-Auth-Token** field in the request header, and the token must have the permission to access the API and the **secu_admin** permission.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/obs/agencies
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "agency_id" : "078ade0fc20010004f8fc0034fad529d"
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.3.3 Querying the List of OBS Buckets

Function

This API is used to query the list of OBS buckets.

 NOTE

This API can be used only when an agency is created. For details about how to create an agency, see [Certificate Revocation > Creating an Agency](#) in this document.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

GET /v1/private-certificate-authorities/obs/buckets

Request Parameters

Table 4-292 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-293 Response body parameters

Parameter	Type	Description
total	Integer	Total number of the OBS buckets.
obs_buckets	Array of ObsBuckets objects	For details, see data structure for the ObsBuckets field. Array Length: 0 - 256

Table 4-294 ObsBuckets

Parameter	Type	Description
bucket_name	String	Bucket name Minimum: 3 Maximum: 63
create_time	Long	Creation time. The value is a timestamp in milliseconds.

Status code: 400**Table 4-295** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-296** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-297** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-298 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-299** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

GET <https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/obs/buckets>

Example Responses

Status code: 200

Request succeeded.

```
{
  "total" : 2,
  "obs_buckets" : [ {
    "create_time" : 1554867690718,
    "bucket_name" : "admin1"
  }, {
    "create_time" : 1554949519646,
    "bucket_name" : "admin3"
  } ]
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.3.4 Enabling a CRL

Function

This API is used to enable a CRL of the current CA.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:enableCrl	Write	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

POST /v1/private-certificate-authorities/{ca_id}/crl/enable

Table 4-300 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the certificate for the CA you want to enable a CRL for. Minimum: 36 Maximum: 36

Request Parameters

Table 4-301 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-302 Request body parameters

Parameter	Mandatory	Type	Description
crl_name	No	String	Name of the certificate revocation list. NOTE If you do not specify this parameter, the system uses the ID of the parent CA that issues the current certificate by default.
obs_bucket_name	Yes	String	OBS bucket name. NOTE - You must have created an agency and have PCA permissions on OBS granted to it. For details, see ** Certificate Revocation > Checking Permissions of an Agency ** and ** Certificate Revocation > Creating an Agency **. - The specified OBS bucket must exist. Otherwise, an error will be reported.
valid_days	Yes	Integer	CRL update interval, in days. Minimum: 7 Maximum: 30

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400

Table 4-303 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-304** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-305** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-306 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-307** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/crl/enable
```

```
{
  "crL_name" : "test",
  "obs_bucket_name" : "test",
  "valid_days" : 7
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.3.5 Disabling a CRL

Function

This API is used to disable a CRL of the current CA.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:disableCrl	Write	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

POST /v1/private-certificate-authorities/{ca_id}/crl/disable

Table 4-308 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the certificate for the CA you want to disable a CRL for. Minimum: 36 Maximum: 36

Request Parameters

Table 4-309 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400**Table 4-310** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-311** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-312** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-313** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-314** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/crl/disable
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.

Status Code	Description
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4 Tag Management

4.2.4.1 Batch Creating CA Tags

Function

This API is used to create CA tags in batches.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:createTag	Tagging	ca *	g:ResourceTag/<tag-key>	-	-

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
		-	- g:EnterpriseProjectId - g:RequestTag/<tag-key> - g:TagKeys		

URI

POST /v1/private-certificate-authorities/{ca_id}/tags/create

Table 4-315 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the certificate of the CA you want to create tags for. Minimum: 36 Maximum: 36

Request Parameters

Table 4-316 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-317 Request body parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array of ResourceTag objects	Tag list, which is a collection of key-value pairs. Array Length: 1 - 20

Table 4-318 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	Yes	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400

Table 4-319 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-320 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-321** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-322** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-323 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/tags/create

{
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value2"
  } ]
}
```

Example Responses

Status code: 400
Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401
Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403
Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.2 Batch Deleting Tags for a CA

Function

This API is used to delete tags in batches for a CA.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.

- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:deleteTag	Tagging	ca *	g:ResourceTag/<tag-key>	-	-
		-	- g:EnterpriseProjectId - g:TagKeys		

URI

DELETE /v1/private-certificate-authorities/{ca_id}/tags/delete

Table 4-324 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the certificate of the CA you want to delete tags for. Minimum: 36 Maximum: 36

Request Parameters

Table 4-325 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-326 Request body parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array of ResourceTag objects	Tag list, which is a collection of key-value pairs. Array Length: 1 - 20

Table 4-327 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	Yes	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400

Table 4-328 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-329** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-330** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-331** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-332 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

DELETE https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/tags/delete

```
{
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value2"
  } ]
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
}
```

```
"error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.3 Creating a Tag for a CA

Function

This API is used to create a tag for a specific CA.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:createTag	Tagging	ca *	g:ResourceTag/<tag-key>	-	-
		-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v1/private-certificate-authorities/{ca_id}/tags

Table 4-333 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the certificate for the CA you want to create a tag for. Minimum: 36 Maximum: 36

Request Parameters

Table 4-334 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-335 Request body parameters

Parameter	Mandatory	Type	Description
tag	Yes	ResourceTag object	Tag.

Table 4-336 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	Yes	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400**Table 4-337** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-338** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-339** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-340 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-341** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/tags

```
{
  "tag": {
    "key": "key1",
    "value": "value1"
  }
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Certification failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Certification failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.4 Querying the Tag List for a CA

Function

This API is used to query the tag list for a CA by its certificate ID.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:listTags	List	ca *	g:ResourceTag/<tag-key>	-	-
		-	g:EnterpriseProjectId		

URI

GET /v1/private-certificate-authorities/{ca_id}/tags

Table 4-342 Path Parameters

Parameter	Mandatory	Type	Description
ca_id	Yes	String	ID of the certificate for the target CA. Minimum: 36 Maximum: 36

Request Parameters

Table 4-343 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200**Table 4-344** Response body parameters

Parameter	Type	Description
tags	Array of ResourceTag objects	Tag list, which is a collection of key-value pairs. Array Length: 1 - 20

Table 4-345 ResourceTag

Parameter	Type	Description
key	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Status code: 400

Table 4-346 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-347** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-348** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-349 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-350** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
GET https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/tags
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value2"
  } ]
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.5 Querying the Tag List for All CAs

Function

This API is used to query the list of tags configured for all CAs.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:listAllTags	List	ca *	-	-	-

URI

GET /v1/private-certificate-authorities/tags

Request Parameters

Table 4-351 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-352 Response body parameters

Parameter	Type	Description
tags	Array of DomainTags objects	Tag list. Array Length: 1 - 20

Table 4-353 DomainTags

Parameter	Type	Description
key	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
values	Array of strings	Tag value list. Each value can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 0 Maximum: 255 Array Length: 1 - 20

Status code: 400**Table 4-354** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-355 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-356** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-357** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-358 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
GET https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/tags
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "tags": [ {
    "key": "key1",
    "values": [ "value1", "value2" ]
  }, {
    "key": "key2",
    "values": [ "value1", "value2" ]
  } ]
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.6 Querying the CA List by Tags

Function

This API is used to query the CA list by tags.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.

- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:listByTag	List	ca *	-	-	-
		-	- g:EnterpriseProjectId - g:RequestTag/<tag-key> - g:TagKeys		

URI

POST /v1/private-certificate-authorities/resource-instances/filter

Request Parameters

Table 4-359 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-360 Request body parameters

Parameter	Mandatory	Type	Description
tags	No	Array of DomainTags objects	Tag list. The list contains a maximum of 20 keys with each containing no more than 20 values. A key can have empty arrays, but must have the complete structure. Each tag key must be unique, and each tag value in a tag must be unique. The response returns resources containing all tags in this list. Keys in this list are in an AND relationship while values in each key-value structure are in an OR relationship. If no filtering condition is specified, full data is returned. Array Length: 1 - 20
limit	No	Integer	Records on each page. The values can be: • 10: Each page contains 10 resource records. • 20: Each page contains 20 resource records. • 50: Each page contains 50 resource records. Minimum: 10 Maximum: 50 Default: 10
offset	No	Integer	Index position. The query will start from the next records from the position specified by offset. Minimum: 0 Default: 0

Parameter	Mandatory	Type	Description
matches	No	Array of ResourceTag objects	The key-value pair to be matched. The tag key indicates the field to be matched, such as resource_name. The tag value indicates the value to be matched. The key is a fixed dictionary value and cannot be a duplicate key or unsupported key. Array Length: 0 - 20

Table 4-361 DomainTags

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
values	Yes	Array of strings	Tag value list. Each value can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 0 Maximum: 255 Array Length: 1 - 20

Table 4-362 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	Yes	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Response Parameters

Status code: 200

Table 4-363 Response body parameters

Parameter	Type	Description
total_count	Integer	Total number of records. Minimum: 0 Maximum: 100
resources	Array of TagResource objects	Resource instance list. For details, see the data structure of the TagResource field. Array Length: 0 - 100

Table 4-364 TagResource

Parameter	Type	Description
resource_id	String	Specifies the resource ID. Minimum: 0 Maximum: 63

Parameter	Type	Description
resource_detail	Object	Specifies resource details.
tags	Array of ResourceTag objects	Tag list. If there is no tag in the list, an empty array is returned. Array Length: 0 - 100
resource_name	String	Resource name. This parameter is an empty string by default. Minimum: 0 Maximum: 63

Table 4-365 ResourceTag

Parameter	Type	Description
key	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Status code: 400**Table 4-366** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-367** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-368** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-369** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-370 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/resource-instances/filter
{
  "tags": [ {
    "key": "key1",
    "values": [ "value1", "value2" ]
  } ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total_count": 1,
  "resources": [ {
    "resource_id": "806064a8-7478-4657-a8b0-2edc90621235"
  }, {
    "resource_name": "test"
  }, {
    "resource_detail": [ {
      "ca_id": "806064a8-7478-4657-a8b0-2edc90621235",
      "create_time": 1681436805000,
      "delete_time": null,
      "crl_configuration": {
        "enabled": false,
        "obs_bucket_name": null,
        "valid_days": null,
        "crl_name": null,
        "crl_dis_point": null
      },
      "distinguished_name": {
        "country": "CN",
        "state": "guangdong",
        "locality": "shenzhen",
        "organization": "Huawei",
        "organizational_unit": "IT",
        "common_name": "Huawei IT Root CA"
      },
      "enc_cert_info": null,
      "enterprise_project_id": "57d71362-6a1a-4f51-8fa9-693bc3c07f43",
      "freeze_flag": 0,
    } ],
  } ]
}
```

```
{
  "gen_mode": "GENERATE",
  "issuer_id": null,
  "issuer_name": null,
  "key_algorithm": "SM2",
  "not_before": 1681436805000,
  "not_after": 1713059205000,
  "path_length": 7,
  "serial_number": "202203070322544291829058",
  "signature_algorithm": "SM3",
  "status": "ACTIVED",
  "type": "ROOT"
}]
}, {
  "tags": [ {
    "key": "key1",
    "value": "value1"
  } ]
}]
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.7 Querying the CA Quantity by Tag

Function

This API is used to query the number of CAs by tag.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/private-certificate-authorities/resource-instances/count

Request Parameters

Table 4-371 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-372 Request body parameters

Parameter	Mandatory	Type	Description
tags	No	Array of DomainTags objects	Tag list. The list contains a maximum of 20 keys with each containing no more than 20 values. A key can have empty arrays, but must have the complete structure. Each tag key must be unique, and each tag value in a tag must be unique. The response returns resources containing all tags in this list. Keys in this list are in an AND relationship while values in each key-value structure are in an OR relationship. If no filtering condition is specified, full data is returned. Array Length: 1 - 20
limit	No	Integer	Records on each page. The values can be: • 10: Each page contains 10 resource records. • 20: Each page contains 20 resource records. • 50: Each page contains 50 resource records. Minimum: 10 Maximum: 50 Default: 10

Parameter	Mandatory	Type	Description
offset	No	Integer	Index position. The query will start from the next records from the position specified by offset . Minimum: 0 Default: 0
matches	No	Array of ResourceTag objects	The key-value pair to be matched. The tag key indicates the field to be matched, such as resource_name . The tag value indicates the value to be matched. The key is a fixed dictionary value and cannot be a duplicate key or unsupported key. Array Length: 0 - 20

Table 4-373 DomainTags

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
values	Yes	Array of strings	Tag value list. Each value can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 0 Maximum: 255 Array Length: 1 - 20

Table 4-374 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	Yes	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Response Parameters

Status code: 200

Table 4-375 Response body parameters

Parameter	Type	Description
total_count	Integer	Total number of records. Minimum: 0 Maximum: 100

Status code: 400

Table 4-376 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-377** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-378** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-379** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-380 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/resource-instances/count

```
{
  "tags": [ {
    "key": "key1",
    "values": [ "value1", "value2" ]
  } ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total_count": 1
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.8 Batch Creating Tags for a Certificate

Function

This API is used to create tags in batches for a certificate.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:createTag	Tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	-	-

URI

POST /v1/private-certificates/{certificate_id}/tags/create

Table 4-381 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	ID of the certificate you want to create tags for. Minimum: 36 Maximum: 36

Request Parameters

Table 4-382 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-383 Request body parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array of ResourceTag objects	Tag list, which is a collection of key-value pairs. Array Length: 1 - 20

Table 4-384 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	Yes	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400

Table 4-385 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-386 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403

Table 4-387 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-388 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-389** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/4c0e772e-a30c-4029-b929-b7acb04143f7/tags/create
```

```
{
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value2"
  } ]
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
}
```

```
"error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.9 Batch Deleting Tags for a Certificate

Function

This API is used to delete multiple tags for a certificate.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:deleteTag	Tagging	-	• g:EnterpriseProjectId • g:TagKeys	-	-

URI

DELETE /v1/private-certificates/{certificate_id}/tags/delete

Table 4-390 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	ID of the certificate you want to delete tags for. Minimum: 36 Maximum: 36

Request Parameters

Table 4-391 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-392 Request body parameters

Parameter	Mandatory	Type	Description
tags	Yes	Array of ResourceTag objects	Tag list, which is a collection of key-value pairs. Array Length: 1 - 20

Table 4-393 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	Yes	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400

Table 4-394 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401

Table 4-395 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403

Table 4-396 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-397 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-398** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
DELETE https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/4c0e772e-a30c-4029-b929-b7acb04143f7/tags/delete
```

```
{
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value2"
  } ]
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
}
```

```
{  
  "error_msg" : "XXX"  
}
```

Status code: 401

Token required for the requested page.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 403

Authentication failed.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 404

No resources available or found.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status code: 500

Internal service error.

```
{  
  "error_code" : "PCA.XXX",  
  "error_msg" : "XXX"  
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.10 Creating a Tag for a Certificate

Function

This API is used to create a tag for a certificate.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:createTag	Tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys	-	-

URI

POST /v1/private-certificates/{certificate_id}/tags

Table 4-399 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	ID of the certificate you want to create a tag for. Minimum: 36 Maximum: 36

Request Parameters

Table 4-400 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-401 Request body parameters

Parameter	Mandatory	Type	Description
tag	Yes	ResourceTag object	Tag.

Table 4-402 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	Yes	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Response Parameters

Status code: 204

Request succeeded, but no response body returned.

Status code: 400**Table 4-403** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-404** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-405** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-406 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-407** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/4c0e772e-a30c-4029-b929-b7acb04143f7/tags
```

```
{
  "tag": {
    "key": "key1",
    "value": "value1"
  }
}
```

Example Responses

Status code: 400

Invalid request parameters.

```
{
  "error_code": "PCA.XXX",
  "error_msg": "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
204	Request succeeded, but no response body returned.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.11 Querying the Tag List for a Certificate

Function

This API is used to query the tag lists for a certificate by its certificate ID.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:listTags	List	-	g:EnterpriseProjectId	-	-

URI

GET /v1/private-certificates/{certificate_id}/tags

Table 4-408 Path Parameters

Parameter	Mandatory	Type	Description
certificate_id	Yes	String	ID of the target certificate. Minimum: 36 Maximum: 36

Request Parameters

Table 4-409 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-410 Response body parameters

Parameter	Type	Description
tags	Array of ResourceTag objects	Tag list, which is a collection of key-value pairs. Array Length: 1 - 20

Table 4-411 ResourceTag

Parameter	Type	Description
key	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Status code: 400

Table 4-412 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-413** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-414** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-415** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-416 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
GET https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/4c0e772e-a30c-4029-b929-b7acb04143f7/tags
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  }, {
    "key" : "key2",
    "value" : "value2"
  } ]
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

```
{
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.12 Querying the Tag List for All Certificates

Function

This API is used to query the list of tags configured for all certificates.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:listAllTags	List	-	-	-	-

URI

GET /v1/private-certificates/tags

Request Parameters

Table 4-417 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200

Table 4-418 Response body parameters

Parameter	Type	Description
tags	Array of DomainTags objects	Tag list. Array Length: 1 - 20

Table 4-419 DomainTags

Parameter	Type	Description
key	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
values	Array of strings	Tag value list. Each value can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 0 Maximum: 255 Array Length: 1 - 20

Status code: 400**Table 4-420** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-421** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-422** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-423** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-424** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
GET https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/tags
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "tags" : [ {
    "key" : "key1",
    "values" : [ "value1", "value2" ]
  }, {
    "key" : "key2",
    "values" : [ "value1", "value2" ]
  } ]
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
}
```

```
"error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.13 Querying the Certificate List by Tag

Function

This API is used to query the certificate list by a specific tag.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:cert:listByTag	List	-	- g:EnterpriseProjectId - g:RequestTag/<tag-key> - g:TagKeys	-	-

URI

POST /v1/private-certificates/resource-instances/filter

Request Parameters

Table 4-425 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-426 Request body parameters

Parameter	Mandatory	Type	Description
tags	No	Array of DomainTags objects	Tag list. The list contains a maximum of 20 keys with each containing no more than 20 values. A key can have empty arrays, but must have the complete structure. Each tag key must be unique, and each tag value in a tag must be unique. The response returns resources containing all tags in this list. Keys in this list are in an AND relationship while values in each key-value structure are in an OR relationship. If no filtering condition is specified, full data is returned. Array Length: 1 - 20
limit	No	Integer	Records on each page. The values can be: • 10: Each page contains 10 resource records. • 20: Each page contains 20 resource records. • 50: Each page contains 50 resource records. Minimum: 10 Maximum: 50 Default: 10
offset	No	Integer	Index position. The query will start from the next records from the position specified by offset. Minimum: 0 Default: 0

Parameter	Mandatory	Type	Description
matches	No	Array of ResourceTag objects	The key-value pair to be matched. The tag key indicates the field to be matched, such as resource_name . The tag value indicates the value to be matched. The key is a fixed dictionary value and cannot be a duplicate key or unsupported key. Array Length: 0 - 20

Table 4-427 DomainTags

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
values	Yes	Array of strings	Tag value list. Each value can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 0 Maximum: 255 Array Length: 1 - 20

Table 4-428 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	Yes	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Response Parameters

Status code: 200

Table 4-429 Response body parameters

Parameter	Type	Description
total_count	Integer	Total number of records. Minimum: 0 Maximum: 100
resources	Array of TagResource objects	Resource instance list. For details, see the data structure of the TagResource field. Array Length: 0 - 100

Table 4-430 TagResource

Parameter	Type	Description
resource_id	String	Specifies the resource ID. Minimum: 0 Maximum: 63

Parameter	Type	Description
resource_detail	Object	Specifies resource details.
tags	Array of ResourceTag objects	Tag list. If there is no tag in the list, an empty array is returned. Array Length: 0 - 100
resource_name	String	Resource name. This parameter is an empty string by default. Minimum: 0 Maximum: 63

Table 4-431 ResourceTag

Parameter	Type	Description
key	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Status code: 400**Table 4-432** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-433** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-434** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-435** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-436 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/resource-instances/filter
{
  "tags" : [ {
    "key" : "key1",
    "values" : [ "value1", "value2" ]
  } ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total_count" : 1,
  "resources" : [ {
    "resource_id" : "61e1f947-8794-4574-82bd-14fd0cd3af67"
  }, {
    "resource_name" : "test"
  }, {
    "resource_detail" : [ {
      "certificate_id" : "61e1f947-8794-4574-82bd-14fd0cd3af67",
      "create_time" : 1681436805000,
      "delete_time" : null,
      "distinguished_name" : {
        "country" : "CN",
        "state" : "guangdong",
        "locality" : "shenzhen",
        "organization" : "Huawei",
        "organizational_unit" : "IT",
        "common_name" : "Huawei IT Root CA"
      },
      "enc_cert_info" : null,
      "enterprise_project_id" : "0",
      "freeze_flag" : 0,
      "gen_mode" : "GENERATE",
      "issuer_id" : "93fcdaf2-c094-4f39-9cbc-bcacd0baac48",
      "issuer_name" : "test",
      "key_algorithm" : "RSA2048",
      "not_before" : 1681436805000,
      "not_after" : 1713059205000,
      "path_length" : 7,
    } ],
  } ],
}
```

```
{
  "serial_number" : "202203070322544291829058",
  "signature_algorithm" : "SHA256",
  "status" : "ISSUED"
}]
}, {
  "tags" : [ {
    "key" : "key1",
    "value" : "value1"
  } ]
}]
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.

Status Code	Description
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.4.14 Querying the Certificate Quantity by Tags

Function

This API is used to query the number of the certificates by tags.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

POST /v1/private-certificates/resource-instances/count

Request Parameters

Table 4-437 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/intl/en-us/api-iam/iam_30_0001.html).

Table 4-438 Request body parameters

Parameter	Mandatory	Type	Description
tags	No	Array of DomainTags objects	Tag list. The list contains a maximum of 20 keys with each containing no more than 20 values. A key can have empty arrays, but must have the complete structure. Each tag key must be unique, and each tag value in a tag must be unique. The response returns resources containing all tags in this list. Keys in this list are in an AND relationship while values in each key-value structure are in an OR relationship. If no filtering condition is specified, full data is returned. Array Length: 1 - 20
limit	No	Integer	Records on each page. The values can be: • 10: Each page contains 10 resource records. • 20: Each page contains 20 resource records. • 50: Each page contains 50 resource records. Minimum: 10 Maximum: 50 Default: 10

Parameter	Mandatory	Type	Description
offset	No	Integer	Index position. The query will start from the next records from the position specified by offset . Minimum: 0 Default: 0
matches	No	Array of ResourceTag objects	The key-value pair to be matched. The tag key indicates the field to be matched, such as resource_name . The tag value indicates the value to be matched. The key is a fixed dictionary value and cannot be a duplicate key or unsupported key. Array Length: 0 - 20

Table 4-439 DomainTags

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
values	Yes	Array of strings	Tag value list. Each value can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 0 Maximum: 255 Array Length: 1 - 20

Table 4-440 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : = + - @ Minimum: 1 Maximum: 128
value	Yes	String	Tag value. It can contain letters in Chinese, Spanish, or Portuguese, digits, spaces, and the following characters in UTF-8 format: _ . : / = + - @ Minimum: 0 Maximum: 255

Response Parameters

Status code: 200

Table 4-441 Response body parameters

Parameter	Type	Description
total_count	Integer	Total number of records. Minimum: 0 Maximum: 100

Status code: 400

Table 4-442 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-443** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-444** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404**Table 4-445** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36

Parameter	Type	Description
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500

Table 4-446 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you call this API, a token with the permission to use this API is mandatory for the **X-Auth-Token** field.

```
POST https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificates/resource-instances/count
```

```
{
  "tags" : [ {
    "key" : "key1",
    "values" : [ "value1", "value2" ]
  } ]
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "total_count" : 1
}
```

Status code: 400

Invalid request parameters.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal service error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameters.
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal service error.

Error Codes

See [Error Codes](#).

4.2.5 Order Management

4.2.5.1 Purchasing a CA

Function

Purchase a CA.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, the following identity policy-based permissions are required.

Action	Access Level	Resource Type (*: required)	Condition Key	Alias	Dependencies
pca:ca:create	Write	ca *	-	-	-
		-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys		

URI

POST /v1/private-certificate-authorities/order

Request Parameters

Table 4-447 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/en-us/api-iam/iam_30_0001.html).

Table 4-448 Request body parameters

Parameter	Mandatory	Type	Description
cloud_service_type	Yes	String	Cloud service type. The fixed value is hws.service.type.ccm . Minimum: 1 Maximum: 64
charging_mode	Yes	Integer	Billing mode: - 0 : yearly/monthly
period_type	Yes	Integer	Subscription period type. The options are as follows: 2: month; 3: year.
period_num	Yes	Integer	Number of subscription periods.
is_auto_renew	Yes	Integer	Whether to enable auto-renewal. 1: yes; 0: no
promotion_info	No	String	Discount information. Minimum: 0 Maximum: 2048
subscription_num	Yes	Integer	Subscription quantity
is_auto_pay	No	Integer	Whether to perform automatic payment. 1: yes; 0: no. The default value is 0.
enterprise_project_id	No	String	Enterprise project ID. Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
product_infos	Yes	Array of ProductInfo objects	Product list. For details, see parameter description of the ProductInfo field. Array Length: 0 - 10

Table 4-449 ProductInfo

Parameter	Mandatory	Type	Description
cloud_service_type	Yes	String	Cloud service type. The fixed value is hws.service.type.ccm . Minimum: 1 Maximum: 64
resource_type	Yes	String	Resource type. The value of CA is hws.resource.type.pca.duration . Minimum: 1 Maximum: 64
resource_spec_code	Yes	String	Resource specification code. The value of CA is ca.duration . Minimum: 1 Maximum: 64

Response Parameters

Status code: 200

Table 4-450 Response body parameters

Parameter	Type	Description
order_id	String	Order ID. Minimum: 1 Maximum: 64
ca_ids	Array of strings	ID list of the purchased CA certificates. Minimum: 1 Maximum: 64

Status code: 400

Table 4-451 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-452** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-453** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-454 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-455** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you use this API to create a CA, a token is required in the **X-Auth-Token** field in the request header, and the token must have the permission to access the API.

POST <https://ccm.cn-north-4.myhuaweicloud.com/v1/private-certificate-authorities/order>

```
{
  "cloud_service_type" : "hws.service.type.ccm",
  "period_type" : 2,
  "period_num" : 1,
  "charging_mode" : 0,
  "is_auto_renew" : 0,
  "is_auto_pay" : 0,
  "promotion_info" : "",
  "enterprise_project_id" : "0",
  "product_infos" : [ {
    "cloud_service_type" : "hws.service.type.ccm",
    "resource_type" : "hws.resource.type.pca.duration",
    "resource_spec_code" : "ca.duration"
  } ],
  "subscription_num" : 1
}
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "order_id" : "CS1803192259ROA8U",
  "ca_ids" : [ "4284547e-68ef-4a94-adea-9df1e5d8ad65", "211c079c-bab8-41af-8948-c5e2531232c6" ]
}
```

Status code: 400

Invalid request parameter.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

Authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal server error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.

Status Code	Description
401	Token required for the requested page.
403	Authentication failed.
404	No resources available or found.
500	Internal server error.

Error Codes

See [Error Codes](#).

4.2.6 Querying Supported Features of a Site

4.2.6.1 Querying Supported Features in a Site

Function

This API is used to query supported features of a site.

Debugging

You can debug this API through automatic authentication in [API Explorer](#) or use the SDK sample code generated by API Explorer.

Authorization Information

Each account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions.

- If you are using role/policy-based authorization, see [Permissions Policies and Supported Actions](#) for details on the required permissions.
- If you are using identity policy-based authorization, no identity policy-based permission required for calling this API.

URI

GET /v1/pca/config/console

Request Parameters

Table 4-456 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. For details, see [Obtaining a User Token] (https://support.huaweicloud.com/en-us/api-iam/iam_30_0001.html).

Response Parameters

Status code: 200**Table 4-457** Response body parameters

Parameter	Type	Description
is_support_eps	Boolean	Whether enterprise projects are supported.
is_support_sm2	Boolean	Whether the SM2 algorithm is supported.
is_support_dhsm	Boolean	Whether the Dedicated HSM cluster is supported.
dhsm_regions	Array of strings	Regions supported by the Dedicated HSM cluster. Minimum: 1 Maximum: 64
is_support_yearly_monthly_ca	Boolean	Whether yearly/monthly CAs are supported.
is_support_iam5	Boolean	Whether IAM5 authentication is supported.
is_support_ocsp	Boolean	Whether OCSP queries are supported.

Status code: 400

Table 4-458 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 401**Table 4-459** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 403**Table 4-460** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 404

Table 4-461 Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Status code: 500**Table 4-462** Response body parameters

Parameter	Type	Description
error_code	String	Error code Minimum: 3 Maximum: 36
error_msg	String	Error message Minimum: 0 Maximum: 1024

Example Requests

When you use this API to query the supported features of a site, a token is required in the **X-Auth-Token** field in the request header, and the token must have the permission to access the API.

```
GET https://ccm.cn-north-4.myhuaweicloud.com/v1/ccm/config/console
```

Example Responses

Status code: 200

Request succeeded.

```
{
  "is_support_eps" : true,
  "is_support_sm2" : true,
  "is_support_dhsm" : false,
  "dhsm_regions" : [ "cn-north-4" ],
  "is_support_yearly_monthly_ca" : true,
  "is_support_iam5" : true,
  "is_support_ocsp" : true
}
```

Status code: 400

Invalid request parameter.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 401

Token required for the requested page.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 403

The authentication failed.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 404

No resources available or found.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status code: 500

Internal server error.

```
{
  "error_code" : "PCA.XXX",
  "error_msg" : "XXX"
}
```

Status Codes

Status Code	Description
200	Request succeeded.
400	Invalid request parameter.
401	Token required for the requested page.
403	The authentication failed.
404	No resources available or found.
500	Internal server error.

Error Codes

See [Error Codes](#).

5 Permissions and Supported Actions

5.1 Introduction to Permissions Policies and Supported Actions

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

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

Permissions are classified into based on the authorization granularity. Roles are a type of coarse-grained authorization mechanism that defines permissions related to user 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

Policy-based authorization is useful if you want to allow or deny the access to an API.

An account has all the permissions required to call all APIs, but IAM users must be assigned the required permissions. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions allowing the actions can call the API successfully. For example, if an IAM user queries ECSs using an API, the user must have been granted permissions that allow the **ecs:servers:list** action.

Supported Actions

CCM provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- **Permission:** A statement in a policy that allows or denies certain operations.

- APIs: REST APIs that can be called in a custom policy
- Actions: Added to a custom policy to control permissions for specific operations.
- Dependent actions: When assigning an action to users, you also need to assign dependent permissions for that action to take effect.
- IAM projects or enterprise projects: Scope of users a permission is granted to. Policies that contain actions supporting both IAM and enterprise projects can be assigned to user groups and take effect in both IAM and Enterprise Management. Policies that only contain actions supporting IAM projects can be assigned to user groups and only take effect for IAM. Such policies will not take effect if they are assigned to user groups in Enterprise Management.

 NOTE

√: supported; x: not supported

CCM supports the following actions that can be defined in custom policies:

5.2 Private Certificate Authority (PCA)

Authorization information about APIs related to private CAs

Permission	API	Action
Creating a CA	POST /v1/private-certificate-authorities	pca:ca:create
Canceling the scheduled deletion of a CA	POST /v1/private-certificate-authorities/{ca_id}/restore	pca:ca:restore
Querying details about a private CA	GET /v1/private-certificate-authorities/{ca_id}	pca:ca:get
Querying CSR details about a private CA	GET /v1/private-certificate-authorities/{ca_id}/csr	pca:ca:getCsr
Querying the private CA quota	GET /v1/private-certificate-authorities/quotas	pca:ca:quota
Exporting a private CA	POST /v1/private-certificate-authorities/{ca_id}/export	pca:ca:export
Deleting a private CA	DELETE /v1/private-certificate-authorities/{ca_id}	pca:ca:delete
Disabling a private CA	POST /v1/private-certificate-authorities/{ca_id}/disable	pca:ca:disable

Permission	API	Action
Enabling a private CA	POST /v1/private-certificate-authorities/{ca_id}/enable	pca:ca:enable
Activating a private CA	POST /v1/private-certificate-authorities/{ca_id}/activate	pca:ca:active
Importing a CA	POST /v1/private-certificate-authorities/{ca_id}/import	pca:ca:import
Querying the private CA list	GET /v1/private-certificate-authorities	pca:ca:list

Authorization information about APIs related to private certificates

Permission	API	Action
Querying details about a private certificate	GET /v1/private-certificates/{certificate_id}	pca:cert:get
Parsing the CSR of a private certificate	POST /v1/private-certificates/csr/parse	pca:cert:parseCsr
Exporting a private certificate	POST /v1/private-certificates/{certificate_id}/export	pca:cert:export
Querying the private certificate quota	GET /v1/private-certificates/quotas	pca:cert:quota
Creating a private certificate	POST /v1/private-certificates	pca:ca:issueCert
Deleting a private certificate	DELETE /v1/private-certificates/{certificate_id}	pca:ca:delete
Revoking a private certificate	POST /v1/private-certificates/{certificate_id}/revoke	pca:cert:revoke

Permission	API	Action
Creating a private certificate through a CSR	POST /v1/private-certificates/csr	pca:ca:issueCertThroughCSR
Querying the list of private certificates	GET /v1/private-certificates	pca:cert:list

A Appendix

A.1 Status Codes

Statues Codes to Private Certificate Management APIs

Status Codes	Status	Description
200	OK	Request processed successfully.
201	Created	Resource created.
204	NO Content	Request succeeded. No response body is returned.
400	Bad Request	The request parameter is incorrect.
401	Unauthorized	Incorrect or illegal client authentication information.
403	Forbidden	The server understood the request, but is refusing to fulfill it.
404	Not Found	The requested resource does not exist or not found.
500	Internal Server Error	Internal service error.

A.2 Error Codes

A.2.1 SCM Error Codes

Status Code	Error Codes	Error Message	Description	Solution
400	SCM.0003	Tenant has no privilege.	User information is not according with information of cert Owner	Please operate your own certificate.
400	SCM.0005	Incorrect request parameter.	Incorrect request parameter	Enter a valid request parameter.
400	SCM.0006	The uploaded certificate failed to be resolved. Ensure that the uploaded certificate has been issued.	Fail to parse certificate	Please upload the issued certificate.
400	SCM.0008	Abnormal certificate ID	Abnormal certificate ID	Enter a correct certificate ID.
400	SCM.0009	Failed to upload the certificate because no domain name is bound to the certificate.	Failed to upload the certificate. No domain name is bound to the certificate.	Associate the domain name with the certificate before uploading.
400	SCM.0010	This operation is not allowed by the current certificate type or status.	The type or the current status of the certificate does not support this operation.	Enter a certificate type or a certificate status that supports this operation.

Status Code	Error Codes	Error Message	Description	Solution
400	SCM.0011	The max number of free certificates for the current user has been reached, and you cannot continue to purchase free certificates.	The max number of free certificates for the current user has been reached, and you cannot continue to purchase free certificates.	Please dont add further certificates.
400	SCM.0012	The uploaded private key failed to be resolved. Ensure that the certificate has been issued.	The uploaded private key failed to be resolved. Ensure that the uploaded certificate has been issued.	Enter a valid certificate private key.
400	SCM.0014	The uploaded certificate does not match the private key.	The uploaded certificate does not match the uploaded private key.	Upload a valid certificate and private key.
400	SCM.0015	The number or format of domain names entered does not meet the requirements of the your certificate.	The number or format of the domains you entered is not in accordance with requirements of your certificate.	Upload a single-domain or multiple-domain certificate.
400	SCM.0016	Failed to order.	Failed to order.	Please contact technical support.
400	SCM.0020	Incorrect certificate ID.	Incorrect cert ID.	Upload a valid certificate ID.
400	SCM.0023	Modify key format error.	Modify key format error.	Please input nonNull key.
400	SCM.0024	Modify value format error.	Modify value format error.	Please input nonNull value.

Status Code	Error Codes	Error Message	Description	Solution
400	SCM.0025	Exceed the limit	Exceed the limit	The certificate exceeds the re-sign period
400	SCM.0026	Revoke cert error	Revoke cert error	Please contact technical support.
400	SCM.0027	Have no revoke reason	Have no revoke reason	Please input revoke reason.
400	SCM.0028	Push cert error	Push cert error	Please contact technical support.
400	SCM.0030	Certificates cannot be pushed to this service.	Unsupported push service error	Enter a correct service name to which the certificate is pushed.
400	SCM.0031	Certificate parsing error.	Parse certificate error.	Upload a correct certificate.
400	SCM.0032	Incorrect certificate name.	Invalid certificate name.	Enter a valid certificate name.
400	SCM.0033	Csr not bind domain.	Csr not bind domain.	Enter a valid csr with domain.
400	SCM.0034	Csr parse error.	Csr parse error.	Enter a valid csr.
400	SCM.0035	Csr domain not match input domain.	Csr domain not match input domain.	Keep the domain names the same
400	SCM.0036	Domain number not match product.	Domain number not match product.	Please enter the correct number of domain names
400	SCM.0039	The updated quota value must be greater than the currently used quota.	The updated quota value must be greater than the currently used quota.	Please input correct quota value.
400	SCM.0042	Cert has expired.	Cert has expired.	Please dont upload expired cert.

Status Code	Error Codes	Error Message	Description	Solution
400	SCM.0044	Permission denied,please obtain {0} permission.	Permission denied,please obtain {0} permission.	Please obtain permission first.
400	SCM.0049	Cert brand error.	Cert brand error.	Please enter cert brand.
400	SCM.0050	Cert type error.	Cert type error.	Please enter correct cert type.
400	SCM.0051	Domain type error.	Domain type error.	Please enter correct domain type.
400	SCM.0052	Cert effective time error.	Cert effective time error.	Please enter correct cert.
400	SCM.0059	The certificate private key is empty.	No certificate private key found.	Contact the customer service.
400	SCM.0060	Order number error.	Order number error.	Please enter right order number.
400	SCM.0061	Region parameter error.	Region parameter error.	Please enter right region.
400	SCM.0063	Duplicate domain error.	Duplicate domain error.	Please enter unique domain.
400	SCM.0064	The order is executing.	The order is executing.	Please do not place repeated orders.
400	SCM.0065	File size exceeds limit.	File size exceeds limit.	Please enter the correct size file.
400	SCM.0066	Current domain type not allowed to operate.	Current domain type not allowed to operate.	Contact the customer service.
400	SCM.0067	Sans changed.	Sans changed.	Please enter correct sans.
400	SCM.0068	Unsupported region.	Unsupported region.	Please contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
400	SCM.0070	Incorrect format of the domain bound to the certificate to be uploaded.	The format of the domain bound to the certificate is incorrect.	Upload a valid certificate.
400	SCM.0072	SCM does not support this status.	SCM does not support this status.	Please contact technical support.
400	SCM.0073	Help content format error.	Help content format error.	Please enter right content.
400	SCM.0074	Cert is not renewal paid.	Cert is not renewal paid.	Please contact technical support.
400	SCM.0075	Invalid region id.	Invalid region id.	Please enter valid region id.
400	SCM.0076	DIGICERT DV basic not support to renew.	DIGICERT DV basic not support to renew.	Contact the customer service.
400	SCM.0079	Subject of CaCert not match issuer of Cert	Subject of CaCert not match issuer of Cert	Please contact technical support.
400	SCM.0080	Required param cert_info is null or empty.	Required param cert_info is null or empty.	Please enter nonNull cert info.
400	SCM.0081	Required param cert_info is null or empty.	Required param cert_info is null or empty.	Please enter nonNull cert info.
400	SCM.0082	Invalid validity_period, should be 12.	Invalid validity_period, should be 12.	Please enter valid filed.
400	SCM.0083	Required param first_name is null or empty.	Required param first_name is null or empty.	Please enter nonNull filed.

Status Code	Error Codes	Error Message	Description	Solution
400	SCM.0085	Required param phone is null or empty.	Required param phone is null or empty.	Please enter nonNull filed.
400	SCM.0086	Required param email is null or empty.	Required param email is null or empty.	Please enter nonNull filed.
400	SCM.0095	Run RmsApiController failed.	Run RmsApiController failed.	Please contact technical support.
400	SCM.0101	The cert not support to auto deploy.	The cert not support to auto deploy.	Contact the customer service.
400	SCM.0102	This resource has been open to auto deploy.	This resource has been open to auto deploy.	Please do not repeat the operation.
400	SCM.0103	This resource is not exist.	This resource is not exist.	Please do not operate resource that do not exist.
400	SCM.0104	This region is not support.	This region is not support.	Please do not operate unsupported region.
400	SCM.0105	The cert has associated the auto deployed resources.	The cert has associated the auto deployed resources.	Contact the customer service.
400	SCM.0106	The resource domain is not equals the cert.	The resource domain is not equals the cert.	Please enter right domain.
400	SCM.0108	Domain format is invalid.	Domain format is invalid.	Please enter right domain.
400	SCM.0109	Cert chain length must be more than 1.	Cert chain length must be more than 1.	Please contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
400	SCM.0201	Failed to push to ELB.	Failed to push to ELB. Error message returned.	Contact the customer service.
400	SCM.0202	Insufficient ELB permissions	Insufficient ELB permissions	Configure required ELB permissions.
400	SCM.0204	ELB does not support this region.	ELB does not support this region.	Please choose other supported region.
400	SCM.0211	Failed to push to CDN.	Failed to push to CDN. Error message returned.	Contact the customer service.
400	SCM.0212	Insufficient CDN permissions	Insufficient CDN permissions	Configure required CDN permissions.
400	SCM.0221	Failed to push to WAF.	Failed to push to WAF. Error message returned.	Contact the customer service.
400	SCM.0222	Insufficient WAF permissions	WAF permission denied	Configure required WAF permissions.
400	SCM.0224	WAF does not support this region.	WAF does not support this region.	Please choose other supported region.
400	SCM.0225	Insufficient WAF quota.	Insufficient WAF quota.	Contact the customer service.
400	SCM.0301	Tag is not found.	Tag is not found.	Contact the customer service.
400	SCM.0302	Tag quota is upper limit.	Tag quota is upper limit.	Please dont add tag.
400	SCM.0303	Match tag invalid.	Match tag invalid.	Please add valid tag.
400	SCM.0304	Field action is error.	Field action is error.	Contact the customer service.
400	SCM.0305	Tag value is invalid.	Tag value is invalid.	Please enter valid tag value.

Status Code	Error Codes	Error Message	Description	Solution
400	SCM.0306	Tag key is invalid.	Tag key is invalid.	Please enter valid tag key.
400	SCM.0309	Tag value length is invalid.	Tag value length is invalid.	Please enter tag value with valid length.
400	SCM.0310	Tag key length is invalid.	Tag key length is invalid.	Please enter tag key with valid length.
400	SCM.0311	Tag key list is invalid.	Tag key list is invalid.	Please enter valid tag key list.
400	SCM.0312	Tag value list is invalid.	Tag value list is invalid.	Please enter valid tag value list.
400	SCM.0313	Tag list is invalid.	Tag list is invalid.	Please enter valid tag list.
400	SCM.0314	Match resourceId invalid.	Match resourceId invalid.	Contact the customer service.
400	SCM.0318	Tag limit invalid.	Tag limit invalid.	Please enter valid parameter.
400	SCM.0319	Tag offset invalid.	Tag offset invalid.	Please enter valid parameter.
400	SCM.0321	Invalid param sys_tags.	Invalid param sys_tags.	Please enter valid parameter.
400	SCM.0323	Invalid tag parameter.	Invalid tag parameter.	Please enter valid parameter.
400	SCM.0401	Gm cert is not support to be pushed.	Gm cert is not support to be pushed.	Please contact technical support.
400	SCM.0501	The parameter cannot be null or the parameter is wrong. Currently only supports:	The parameter cannot be null or the parameter is wrong. Currently only supports:	Only Support WAF/CDN/ELB.
400	SCM.0502	The certificate ID list cannot be empty.	The certificate ID list cannot be empty.	Please enter nonNull certificate ID list.

Status Code	Error Codes	Error Message	Description	Solution
400	SCM.0505	Parameter error, parameter is null or its list size is out of range, additional info:{0}	Parameter error, parameter is null or its list size is out of range	Please enter list with length less than 51 and more than 0
400	SCM.0506	There is no corresponding certificate ID under the tenant, and the set of certificate IDs that cannot be found:{0}	There is no corresponding certificate ID under the tenant	Please contact technical support.
400	SCM.0507	The list parameter cannot have duplicate elements	The list parameter cannot have duplicate elements, parameter name:{0}	Please enter unique parameter.
400	SCM.0508	Parameter error, the following certificates do not support querying deployed resources:{0}	Parameter error, the following certificates do not support querying deployed resources	Please enter valid cert.
401	SCM.0092	Decrypt jwt token failed.	Decrypt jwt token failed.	Please contact technical support.
401	SCM.1000	The token of the request fails to be authenticated	The token of the request fails to be authenticated	Enter a correct token.
401	SCM.1004	Failed to apply for OBT.	Failed to apply for OBT.	Apply for OBT.
401	SCM.1009	Your account is restricted.	The account is restricted	Contact the administrator for unfreezing.

Status Code	Error Codes	Error Message	Description	Solution
401	SCM.1010	Your account is frozen.	The account is frozen	Contact the administrator for unfreezing.
401	SCM.4002	You do not have permission to perform this operation.	You do not have permission to perform this operation.	Contact the administrator to obtain the permission.
403	SCM.0001	Service is not open.	Service is not open	Please contact technical support.
403	SCM.0002	Incorrect tenant ID.	Incorrect tenant ID or domain ID	Ensure that the projectId that matches the projectId in X-Auth-Token.
403	SCM.0040	The max number of free certificates for the current user has been reached, and you cannot continue to purchase free certificates.	The max number of free certificates for the current user has been reached, and you cannot continue to purchase free certificates.	Please stop buying free cert.
403	SCM.0322	Invalid user token, user role don't contain op_service.	Invalid user token, user role don't contain op_service.	Contact the customer service.
403	SCM.1019	The user role has no permission to access the interface	The user role has no permission to access the interface	Please contact technical support.
404	SCM.0069	No projects found.	No projects found.	Select a valid project.
404	SCM.0094	Resource not found.	Resource not found.	Please contact technical support.
500	SCM.0004	Fail to get ca response.	Fail to request from ca	Please contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
500	SCM.0007	Failed to download the certificate.	Failed to download the certificate.	Contact the customer service.
500	SCM.0013	The uploaded certificate chain failed to be resolved. Ensure that the certificate has been issued.	The uploaded certificate chain failed to be resolved. Ensure that the uploaded certificate has been issued.	Enter a correct certificate chain.
500	SCM.0017	product wrong.	product wrong.	Please contact technical support.
500	SCM.0019	CSB response error.	CSB response error.	Please contact technical support.
500	SCM.0037	Failed to encrypt the certificate.	Failed to encrypt the certificate.	Contact the customer service.
500	SCM.0038	Cert decrypt fail.	Cert decrypt fail.	Please contact technical support.
500	SCM.0062	DNS query fail.	DNS query fail.	Please contact technical support.
500	SCM.0071	SCM does not support this resourceType.	SCM does not support this resourceType.	Please contact technical support.
500	SCM.0087	Request cert failed.	Request cert failed.	Please contact technical support.
500	SCM.0091	Connect jwt server failed.	Connect jwt server failed.	Please contact technical support.
500	SCM.0093	Invalid jwt token.	Invalid jwt token.	Please contact technical support.
500	SCM.0097	Encode next token failed.	Encode next token failed.	Please contact technical support.
500	SCM.0098	Decode next token failed.	Decode next token failed.	Please contact technical support.
500	SCM.0099	Invalid domain id.	Invalid domain id.	Please enter valid domain id.
500	SCM.0100	UnKnown error.	UnKnown error.	Please contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
500	SCM.0203	Failed to push to ELB.	Failed to push to ELB.	Contact the customer service.
500	SCM.0213	Failed to push to CDN.	CDN push failed	Contact the customer service.
500	SCM.0223	Failed to push to WAF.	WAF push failed	Contact the customer service.
500	SCM.0324	Calculate digest failure.	Calculate digest failure.	Please contact technical support.
500	SCM.0402	Encrypt cert content or private key is null.	Encrypt cert content or private key is null.	Please contact technical support.
500	SCM.0504	Service internal error, please contact technical support.	Service internal error, please contact technical support.	Please contact technical support.
500	SCM.4001	An error occurred when accessing the PDP API.	Failed to obtain fine-grained permission.	Contact the customer service.

A.2.2 PCA Error Codes

Status Code	Error Codes	Error Message	Description	Solution
400	PCA.00020001	Incorrect parameter.	Incorrect parameter.	Please confirm whether the input parameters are correct.
400	PCA.00020101	Incorrect certificate distinguished name.	Incorrect certificate distinguished name.	Please confirm whether all fields in the parameter distinguished_name meet the requirements.

Status Code	Error Codes	Error Message	Description	Solution
400	PCA.00020102	Invalid key algorithm. Only RSA2048, RSA4096, EC256, and EC384 are supported.	Invalid key algorithm. Only RSA2048, RSA4096, EC256, and EC384 are supported.	Please confirm whether the key algorithm input is correct.
400	PCA.00020103	Invalid signature hash algorithm. Only SHA256, SHA384, and SHA512 are supported.	Invalid signature hash algorithm. Only SHA256, SHA384, and SHA512 are supported.	Please confirm whether the entered signature hash algorithm is correct.
400	PCA.00020109	Invalid validity period type or value. Only year, month, or day supported.	Invalid validity period type or value. Only year, month, or day supported.	Please confirm whether the validity period type and value entered are correct.
400	PCA.00020110	Incorrect domain name.	Incorrect domain name.	Please confirm that the length of the entered domain name is in the range of [1,64] and conforms to the domain name rules.
400	PCA.00020111	Invalid IP. Enter an IPv4 address.	Invalid IP. Enter an IPv4 address.	Please confirm that the IP address conforms to IPv4 rules.
400	PCA.00020112	Invalid alternative name type of the certificate subject. Enter an IP or DNS.	Invalid alternative name type of the certificate subject. Enter an IP or DNS.	Please confirm that the type is IP or DNS.

Status Code	Error Codes	Error Message	Description	Solution
400	PCA.00020201	Invalid CA ID. Valid CA IDs use a hexadecimal xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx format.	Invalid CA ID. Valid CA IDs use a hexadecimal xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx format.	Please enter the correct CA certificate ID.
400	PCA.00020202	Invalid CA type. Only root CA and subordinate CA are supported.	Invalid CA type. Only root CA and subordinate CA are supported.	Invalid CA type. Only root CA and subordinate CA are supported.
400	PCA.00020203	Invalid CA path length. The value range is [0, 6].	Invalid CA path length. The value range is [0, 6].	Please confirm whether the length of the entered CA path is correct. The value range of the CA path is [0,6].
400	PCA.00020204	Invalid CRL configuration.	Invalid CRL configuration.	Please check whether the entered certificate revocation list configuration is correct, including the OBS bucket name, CRL file name and the value range of the update cycle [7,30].
400	PCA.00020301	Invalid certificate ID. Valid certificate IDs use a hexadecimal xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx format.	Invalid certificate ID. Valid certificate IDs use a hexadecimal xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx format.	Please enter the correct certificate ID.

Status Code	Error Codes	Error Message	Description	Solution
400	PCA.00020401	Incorrect certificate signature request.	Incorrect certificate signature request.	Please check that the certificate signing request is correct.
400	PCA.00020402	Incorrect certificate. Please contact technical support.	Incorrect certificate. Please contact technical support.	Please contact technical support.
400	PCA.00020403	Incorrect certificate chain.	Incorrect certificate chain.	Please confirm that the certificate chain entered meets the requirements: 1. The format should be correct. When requesting through API, you need to use " 2. The certificate chain should be complete. Some intermediate CA certificates cannot be missing. The order is: intermediate CA >... > Root ca. " or "\r " instead of line feed;

Status Code	Error Codes	Error Message	Description	Solution
400	PCA.00020404	Invalid status. The status can only be Pending activation, Activated, Disabled, Pending deletion, or Expired.	Invalid status. The current support status is PENDING, ACTIVED, DISABLED, DELETED, and EXPIRED.	Please enter a valid status value. The currently supported status values are: PENDING, ACTIVED, DISABLED, DELETED, EXPIRED.
401	PCA.00000101	Access Denied. No permissions granted for this OBT.	Access Denied. No permissions granted for this OBT.	Please apply for public beta permission.
401	PCA.00010001	Incorrect X-Auth-Token in the request header.	Incorrect X-Auth-Token in the request header.	Please check: 1. Check whether the token is obtained according to the interface provided by the Identity and Access Management(IAM); 2. Check whether the token has expired. If the problem is not solved after checking the above conditions, please contact technical support.
401	PCA.00010002	Account frozen. Please contact technical support.	Account frozen. Please contact technical support.	Please contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
401	PCA.00010003	Access denied. Real-name authentication failed or account in arrears.	Access denied. Real-name authentication failed or account in arrears.	Please confirm whether the account has been authenticated by real name and whether it is in arrears. If it is still not resolved, please contact technical support.
401	PCA.00010004	Insufficient permissions. Contact administrator.	Insufficient permissions. Contact administrator.	Please contact the account administrator to confirm the account permissions. If the problem is still not resolved, please contact technical support.
403	PCA.00000006	Obtaining OBS buckets failed. Please contact technical support.	Obtaining OBS buckets failed. Please contact technical support.	Please contact technical support.
403	PCA.00030001	CA or certificate quantity exceeds quota.	CA or certificate quantity exceeds quota.	Please check whether the number of CAs that have been created or the number of certificates that have been applied for has reached the maximum value. If you need to increase the quota, please contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
403	PCA.00030201	Operation not allowed in the current status.	Operation not allowed in the current status.	There are restrictions on the operations that the CA or certificate is allowed to perform in different states, please check the conditions of the operations: 1. Disable CA: CA status must be in "ACTIVED" or "EXPIRED" status; 2. Enable CA: CA status must be in "DISABLED" status; 3. Delete CA: CA status must be in "PENDING" or "DISABLED" status; 4. Restore CA: CA status needs to be in "DELETED" status; 5. Export the CSR of the CA: the CA status needs to be in the "PENDING" state; 6. Export CA certificate: CA status needs to be in "ACTIVED" or "EXPIRED" status; 7. Activate CA: The CA status needs to be in the "PENDING" state;

Status Code	Error Codes	Error Message	Description	Solution
				8. Applying for a certificate: The issuing CA status needs to be in the "ACTIVED" status; 9. Export certificate: The certificate status needs to be in the "ISSUED" status. If the problem is not resolved after checking the operating conditions, please contact technical support.
403	PCA.0003020 2	CA or certificate frozen. Contact administrator.	CA or certificate frozen. Contact administrator.	Please contact technical support.
403	PCA.0003030 1	Certificate public key and private key does not match.	Certificate public key and private key does not match.	If this error message appears when importing a CA certificate, please check whether the CSR of the generated certificate is derived from the CA.
404	PCA.0003010 2	CA or certificate is not found.	CA or certificate is not found.	Please confirm that the CA or certificate already exists.
404	PCA.0003010 3	Issuer CA is not found	Issuer CA is not found	Please confirm that the specified issuing CA has been created and the status is "ACTIVED".

Status Code	Error Codes	Error Message	Description	Solution
500	PCA.00000001	Unknown error. Please contact technical support.	Unknown error. Please contact technical support.	Please contact technical support.
500	PCA.00000002	Parameter processing failed. Please contact technical support.	Parameter processing failed. Please contact technical support.	Please contact technical support.
500	PCA.00000003	Certificate processing failed. Please contact technical support.	Certificate processing failed. Please contact technical support.	Please contact technical support.
500	PCA.00000004	Key processing failed. Please contact technical support.	Key processing failed. Please contact technical support.	Please contact technical support.
500	PCA.00000005	Authentication failed. Please contact technical support.	Authentication failed. Please contact technical support.	Please contact technical support.

A.3 Obtaining a Project ID

Scenario

A project ID is required for some URLs when an API is called. Obtain the required project ID using either of the following methods:

- [Obtaining a Project ID by Calling an API](#)
- [Obtaining a Project ID from the Console](#)

Obtaining a Project ID by Calling an API

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

The API used to obtain a project ID is GET `https://{Endpoint}/v3/projects`. **{Endpoint}** is the IAM endpoint and can be obtained from the administrator. For details about API authentication, see [Authentication](#).

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

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

1. Log in to the management console.
2. Hover the cursor over the username in the upper right corner and select **My Credentials** from the drop-down list.

On the **API Credentials** page, view the project ID in the project list.

Figure A-1 Viewing project IDs

