## Cloud Certificate Manager

# API Reference

| | |
|---|---|
| **Issue** | 03 |
| **Date** | 2023-05-16 |

HUAWEI TECHNOLOGIES CO., LTD.

## Trademarks and Permissions

## Notice

The purchased products, services and features are stipulated by the contract made between Huawei 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

## 1.1 Overview

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?**

## 1.2 API Calling

CCM supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS. For details about API calling, see **Calling APIs**.

## 1.3 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. You can obtain CCM endpoints at **Regions and Endpoints**.

**Table 1-1** CCM endpoints

| Region | Endpoint Region | Endpoint | Protocol | Included Microservices |
|---|---|---|---|---|
| All | All | scm.ap-southeast-1.myhuaweicloud.com | HTTPS | SCM |

| Region | Endpoint Region | Endpoint | Protocol | Included Microservices |
|---|---|---|---|---|
| All | ALL | ccm.ap-southeast-3.myhuaweicloud.com | HTTPS | PCA |

## 1.4 Concepts

- Account

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

- User

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

  The account name, username, and password will be required for API authentication.

- Region

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

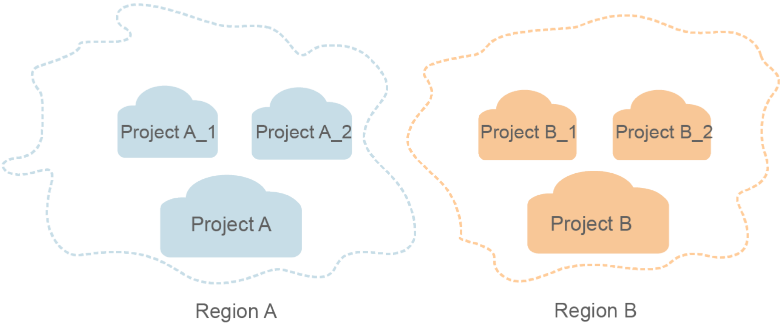
- Availability Zone (AZ)

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

- Project

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

**Figure 1-1** Project isolation model



- Enterprise project

  Enterprise projects group and manage resources across regions. Resources in enterprise projects are logically isolated from each other. An enterprise project can contain resources in multiple regions, and resources can be directly transferred between enterprise projects.

  For details about how to obtain enterprise project IDs and features, see **Enterprise Management User Guide**.

# 1.5 Selecting an API Type

For SSH key pairs, V2.1 and V2 API Types are available. It is recommended that you choose V2.1, which can better meet your demands.

# 2 Calling APIs

## 2.1 Making an API Request

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

### Request URI

A request URI is in the following format:

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

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

- **URI-scheme**:

  Protocol used to transmit requests. All APIs use HTTPS.

- **Endpoint**:

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

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

- **resource-path**:

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

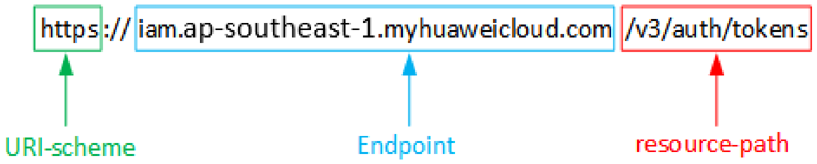
- **query-string**:

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

For example, to obtain an IAM token in the **CN-Hong Kong** region, obtain the endpoint of IAM (iam.ap-southeast-1.myhuaweicloud.com)) for this region and the **resource-path** (**/v3/auth/tokens**) in the URI of the API used to **obtain a user token**. Then, construct the URI as follows:

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

**Figure 2-1** Example URI



NOTE

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

## Request Methods

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

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

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

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

## Request Header

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

Common request header fields are as follows:

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

NOTE

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

For more information, see **AK/SK-based Authentication**.

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

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

## Request Body

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

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

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

NOTE

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

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

```
  }
}
```

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

# 2.2 Authentication

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

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

## Token-based Authentication

NOTE

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

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

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

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

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

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

### AK/SK-based Authentication

NOTE

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

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

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

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

NOTICE

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

## 2.3 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**.

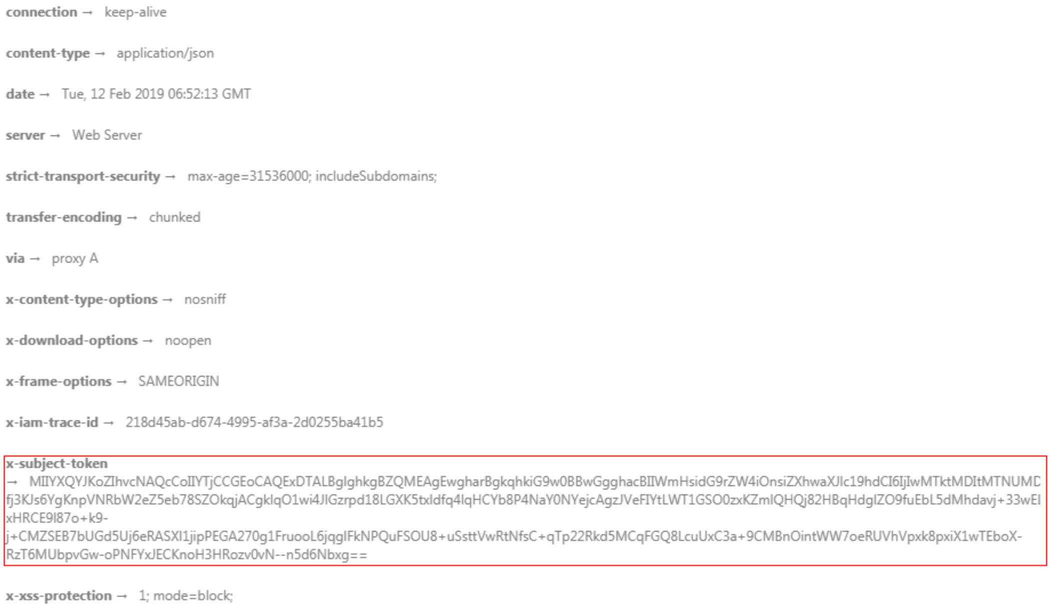
For example, if status code **201** is returned for calling the API used to **obtain a user token**, the request is successful.

### Response Header

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

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



```
connection → keep-alive

content-type → application/json

date → Tue, 12 Feb 2019 06:52:13 GMT

server → Web Server

strict-transport-security → max-age=31536000; includeSubdomains;

transfer-encoding → chunked

via → proxy A

x-content-type-options → nosniff

x-download-options → noopen

x-frame-options → SAMEORIGIN

x-iam-trace-id → 218d45ab-d674-4995-af3a-2d0255ba41b5

x-subject-token
→ MIIYXQYJKoZIhvcNAQcCoIIYTjCCGEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOnsiZXhwaXJlc19hdCI6IjIwMTktMDItMTNUMD
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkqjACgklqO1wi4JlGzrpd18LGXK5txldfq4lqHCYb8P4NaY0NYejcAgzJVeFIYtLWT1GSO0zxKZmIQHQj82HBqHdglZO9fuEbL5dMhdavj+33wEl
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jqglFkNPQuFSOU8+uSsttVwRtNfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUVhVpxk8pxiX1wTEboX-
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": "xxxxxxxx",
......
```

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

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

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

# 3 API Overview

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

## Managing SSL Certificates

| API | Description |
|---|---|
| **Querying the certification list** | Query the SSL certificate list. |
| **Importing an external certificate** | Import a certificate to SCM. |
| **Obtaining the certificate details** | Query details of an SSL certificate. |
| **Deleting a certificate** | Delete an SSL certificate. |
| **Exporting a certificate** | Export an SSL certificate. |
| **Pushing a certificate** | Push an SSL certificate to other Huawei Cloud services. |

## Managing Private Certificates

| API | Description |
|---|---|
| **Managing private CAs** | Manage private CAs, including creating, querying, and deleting private CAs. |
| **Managing private certificates** | Manage private certificates, including creating, querying, and deleting private certificates. |
| **Revoking a certificate** | Revoke certificates, including creating an agency, querying an agency, and querying the OBS bucket list. |

# 4 API Description

## 4.1 Managing SSL Certificates

## 4.1.1 Querying the Certificate List

### Function

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

### URI

GET /v3/scm/certificates

**Table 4-1** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| limit | No | Integer | Number of certificate records displayed on each page. The values can be：  - 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.<br>Minimum: **10**<br>Maximum: **50**<br>Default: **10** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| offset | No | Integer | Offset.<br>Minimum: **0**<br>Default: **0** |
| sort_dir | No | String | Sorting method. Sorting is performed based on the sorting parameter sort_key. The value can be: - ASC: Ascending order - DESC: descending order.<br>Default: **DESC**<br>Minimum: **0**<br>Maximum: **32** |
| sort_key | No | String | Parameter by which the certificates are sorted out. The value can be: - certExpiredTime: certificate expiration time. - certStatus: certificate status. - certUpdateTime: certificate update time.<br>Default: **certUpdateTime**<br>Minimum: **0**<br>Maximum: **64** |

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

## Request Parameters

**Table 4-2** Request header parameters

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

## Response Parameters

**Status code: 200**

**Table 4-3** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| certificates | Array of **CertificateDetail** objects | Certificate list. For details, see Data structure of the **CertificateDetail** field. |
| total_count | Integer | Number of certificates.<br>Minimum: **0**<br>Maximum: **10000** |

**Table 4-4** CertificateDetail

| Parameter | Type | Description |
|---|---|---|
| id | String | Certificate ID<br>Minimum: **16**<br>Maximum: **16** |
| name | String | Certificate name<br>Minimum: **1** |
| domain | String | Domain name associated with the certificate.<br>Minimum: **1**<br>Maximum: **255** |

| Parameter | Type | Description |
|---|---|---|
| sans | String | Additional domain name associated with the certificate<br>Minimum: **1**<br>Maximum: **4096** |
| signature_algorithm | String | Signature algorithm.<br>Minimum: **0**<br>Maximum: **64** |
| deploy_support | Boolean | Whether the certificate can be deployed to other services. |
| type | String | Certificate type. The value can be: **DV_SSL_CERT DV_SSL_CERT_BASIC EV_SSL_CERT EV_SSL_CERT_PRO OV_SSL_CERT OV_SSL_CERT_PRO**<br>Minimum: **1**<br>Maximum: **128** |
| brand | String | Certificate authority. The value can be: **GLOBALSIGN SYMANTEC GEOTRUST CFCA**.<br>Minimum: **1**<br>Maximum: **255** |
| expire_time | String | Certificate expiration time.<br>Minimum: **1**<br>Maximum: **32** |
| domain_type | String | Domain name type. The options are as follows:<br>● **SINGLE_DOMAIN**: Single domain names<br>● **WILDCARD**: Wildcard domain names<br>● **MULTI_DOMAIN**: Multiple domain names<br>Minimum: **1**<br>Maximum: **128** |
| validity_period | Integer | Certificate validity period, in months.<br>Minimum: **12**<br>Maximum: **12** |

| Parameter | Type | Description |
|---|---|---|
| status | String | Certificate status. The options are as follows:<br>● **PAID**: The certificate has been paid and needs to be applied for from the CA.<br>● **ISSUED**: The certificate has been issued.<br>● **CHECKING**: The certificate application is being reviewed.<br>● **CANCELCHECKING**: The certificate application cancellation is being reviewed.<br>● **UNPASSED**: The certificate application fails.<br>● **EXPIRED**: The certificate has expired.<br>● **REVOKING**: The certificate revocation application is being reviewed.<br>● **CANCLEREVOKING**: The cancellation on certificate revocation is being reviewed.<br>● **REVOKED**: The certificate has been revoked.<br>● **UPLOAD**: The certificate is being managed.<br>● **SUPPLEMENTCHECKING**: Additional domain names to be added for a multi-domain certificate are being reviewed.<br>● **CANCELSUPPLEMENTING**: The cancellation on additional domain names to be added is being reviewed.<br>Minimum: **0**<br>Maximum: **64** |
| domain_count | Integer | Number of domain names that can be associated with the certificate.<br>Minimum: **1**<br>Maximum: **100** |
| wildcard_count | Integer | Number of wildcard domain names that can be associated with the certificate.<br>Minimum: **0**<br>Maximum: **100** |
| description | String | Certificate description.<br>Minimum: **0**<br>Maximum: **255** |

**Status code: 401**

**Table 4-5** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-6** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-7** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Normal response.

```
{
  "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
  } ],
  "total_count" : 1
}
```

**Status code: 401**

Verification 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 respond the request due to an internal server error.

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

## Status Codes

| Status Code | Description |
|---|---|
| 200 | Normal response. |
| 401 | Verification failed. |
| 403 | Access denied. |
| 404 | Requested page not found. |

| Status Code | Description |
|---|---|
| 500 | Failed to respond the request due to an internal server error. |

## Error Codes

See **Error Codes**.

# 4.1.2 Importing a Certificate

## Function

This API is used to import a certificate to SCM.

## URI

POST /v3/scm/certificates/import

## Request Parameters

**Table 4-8** Request header parameters

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

**Table 4-9** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | Yes | String | SSL certificate name. The value contains 0 to 63 characters.<br>Minimum: **0**<br>Maximum: **255** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate | Yes | String | Certificate content. Use the escape character **\n** or **\r\n** to replace carriage return and line feed characters.<br>Minimum: **0**<br>Maximum: **4096** |
| certificate_chain | Yes | String | Certificate chain. Use the escape character **\n** or **\r\n** to replace carriage return and line feed characters.<br>Minimum: **0**<br>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**.<br>Minimum: **0**<br>Maximum: **4096** |

## Response Parameters

**Status code: 200**

**Table 4-10** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| certificate_id | String | Certificate ID<br>Minimum: **16**<br>Maximum: **16** |

**Status code: 401**

**Table 4-11** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-12** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-13** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Normal response.

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

**Status code: 401**

Verification 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 respond the request due to an internal server error.

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

## Status Codes

| Status Code | Description |
|---|---|
| 200 | Normal response. |
| 401 | Verification failed. |
| 403 | Access denied. |
| 404 | Requested page not found. |
| 500 | Failed to respond the request due to an internal server error. |

## Error Codes

See **Error Codes**.

# 4.1.3 Obtaining Details of a Certificate

## Function

This API is used to query details about a certificate.

## URI

GET /v3/scm/certificates/{certificate_id}

**Table 4-14** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate_id | Yes | String | Certificate ID<br>Minimum: **16**<br>Maximum: **16** |

## Request Parameters

**Table 4-15** Request header parameters

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

## Response Parameters

**Status code: 200**

**Table 4-16** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| id | String | Certificate ID<br>Minimum: **16**<br>Maximum: **16** |

| Parameter | Type | Description |
|---|---|---|
| status | String | Certificate status. The value can be:<br>● **PAID**: The certificate has been paid and needs to be applied for from the CA.<br>● **ISSUED**: The certificate has been issued.<br>● **CHECKING**: The certificate application is being reviewed.<br>● **CANCELCHECKING**: The certificate application cancellation is being reviewed.<br>● **UNPASSED**: The certificate application fails.<br>● **EXPIRED**: The certificate has expired.<br>● **REVOKING**: The certificate revocation application is being reviewed.<br>● **REVOKED**: The certificate has been revoked.<br>● **UPLOAD**: The certificate is being managed.<br>● **SUPPLEMENTCHECKING**: Additional domain names to be added for a multi-domain certificate are being reviewed.<br>● **CANCELSUPPLEMENTING**: The cancellation on additional domain names to be added is being reviewed.<br>Minimum: **0**<br>Maximum: **32** |
| order_id | String | Order ID<br>Minimum: **36**<br>Maximum: **36** |
| name | String | SSL certificate name<br>Minimum: **0**<br>Maximum: **255** |
| type | String | Certificate type. The value can be: **DV_SSL_CERT DV_SSL_CERT_BASIC EV_SSL_CERT EV_SSL_CERT_PRO OV_SSL_CERT OV_SSL_CERT_PRO**<br>Minimum: **0**<br>Maximum: **32** |
| brand | String | Certificate authority. The value can be: GLOBALSIGN SYMANTEC GEOTRUST CFCA<br>Minimum: **0**<br>Maximum: **32** |

| Parameter | Type | Description |
|---|---|---|
| push_support | String | Whether the certificate can be pushed to other services.<br>Minimum: **0**<br>Maximum: **32** |
| revoke_reason | String | Reason for certificate revocation.<br>Minimum: **0**<br>Maximum: **255** |
| signature_algorithm | String | Signature algorithm.<br>Minimum: **0**<br>Maximum: **64** |
| issue_time | String | Time when the certificate was issued. If no valid value is obtained, this parameter is left blank.<br>Minimum: **0**<br>Maximum: **32** |
| not_before | String | Time when the certificate took effect. If no valid value is obtained, this parameter is left blank.<br>Minimum: **0**<br>Maximum: **32** |
| not_after | String | Time when the certificate expired. If no valid value is obtained, this parameter is left blank.<br>Minimum: **0**<br>Maximum: **32** |
| validity_period | Integer | Certificate validity period, in months.<br>Minimum: **12**<br>Maximum: **12** |
| validation_method | String | Domain name ownership verification method. The value can be: **DNS FILE EMAIL**<br>Minimum: **0**<br>Maximum: **32** |
| domain_type | String | Domain name type. The options are as follows:<br>● **SINGLE_DOMAIN**: Single domain names<br>● **WILDCARD**: Wildcard domain names<br>● **MULTI_DOMAIN**: Multiple domain names<br>Minimum: **0**<br>Maximum: **32** |

| Parameter | Type | Description |
|---|---|---|
| domain | String | Domain name associated with the certificate.<br>Minimum: **0**<br>Maximum: **255** |
| sans | String | Additional domain name associated with the certificate<br>Minimum: **0**<br>Maximum: **4096** |
| domain_count | Integer | Number of domain names can be associated with the certificate.<br>Minimum: **1**<br>Maximum: **100** |
| wildcard_count | Integer | Number of additional domain names can be associated with the certificate.<br>Minimum: **0**<br>Maximum: **99** |
| authentification | Array of **Authentification** objects | Domain ownership verification information. For details, see data structure of the **Authentification** field. |

**Table 4-17** Authentification

| Parameter | Type | Description |
|---|---|---|
| record_name | String | Name of a domain ownership verification value.<br>Minimum: **0**<br>Maximum: **255** |
| record_type | String | Type of the domain name verification value.<br>Minimum: **0**<br>Maximum: **255** |
| record_value | String | Type of the domain name verification value.<br>Minimum: **0**<br>Maximum: **255** |
| domain | String | Domain name mapping to the verification record.<br>Minimum: **0**<br>Maximum: **255** |

**Status code: 401**

**Table 4-18** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-19** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-20** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Normal response.

```
{
  "id" : "scs1590053258704",
  "order_id" : "CS20052117270N7V9",
  "name" : "scm-testing",
  "type" : "DV_SSL_CERT",
  "brand" : "SYMANTEC",
  "push_support" : "OFF",
  "status" : "CHECKING_DOMAIN",
  "validity_period" : 12,
  "validation_method" : "DNS",
  "domain_type" : "SINGLE_DOMAIN",
  "domain" : "hosting-******.hwcloudtest.cn",
  "domain_count" : 1,
  "wildcard_count" : 0,
  "authentification" : [ {
    "record_name" : "_dnsauth.hosting-****.hwcloudtest.cn",
    "record_type" : "TXT",
    "record_value" : "201801040000001ytm4q************cd8p7eg9ktlwfsord",
    "domain" : "hosting-*****.hwcloudtest.cn"
  } ]
}
```

**Status code: 401**

Verification 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 respond the request due to an internal server error.

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

## Status Codes

| Status Code | Description |
|---|---|
| 200 | Normal response. |
| 401 | Verification failed. |
| 403 | Access denied. |

| Status Code | Description |
|---|---|
| 404 | Requested page not found. |
| 500 | Failed to respond the request due to an internal server error. |

## Error Codes

See **Error Codes**.

# 4.1.4 Deleting a Certificate

## Function

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

## URI

DELETE /v3/scm/certificates/{certificate_id}

**Table 4-21** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate_id | Yes | String | Certificate ID<br>Minimum: **16**<br>Maximum: **16** |

## Request Parameters

None

## Response Parameters

**Status code: 401**

**Table 4-22** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-23** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-24** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 401**

Verification 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 respond the request due to an internal server error.

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

## Status Codes

| Status Code | Description |
|---|---|
| 204 | Normal response. |
| 401 | Verification failed. |
| 403 | Access denied. |
| 404 | Requested page not found. |
| 500 | Failed to respond the request due to an internal server error. |

## Error Codes

See **Error Codes**.

# 4.1.5 Exporting a Certificate

## Function

This API is used to export a certificate.

## URI

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

**Table 4-25** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate_id | Yes | String | Certificate ID<br>Minimum: **16**<br>Maximum: **16** |

## Request Parameters

**Table 4-26** Request header parameters

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

## Response Parameters

**Status code: 200**

**Table 4-27** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| certificate | String | Certificate content<br>Minimum: **1**<br>Maximum: **4096** |
| certificate_chain | String | Certificate chain<br>Minimum: **1**<br>Maximum: **8192** |
| private_key | String | Private key of the certificate<br>Minimum: **1**<br>Maximum: **4096** |

**Status code: 401**

**Table 4-28** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-29** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-30** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 200**

Normal response.

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

**Status code: 401**

Verification 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 respond the request due to an internal server error.

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

## Status Codes

| Status Code | Description |
|---|---|
| 200 | Normal response. |
| 401 | Verification failed. |
| 403 | Access denied. |
| 404 | Requested page not found. |
| 500 | Failed to respond the request due to an internal server error. |

## Error Codes

See **Error Codes**.

## 4.1.6 Pushing a Certificate to a Service

### Function

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

### URI

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

**Table 4-31** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate_id | Yes | String | Certificate ID<br>Minimum: **16**<br>Maximum: **16** |

### Request Parameters

**Table 4-32** Request header parameters

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

**Table 4-33** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| target_project | Yes | String | Region where the service you want to push a certificate to is deployed.<br>Minimum: **1**<br>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.<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 401**

**Table 4-34** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-35** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-36** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code returned for a request.<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message of an error code.<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

None

## Example Responses

**Status code: 401**

Verification 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 respond the request due to an internal server error.

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

## Status Codes

| Status Code | Description |
|---|---|
| 204 | Normal response. |
| 401 | Verification failed. |
| 403 | Access denied. |
| 404 | Requested page not found. |

| Status Code | Description |
|---|---|
| 500 | Failed to respond the request due to 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.

## URI

GET /v1/private-certificate-authorities

**Table 4-37** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| limit | No | Integer | The number of returned records. The default value is **10**.<br>Minimum: **0**<br>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.<br>Minimum: **1**<br>Maximum: **64** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| offset | No | Integer | Index position. The query starts from the next data record indexed by this parameter. The default value is **0**.<br>Minimum: **0** |
| status | No | String | The CA certificate status. You can search CA certificates by status.<br>● **PENDING**: The CA certificate is to be activated. A CA certificate in this status cannot issue certificates.<br>● **ACTIVED**: The CA certificate is activated. A CA certificate in this status can issue certificates.<br>● **DISABLED**: The CA certificate is disabled. A CA certificate in this status cannot issue certificates.<br>● **DELETED**: The CA certificate is to be deleted as scheduled. A CA certificate in this status cannot issue certificates.<br>● **EXPIRED**: The CA certificate has expired. A CA certificate in this status cannot issue certificates. |
| type | No | String | CA certificate types:<br>● **ROOT**: a root CA certificate<br>● **SUBORDINATE**: a subordinate CA certificate |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| sort_key | No | String | Sorting attribute. The following attributes are available now:<br>● **create_time**: Time the certificate was created (default)<br>● **common_name**: The certificate name<br>● **ca_type**: The CA certificate type<br>● **not_after**: The certificate expiration time |
| sort_dir | No | String | Sorting direction. The options are as follows:<br>● **DESC**: descending order (default)<br>● **ASC**: ascending order |

## Request Parameters

**Table 4-38** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 200**

**Table 4-39** 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 4-40** CertificateAuthorities

| Parameter | Type | Description |
|---|---|---|
| ca_id | String | ID of the CA certificate<br>Minimum: **36**<br>Maximum: **36** |
| type | String | The CA type can be:<br>- **ROOT**: a root CA<br>- **SUBORDINATE**: a subordinate CA |
| status | String | CA certificate status:<br>- **PENDING**: The CA certificate is to be activated. A CA certificate in this status cannot issue certificates.<br>- **ACTIVED**: The CA certificate is activated. A CA certificate in this status can issue certificates.<br>- **DISABLED**: The CA certificate is disabled. A CA certificate in this status cannot issue certificates.<br>- **DELETED**: The CA certificate is to be deleted as scheduled. A CA certificate in this status cannot issue certificates.<br>- **EXPIRED**: The CA certificate has expired. A CA certificate in this status cannot issue certificates. |
| path_length | Integer | CA path length.<br>**NOTE**<br>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 the subordinate CA. The default value is **0**.<br>Minimum: **0**<br>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**.<br>Minimum: **36**<br>Maximum: **36** |
| issuer_name | String | The name of the parent CA certificate. For a root CA, the value of this parameter is **null**.<br>Minimum: **1**<br>Maximum: **64** |
| key_algorithm | String | Key algorithm |

| Parameter | Type | Description |
|---|---|---|
| signature_algorithm | String | Signature hash algorithm |
| freeze_flag | Integer | Freezing tag:<br>- **0**: The certificate is not frozen.<br>- **Other values**: The certificate is frozen (The type of value is reserved). |
| gen_mode | String | Certificate generation method.<br>- **GENERATE**: The certificate is generated through the PCA system.<br>- **IMPORT**: The certificate is imported externally.<br>- **CSR**: The CSR is imported externally and issued by the internal CA. The private key is not managed in PCA. |
| serial_number | String | Serial number of the certificate<br>Minimum: **1**<br>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. |

**Table 4-41** DistinguishedName

| Parameter | Type | Description |
|---|---|---|
| common_name | String | Common certificate name (CN).<br>Minimum: **1**<br>Maximum: **64** |

| Parameter | Type | Description |
|---|---|---|
| country | String | Country code, which must comply with the regular expression "**[A-Za-z]{2}**".<br>Minimum: **2**<br>Maximum: **2** |
| state | String | State or city name.<br>Minimum: **1**<br>Maximum: **128** |
| locality | String | Country/Region.<br>Minimum: **1**<br>Maximum: **128** |
| organization | String | Organization name.<br>Minimum: **1**<br>Maximum: **64** |
| organizational_unit | String | Organization Unit (OU).<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-42** ListCrlConfiguration

| Parameter | Type | Description |
|---|---|---|
| enabled | Boolean | Whether to enable the gray release for the CRL.<br>● **true**<br>● **false** |
| crl_name | String | Name of the CRL.<br>**NOTE**<br>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.<br>Minimum: **7**<br>Maximum: **30** |

| Parameter | Type | Description |
|---|---|---|
| crl_dis_point | String | The address of the CRL file in the OBS bucket.<br>**NOTE**<br>This parameter is composed of **crl_name**, **obs_bucket_name**, and OBS address. |

**Status code: 400**

**Table 4-43** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-44** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-45** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-46** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-47** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>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.ap-southeast-3.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-0fdcb96dfcbe",
    "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

This API is used to create a CA. If you wish to:

- Create a root CA, configure mandatory parameters based on the parameter description.
- Create a subordinate CA and activate its certificate, configure mandatory parameters based on the parameter description.
- Create a subordinate CA, but not want to activate its certificate, exclude one of the following parameters in the request body: **issuer_id**, **signature_algorithm**, and **validity**.

## URI

POST /v1/private-certificate-authorities

## Request Parameters

**Table 4-48** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

**Table 4-49** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| type | Yes | String | Type of the CA you want to create:<br>● **ROOT**: a root CA<br>● **SUBORDINATE**: a subordinate CA |
| distinguished_name | Yes | **DistinguishedName** object | Certificate name. For details, see data structure for the **DistinguishedName** field. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| key_algorithm | Yes | String | Key algorithm. The options are as follows:<br>● **RSA2048**: RSA algorithm with the key length of 2048 bits<br>● **RSA4096**: RSA algorithm with the key length of 4096 bits<br>● **EC256**: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 256 bits<br>● **EC384**: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 384 bits |
| validity | No | **Validity** object | Validity period of a certificate. The options are as follows:<br>● If you want to create a root CA, this parameter is mandatory.<br>● If you want to create a subordinate CA and activate it, this parameter is mandatory.<br>● 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.<br>**NOTE**<br>For details, see data structure description of the **Validity** field. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| issuer_id | No | String | ID of the parent CA. The options are as follows:<br>● If you want to create a root CA, this parameter is not required because a root CA is a self-signed certificate and does not have a parent CA.<br>● If you want to create a subordinate CA and activate it, this parameter is mandatory.<br>● 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.<br>Minimum: **36**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| path_length | No | Integer | Length of the CA certificate path. The options are as follows:<br>● 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. To limit the CA hierarchies, you can specify this parameter when creating a subordinate CA.<br>● If you want to create a subordinate CA and activate it, specify this parameter based on your need. Default value: **0**<br>● If you want to create a subordinate CA but not need to activate it, this parameter is not required. You can specify this parameter when you activate the subordinate CA.<br>Minimum: **0**<br>Maximum: **6** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| signature_algorithm | No | String | Signature hash algorithm.<br>● There are three scenarios:<br>– If you want to create a root CA, this parameter is mandatory.<br>– If you want to create a subordinate CA and activate it, this parameter is mandatory.<br>– 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.<br>● The options are as follows:<br>– **SHA256**<br>– **SHA384**<br>– **SHA512** |

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

**Table 4-50** DistinguishedName

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| common_name | Yes | String | Common certificate name (CN).<br>Minimum: **1**<br>Maximum: **64** |
| country | Yes | String | Country code, which must comply with the regular expression "**[A-Za-z]{2}**".<br>Minimum: **2**<br>Maximum: **2** |
| state | Yes | String | State or city name.<br>Minimum: **1**<br>Maximum: **128** |
| locality | Yes | String | Country/Region.<br>Minimum: **1**<br>Maximum: **128** |
| organization | Yes | String | Organization name.<br>Minimum: **1**<br>Maximum: **64** |
| organizational_unit | Yes | String | Organization Unit (OU).<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-51** Validity

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| type | Yes | String | Validity period type, which is mandatory. The options are as follows:<br>● **YEAR**: Year (12 months)<br>● **MONTH**: Month (31 days)<br>● **DAY**: Day<br>● **HOUR**: Hour |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| value | Yes | Integer | The certificate validity period. The value of this parameter varies depending on the value of **type**:<br>● Root CA certificates: no longer than 30 years<br>● Subordinate CA or private certificates: no longer than 20 years |
| start_from | No | Integer | Start time. The options are as follows:<br>● The value is a timestamp in milliseconds. For example, 1645146939688 indicates 2022-02-18 09:15:39.<br>● The value of **start_from** cannot be earlier than the result of the value of **current_time** minus 5 minutes. |

**Table 4-52** CrlConfiguration

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| enabled | Yes | Boolean | Whether to enable the gray release function of CRL.<br>● **true**<br>● **false** |
| crl_name | No | String | Name of the certificate revocation list.<br>**NOTE**<br>If you do not specify this parameter, the system uses the ID of the parent CA that issues the current certificate by default. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| obs_bucket_name | No | String | OBS bucket name.<br>**NOTE**<br>To enable the CRL release function:<br>● This parameter is mandatory. You must have created an agency to authorize the PCA service to access OBS. For details, see **Certificate Revocation** > **Checking the Agency Permission** and **Certificate Revocation** > **Creating an Agency** in this document.<br>● 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.<br>Minimum: **7**<br>Maximum: **30** |

## Response Parameters

**Status code: 200**

**Table 4-53** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| ca_id | String | ID of the CA certificate being issued.<br>Minimum: **36**<br>Maximum: **36** |

**Status code: 400**

**Table 4-54** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-55** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-56** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-57** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-58** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>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.ap-southeast-3.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",
    "organization_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. |

| Status Code | Description |
|---|---|
| 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.

## URI

GET /v1/private-certificate-authorities/quotas

## Request Parameters

**Table 4-59** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 200**

**Table 4-60** Response body parameters

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

**Table 4-61** Quotas

| Parameter | Type | Description |
|---|---|---|
| resources | Array of **Resources** objects | Resource quota list. For details, see data structure for the **Resources** field. |

**Table 4-62** Resources

| Parameter | Type | Description |
|---|---|---|
| type | String | Certificate type<br>- **CERTIFICATE_AUTHORITY**: CA certificate.<br>- **CERTIFICATE**: private certificate. |
| used | Integer | Used quota |
| quota | Integer | Total quota<br>- **CERTIFICATE_AUTHORITY**: 100<br>- **CERTIFICATE**: 100,000 |

**Status code: 400**

**Table 4-63** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-64** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-65** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-66** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-67** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to query the CA certificate quota, 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.ap-southeast-3.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.

## URI

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

**Table 4-68** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ca_id | Yes | String | ID of the CA certificate<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-69** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 200**

**Table 4-70** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| ca_id | String | ID of the CA certificate<br>Minimum: **36**<br>Maximum: **36** |
| type | String | The CA type can be:<br>● **ROOT**: a root CA<br>● **SUBORDINATE**: a subordinate CA |
| status | String | CA certificate status:<br>● **PENDING**: The CA certificate is to be activated. A CA certificate in this status cannot issue certificates.<br>● **ACTIVED**: The CA certificate is activated. A CA certificate in this status can issue certificates.<br>● **DISABLED**: The CA certificate is disabled. A CA certificate in this status cannot issue certificates.<br>● **DELETED**: The CA certificate is to be deleted as scheduled. A CA certificate in this status cannot issue certificates.<br>● **EXPIRED**: The CA certificate has expired. A CA certificate in this status cannot issue certificates. |
| path_length | Integer | CA path length.<br>**NOTE**<br>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 the subordinate CA. The default value is **0**.<br>Minimum: **0**<br>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**.<br>Minimum: **36**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| issuer_name | String | The name of the parent CA certificate. For a root CA, the value of this parameter is **null**.<br>Minimum: **1**<br>Maximum: **64** |
| key_algorithm | String | Key algorithm |
| signature_algorithm | String | Signature hash algorithm |
| freeze_flag | Integer | Freezing tag:<br>● **0**: The certificate is not frozen.<br>● **Other values**: The certificate is frozen (The type of value is reserved). |
| gen_mode | String | Certificate generation method.<br>● **GENERATE**: The certificate is generated through the PCA system.<br>● **IMPORT**: The certificate is imported externally.<br>● **CSR**: The CSR is imported externally and issued by the internal CA. The private key is not managed in PCA. |
| serial_number | String | Serial number of the certificate<br>Minimum: **1**<br>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. |

**Table 4-71** DistinguishedName

| Parameter | Type | Description |
|---|---|---|
| common_name | String | Common certificate name (CN).<br>Minimum: **1**<br>Maximum: **64** |
| country | String | Country code, which must comply with the regular expression "**[A-Za-z]{2}**".<br>Minimum: **2**<br>Maximum: **2** |
| state | String | State or city name.<br>Minimum: **1**<br>Maximum: **128** |
| locality | String | Country/Region.<br>Minimum: **1**<br>Maximum: **128** |
| organization | String | Organization name.<br>Minimum: **1**<br>Maximum: **64** |
| organizational_unit | String | Organization Unit (OU).<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-72** ListCrlConfiguration

| Parameter | Type | Description |
|---|---|---|
| enabled | Boolean | Whether to enable the gray release for the CRL.<br>● **true**<br>● **false** |
| crl_name | String | Name of the CRL.<br>**NOTE**<br>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.<br>Minimum: **7**<br>Maximum: **30** |
| crl_dis_point | String | The address of the CRL file in the OBS bucket.<br>**NOTE**<br>This parameter is composed of **crl_name**, **obs_bucket_name**, and OBS address. |

**Status code: 400**

**Table 4-73** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-74** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-75** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-76** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-77** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to query details about a CA, 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.ap-southeast-3.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
  }
}
```

**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 a CA certificate is in the **Pending activation** status, the CA certificate will be deleted immediately, scheduled deletion is not supported.

## URI

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

**Table 4-78** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ca_id | Yes | String | ID of the CA certificate you plan to delete.<br>Minimum: **36**<br>Maximum: **36** |

**Table 4-79** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| pending_days | Yes | String | Delayed deletion time, in days<br>Minimum: **7**<br>Maximum: **30** |

## Request Parameters

**Table 4-80** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 400**

**Table 4-81** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-82** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-83** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-84** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-85** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

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

```
DELETE https://ccm.ap-southeast-3.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. |
| 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.

## URI

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

**Table 4-86** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ca_id | Yes | String | ID of the subordinate CA you want to activate.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-87** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

**Table 4-88** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| issuer_id | Yes | String | ID of the parent CA.<br>Minimum: **1**<br>Maximum: **64** |
| path_length | Yes | Integer | Path length.<br>Minimum: **0**<br>Maximum: **6** |
| signature_algorithm | Yes | String | Signature hash algorithm. The options are as follows:<br>● **SHA256**<br>● **SHA384**<br>● **SHA512** |
| validity | Yes | **Validity** object | Certificate validity. For details, see data structure for the **Validity** field. |

**Table 4-89** Validity

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| type | Yes | String | Validity period type, which is mandatory. The options are as follows:<br>● **YEAR**: Year (12 months)<br>● **MONTH**: Month (31 days)<br>● **DAY**: Day<br>● **HOUR**: Hour |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| value | Yes | Integer | The certificate validity period. The value of this parameter varies depending on the value of **type**:<br>● Root CA certificates: no longer than 30 years<br>● Subordinate CA or private certificates: no longer than 20 years |
| start_from | No | Integer | Start time. The options are as follows:<br>● The value is a timestamp in milliseconds. For example, 1645146939688 indicates 2022-02-18 09:15:39.<br>● The value of **start_from** cannot be earlier than the result of the value of **current_time** minus 5 minutes. |

## Response Parameters

**Status code: 400**

**Table 4-90** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-91** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-92** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-93** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-94** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to activate 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.ap-southeast-3.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. |
| 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.

## URI

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

**Table 4-95** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ca_id | Yes | String | ID of the subordinate CA that has not been activated.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-96** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 200**

**Table 4-97** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| csr | String | Content of the CSR. The content varies depending on how you obtain the CSR:<br>● If you use an API to obtain the CSR, the newline characters in it have been replaced with **\r\n**.<br>● If you export the CSR from the console, the CSR is in PEM format.<br>Minimum: **1**<br>Maximum: **4096** |

**Status code: 400**

**Table 4-98** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-99** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-100** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-101** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-102** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to export a CSR of 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.

```
GET https://ccm.ap-southeast-3.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-
b929-b7acb04143f7/csr
```

## Example Responses

**Status code: 200**

Request succeeded.

```
{
  "csr" : "-----BEGIN CERTIFICATE REQUEST-----\r
\nMIIBUDCB2AIBADBZMRAwDgYDVQQDDAdDU1IsMTIzMQswCQYDVQQGEwJjbjERMA8G\r
\nA1UECAwIc2hhbmdoYWkxETAPBgNVBAcMCHNoYW5naGFpMRIwEAYDVQQKDAlzaGFu\r
\nZyxoYWkwdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAQl9M7bK+vys5x9mnfG3783aPRh\r\nP/
xqLPKVsRsqniC3vPZvIz9E7SasMfZLrXVK37QWhtAEtgNG7NrQnwiOye0/8VZL\r
\nVX7ildM6CZY4SlJYSa6TBUsXyGjOs514fjxbuT6gADAKBggqhkjOPQQDAgNnADBk\r\nAjBlQiPXU7TDDDwxrh
+JfZEYgmr61cIQdE5GMozPDYime30zcuMnVrb9i3o/2BW+\r
\n0lECMG0QWbAYh0LoqnmAYqlgTKK8nKsxm0xFuTRyfxynWi8BpCvAGx803Qpa8EJV\r\nJTTjcw==\r\n-----
END 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.

## URI

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

**Table 4-103** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ca_id | Yes | String | ID of the CA certificate you want to disable.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-104** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 400**

**Table 4-105** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-106** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-107** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-108** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-109** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to disable 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.ap-southeast-3.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. |
| 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.

## URI

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

**Table 4-110** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ca_id | Yes | String | ID of the CA you want to enable.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-111** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 400**

**Table 4-112** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-113** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-114** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-115** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-116** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to enable a CA, 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.ap-southeast-3.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. |

| Status Code | Description |
|---|---|
| 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.

## URI

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

**Table 4-117** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ca_id | Yes | String | ID of the CA certificate you want to export.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-118** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 200**

**Table 4-119** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| certificate | String | Certificate content.<br>**NOTE**<br>● If you use an API to obtain the certificate, the newline characters in it have been replaced with **\r\n**.<br>● If you export the certificate from the console, the certificate is in PEM format.<br>Minimum: **1**<br>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.<br>**NOTE**<br>● If you use an API to obtain the certificate chain, the newline characters in it have been replaced with **\r\n**.<br>● If you export the certificate chain from the console, the certificate chain is in PEM format.<br>Minimum: **1**<br>Maximum: **2097152** |

**Status code: 400**

**Table 4-120** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-121** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-122** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-123** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-124** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to export 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.ap-southeast-3.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-
a30c-4029-b929-b7acb04143f7/export
```

## Example Responses

**Status code: 200**

Request succeeded.

```
{
  "certificate" : "-----BEGIN CERTIFICATE-----\r
\nMIIDczCCAlugAwIBAgIKKsxppf9kUcq6dDANBgkqhkiG9w0BAQsFADBOMQowCAYD\r
\nVQQDDAE3MQswCQYDVQQGEwJDTjEQMA4GA1UECAwHU2ljaHVhbjEQMA4GA1UEBwwH\r
\nQ2hlbmdkdTEPMA0GA1UECgwGSHVhd2VpMB4XDTIxMTAxNDA4NDMxMVoXDTIyMTAx\r
\nNDA4NDQxMVowPjELMAkGA1UEAwwCWVUxCzAJBgNVBAYTAmNuMQowCAYDVQQIDAEz\r
\nMQowCAYDVQQHDAE0MQowCAYDVQQKDAE1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A\r
\nMIIBCgKCAQEA1NZyv9qhA711c/99lNO80/uSXjoL1kEjljBtJVB7vqkDf0Ejs20A\r\nfQoHEVTuHams9XLvrllu
+YTws4QO8hjbnLI9mmerRRJK0pp+tBmCS3ZFoC23c5vz\r\ny+l0t+Yc2JYhvaOFr823Yo0WC2+NB065nIKH6/
duoONfD+3c5Ynkib0nBNyDV+DB\r\nhdKM0nrlqI07cNpYDWpfX5IiDL+4Oh+kY1xGLZCObgsXl34zTf6E7bxJ1/
iDZjwJ\r\ndpf6OUQONmIcT49993YCrMDisjJ2OwW9e41S7D2xy/1xmPwWwnid1WHOkTfK4cyl\r
\n2PHaHh3FTXIGYjVSg3yKfujauVOFpZ9bTwIDAQABo2MwYTAfBgNVHSMEGDAWgBTu\r
\nY36JXjwX7XiLcwKtUto8RZa52DAdBgNVHQ4EFgQUyuAS2HonxOWDIPOgPIMFQ9rr\r
\nGiMwEgYDVR0TAQH/BAgwBgEB/wIBADALBgNVHQ8EBAMCAYYwDQYJKoZIhvcNAQEL\r
\nBQADggEBALea9Hf5iGCfKLpjf30KCBelEgj3ZxLSBOgsn8UkulB62FyUgnne4AmY\r
\nuWHY0xjbamIs8Dgt1GtQrfh3kKq2rfjdasFvrQnAQkjn61O16nbCbWS2H+sqy7Ae\r
\nTJZWefx1eIAv8XH7g491C5Rb5TGykk/bFm7RvGhr35ri+nIcqiDmjO44zHr1aPvm\r
\ns4vA06UQFvlWFY2wiynZ6f+PuvsPraL7kjQVJqsel8TYpZjMWl/hc3VkXEX6gqPm\r
\nbzTypaxa63FCETXtXNlsdid/QWX7l/pUtQ2U57mHi+xJNkA8/Spf1y4zH1rANkmw\r
\ntBjeKGRphA4LKir3wsbdXRYbBe7POZo=\r\n-----END CERTIFICATE-----",
  "certificate_chain" : "-----BEGIN CERTIFICATE-----\r
\nMIIDczCCAlugAwIBAgIKKsxpOVE4imyq4zANBgkqhkiG9w0BAQsFADBOMQowCAYD\r
\nVQQDDAE3MQswCQYDVQQGEwJDTjEQMA4GA1UECAwHU2ljaHVhbjEQMA4GA1UEBwwH\r
\nQ2hlbmdkdTEPMA0GA1UECgwGSHVhd2VpMB4XDTIxMTAxMTAyNTIzMVoXDTIyMTAx\r
\nMTAyNTMzMVowTjEKMAgGA1UEAwwBNzELMAkGA1UEBhMCQ04xEDAOBgNVBAgMB1Np\r
\nY2h1YW4xEDAOBgNVBAcMB0NoZW5nZHUxDzANBgNVBAoMBkh1YXdlaTCCASIwDQYJ\r
\nKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMH7+ovgT/xbBfbLAG0yBs9QERnfgdLL\r
\n5BFlgjJNP0Ashw2k5EaWq1qDfY6o4AqGfJHjPd2kLy5ZW7Cq6vuqTD3Uj3tX98N2\r\n6T2Na/
s1JGmlExX7Udsikv6hsoKmAjrGdDBEs2Jl/2FRnxO8uFnOuSLqvPUvlR7c\r
\ndIoDq4WqVyI4sXAoUq7xB8GoTsGLANn8eYHVNsZcSZ9E0qEiWx3WqhPh9Ncto949\r\nVuDVqkQ9QjjFo/
yEO6+KhxqyVDWQwdI3UsyzjqGtFzKQksLUQ0AUec4IsK/VWypG\r\nu34jEkaWGv72CmFGoJEK/K/
WoXyzKyCmnS3Wcz4ETliRG5fb7aqP56sCAwEAAaNT\r\nMFEwHwYDVR0jBBgwFoAU7mN+iV48F
+14i3MCrVLaPEWWudgwHQYDVR0OBBYEFO5j\r\nfolePBfteItzAq1S2jxFlrnYMA8GA1UdEwEB/
wQFMAMBAf8wDQYJKoZIhvcNAQEL\r
\nBQADggEBACHJruSBkb8gA0VajkTZWN7QOvUoJPA2TdOmIlnkzxyR5sXkOmsllHLp\r\njzze9LBKbkMl4/
ZfWvLUde7wKJJzV208E1c3mf0iZFqRJ0Ms+o/DStVw/ap+98ML\r\n4oevJk2y/bn7IQTL2bvnEi/
+iSzmz1CIlnRUyfEWBW2aVFgjrm/ZaFTiEb5jIdzm\r\ns75YNCvIvn3eKp+yOQ8fyG7mKvvn3nlRKfMTv+
+bLLUh9or/e/phWkUj0gtSyDEn\r
\nyOnVuhxyveLwoag27U8THe5E4Ygrrg98v2eGNFyGMmtsXXKNgFSf5FBqvyED9d61\r\nZ86vYp/
N2dbauF7uUUaX5RbtFANYFU0=\r\n-----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. |

| Status Code | Description |
|---|---|
| 404 | No resources available or found. |
| 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:

- The certificate of the subordinate CA is in the **Pending activation** status.
- The certificate body you want to import must meet the following requirements:
  - When the certificate is issued, its certificate signature request must be exported from the PCA system.
  - Although the certificate chain is optional, importing the complete certificate chain is recommended so that you can export a complete certificate chain later.
  - The certificate body and certificate chain must be in PEM format.

## URI

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

**Table 4-125** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ca_id | Yes | String | ID of the CA certificate you want to import.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-126** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

**Table 4-127** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate | Yes | String | Certificate content<br>Minimum: **1**<br>Maximum: **32768** |
| certificate_chain | No | String | Certificate chain content<br>Minimum: **0**<br>Maximum: **2097152** |

## Response Parameters

**Status code: 400**

**Table 4-128** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-129** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-130** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-131** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-132** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to import 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.ap-southeast-3.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/import

{
  "certificate" : "-----BEGIN CERTIFICATE---******----END CERTIFICATE-----",
  "certificate_chain" : "-----BEGIN CERTIFICATE-----**********-----END 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. After a CA is restored, its status changes from **Pending deletion** to **Disabled**.

NOTE

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

## URI

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

**Table 4-133** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ca_id | Yes | String | ID of the CA certificate you want to restore.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-134** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 400**

**Table 4-135** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-136** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-137** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-138** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-139** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to restore a CA, 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.ap-southeast-3.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. |
| 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

Reason for revocation.

NOTE

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

## URI

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

**Table 4-140** Path Parameters

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

## Request Parameters

**Table 4-141** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

**Table 4-142** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| reason | No | String | Reason for revocation.The options are as follows:<br>• **UNSPECIFIED** : Default value. No reason is specified for revocation.<br>• **KEY_COMPROMISE** : The certificate key material has been leaked.<br>• **CERTIFICATE_AUTHORITY_COMPROMISE** : Key materials of the CA have been leaked in the certificate chain.<br>• **AFFILIATION_CHANGED** : The subject or other information in the certificate has been changed.<br>• **SUPERSEDED** : The certificate has been replaced.<br>• **CESSATION_OF_OPERATION** : The entity in the certificate or certificate chain has ceased to operate.<br>• **CERTIFICATE_HOLD** : The certificate should not be considered valid currently and may take effect in the future.<br>• **PRIVILEGE_WITHDRAWN** : This certificate no longer has permissions on the properties it claims.<br>• **ATTRIBUTE_AUTHORITY_COMPROMISE** : The authority which determines appropriate attributes for a Certificate may have been compromised.<br>**NOTE**<br>If you do not want to provide the revocation reason, set the request body to **{}**. Otherwise, an error will be reported. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| | | | Enumeration values:<br>● **UNSPECIFIED**<br>● **KEY_COMPROMISE**<br>● **CERTIFICATE_AUTHORITY_COMPROMISE**<br>● **AFFILIATION_CHANGED**<br>● **SUPERSEDED**<br>● **CESSATION_OF_OPERATION**<br>● **CERTIFICATE_HOLD**<br>● **PRIVILEGE_WITHDRAWN**<br>● **ATTRIBUTE_AUTHORITY_COMPROMISE** |

## Response Parameters

**Status code: 400**

**Table 4-143** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-144** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-145** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-146** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-147** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to revoke a subordinate CA, 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.ap-southeast-3.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.

## URI

GET /v1/private-certificates

**Table 4-148** Query Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| limit | No | Integer | The number of returned records. The default value is **10**.<br>Minimum: **0**<br>Maximum: **1000** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| name | No | String | The name of the private certificate. The set of certificates whose names contain the name field is returned.<br>Minimum: **1**<br>Maximum: **64** |
| offset | No | Integer | Index position. The query starts from the next data record indexed by this parameter.<br>Minimum: **0** |
| status | No | String | The private certificate status. You can query private certificates by status.<br>● **ISSUED**: The certificate is issued.<br>● **REVOKED**: The certificate is revoked.<br>● **EXPIRED**: The certificate expired. |
| sort_key | No | String | Sorting attribute. The following attributes are available now:<br>● **create_time**: Time the certificate was created (default)<br>● **common_name**: The certificate name<br>● **issuer_name**: The name of the CA who issued the certificate.<br>● **not_after**: The certificate expiration time |
| sort_dir | No | String | Sorting direction. The options are as follows:<br>● **DESC**: descending order (default)<br>● **ASC**: ascending order |

## Request Parameters

**Table 4-149** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 200**

**Table 4-150** Response body parameters

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

**Table 4-151** Certificates

| Parameter | Type | Description |
|---|---|---|
| certificate_id | String | ID of the private certificate<br>Minimum: **36**<br>Maximum: **36** |
| status | String | Certificate status:<br>● **ISSUED**: The certificate is issued.<br>● **EXPIRED**: The certificate expired.<br>● **REVOKED**: The certificate is revoked. |
| issuer_id | String | ID of the parent CA.<br>Minimum: **36**<br>Maximum: **36** |
| issuer_name | String | The name of the parent CA certificate.<br>Minimum: **1**<br>Maximum: **64** |
| key_algorithm | String | Key algorithm |

| Parameter | Type | Description |
|---|---|---|
| signature_algorithm | String | Signature algorithm |
| freeze_flag | Integer | Freezing tag:<br>- **0**: The certificate is not frozen.<br>- **Other values**: The certificate is frozen (The type of value is reserved). |
| gen_mode | String | Certificate generation method.<br>- **GENERATE**: The certificate is generated through the PCA system.<br>- **IMPORT**: The certificate is imported externally.<br>- **CSR**: The CSR is imported externally and issued by the internal CA. The private key is not managed in PCA. |
| serial_number | String | Serial number.<br>Minimum: **1**<br>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. |

**Table 4-152** DistinguishedName

| Parameter | Type | Description |
|---|---|---|
| common_name | String | Common certificate name (CN).<br>Minimum: **1**<br>Maximum: **64** |

| Parameter | Type | Description |
|---|---|---|
| country | String | Country code, which must comply with the regular expression "**[A-Za-z]{2}**".<br>Minimum: **2**<br>Maximum: **2** |
| state | String | State or city name.<br>Minimum: **1**<br>Maximum: **128** |
| locality | String | Country/Region.<br>Minimum: **1**<br>Maximum: **128** |
| organization | String | Organization name.<br>Minimum: **1**<br>Maximum: **64** |
| organizational_unit | String | Organization Unit (OU).<br>Minimum: **1**<br>Maximum: **64** |

**Status code: 400**

**Table 4-153** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-154** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-155** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-156** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-157** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to query the private 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.ap-southeast-3.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"
  }, {
    "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"
  } ]
}
```

**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. |

| 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**.

# 4.2.2.2 Applying for a Certificate

## Function

This API is used to apply for a certificate.

## URI

POST /v1/private-certificates

## Request Parameters

**Table 4-158** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

**Table 4-159** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| issuer_id | Yes | String | ID of the parent CA.<br>Minimum: **36**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| key_algorithm | Yes | String | Key algorithm. The options are as follows:<br>- **RSA2048**: RSA algorithm with the key length of 2048 bits<br>- **RSA4096**: RSA algorithm with the key length of 4096 bits<br>- **EC256**: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 256 bits<br>- **EC384**: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 384 bits |
| signature_algorithm | Yes | String | Signature hash algorithm. The options are as follows:<br>- **SHA256**<br>- **SHA384**<br>- **SHA512** |
| 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.<br>- **digitalSignature**: The key is used as a digital signature.<br>- **nonRepudiation**: The key can be used for non-repudiation.<br>- **keyEncipherment**: The key can be used for key encryption.<br>- **dataEncipherment**: The key can be used for data encryption.<br>- **keyAgreement**: The key can be used for key negotiation.<br>- **keyCertSign**: The key can issue a certificate.<br>- **cRLSign**: The key can issue a certificate revocation list (CRL).<br>- **encipherOnly**: The key is used only for encryption.<br>- **decipherOnly**: The key is used only for decryption. |
| subject_alternative_names | No | Array of **SubjectAlternativeName** objects | Alternative name for the subject. For details, see data structure for the **SubjectAlternativeName** field.<br>- Array size: [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. |

**Table 4-160** CertDistinguishedName

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| common_name | Yes | String | Common certificate name (CN).<br>Minimum: **1**<br>Maximum: **64** |
| country | No | String | Country code, which must comply with the regular expression "**[A-Za-z]{2}**".If not passed in, the value corresponding to the parent CA is inherited by default.<br>Minimum: **2**<br>Maximum: **2** |
| state | No | String | State or city name.If not passed in, the value corresponding to the parent CA is inherited by default.<br>Minimum: **1**<br>Maximum: **128** |
| locality | No | String | Country/Region.If not passed in, the value corresponding to the parent CA is inherited by default.<br>Minimum: **1**<br>Maximum: **128** |
| organization | No | String | Organization name.If not passed in, the value corresponding to the parent CA is inherited by default.<br>Minimum: **1**<br>Maximum: **64** |
| organizational_unit | No | String | Organization Unit (OU).If not passed in, the value corresponding to the parent CA is inherited by default.<br>Minimum: **1**<br>Maximum: **64** |

**Table 4-161** Validity

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| type | Yes | String | Validity period type, which is mandatory. The options are as follows:<br>- **YEAR**: Year (12 months)<br>- **MONTH**: Month (31 days)<br>- **DAY**: Day<br>- **HOUR**: Hour |
| value | Yes | Integer | The certificate validity period. The value of this parameter varies depending on the value of **type**:<br>- Root CA certificates: no longer than 30 years<br>- Subordinate CA or private certificates: no longer than 20 years |
| start_from | No | Integer | Start time. The options are as follows:<br>- The value is a timestamp in milliseconds. For example, 1645146939688 indicates 2022-02-18 09:15:39.<br>- The value of **start_from** cannot be earlier than the result of the value of **current_time** minus 5 minutes. |

**Table 4-162** SubjectAlternativeName

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| type | Yes | String | Type of the alternative name. Currently, only **DNS**, **IP**, **DNS**, and **URI** are allowed.<br>- **DNS**<br>- **IP**<br>- **EMAIL**<br>- **URI** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| value | Yes | String | Value of the corresponding alternative name type.<br>- DNS type. Length range: 0 to 253 characters<br>- IP address type. Length range: 0 to 39 characters<br>- EMAIL type. Length range: 0 to 256 characters<br>- URI address type. Length range: 0 to 253 characters |

**Table 4-163** ExtendedKeyUsage

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| server_auth | No | Boolean | Server authentication. The OID is 1.3.6.1.5.5.7.3.1.<br>- **true**<br>- **false**<br>**NOTE**<br>Enable this enhanced key usage for the server certificate. The default value is false.<br>Default: **false** |
| client_auth | No | Boolean | Client authentication. The OID is 1.3.6.1.5.5.7.3.2<br>- **true**<br>- **false**<br>**NOTE**<br>Enable this enhanced key usage for the client certificate. The default value is false.<br>Default: **false** |
| code_signing | No | Boolean | Signing of downloadable executable code client authentication. The OID is 1.3.6.1.5.5.7.3.3.<br>- **true**<br>- **false**<br>**NOTE**<br>The default value is false.<br>Default: **false** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| email_protection | No | Boolean | Email protection. The OID is 1.3.6.1.5.5.7.3.4.<br>● **true**<br>● **false**<br>**NOTE** The default value is false.<br>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<br>● **true**<br>● **false**<br>**NOTE** The default value is false.<br>Default: **false** |

**Table 4-164** CustomizedExtension

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| object_identifier | No | String | Object identifier<br>**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.<br>Minimum: **1**<br>Maximum: **64** |
| value | No | String | Custom attribute content<br>Minimum: **1**<br>Maximum: **64** |

## Response Parameters

**Status code: 200**

**Table 4-165** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| certificate_id | String | ID of the certificate being issued.<br>Minimum: **36**<br>Maximum: **36** |

**Status code: 400**

**Table 4-166** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-167** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-168** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-169** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-170** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to apply for a 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.ap-southeast-3.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 via CSR

## Function

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

- The default parameters are as follows:
  - Default CA parameters:
    - **keyUsage**: The options are **digitalSignature**, **keyCertSign**, and **cRLSign**. The parameters in the CSR are preferentially used.
    - **SignatureHashAlgorithm**: **SHA384**
    - **PathLength**: **0** (user-defined)
  - Private certificates
    - **keyUsage**: The options are **digitalSignature** and **keyAgreement**. The parameters in the CSR are preferentially used.
    - **SignatureHashAlgorithm**: **SHA384**
- If **type** is set to **INTERMEDIATE_CA**, the created subordinate CA certificate has the following features:

  - It does not use the CA quota. When you query the CA list, this certificate is not included.
  - Only the following two APIs can be used to obtain its information:
    - To obtain its details: GET /v1/private-certificate-authorities/{ca_id}
    - To export it: POST /v1/private-certificate-authorities/{ca_id}/export
  - The value of **certificate_id** returned by this API is the value of **ca_id** for the subordinate CA.
  - It cannot issue certificates as its key is on the user side.
- If **type** is set to **ENTITY_CERT**, the created private certificate has the following features:
  - It uses the private certificate quota. When you query the private certificate list, this certificate is included.
  - The usage of this certificate is the same as that of other private certificates except that the exported certificate does not contain the key information (the key is on the client).

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.

## URI

POST /v1/private-certificates/csr

## Request Parameters

**Table 4-171** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

**Table 4-172** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| issuer_id | Yes | String | ID of the parent CA.<br>Minimum: **36**<br>Maximum: **36** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| csr | Yes | String | Certificate signature request. Use **\r\n** or **\n** to replace the newline characters in the CSR. The replacement is not required if this API is requested through the console.<br>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.<br>● **ENTITY_CERT**: A private certificate is issued. It is the default value.<br>● **INTERMEDIATE_CA**: A subordinate CA certificate is issued. |
| path_length | No | Integer | Path length. This parameter is valid only when a subordinate CA is issued.<br>Minimum: **0**<br>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. |

**Table 4-173** Validity

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| type | Yes | String | Validity period type, which is mandatory. The options are as follows:<br>● **YEAR**: Year (12 months)<br>● **MONTH**: Month (31 days)<br>● **DAY**: Day<br>● **HOUR**: Hour |
| value | Yes | Integer | The certificate validity period. The value of this parameter varies depending on the value of **type**:<br>● Root CA certificates: no longer than 30 years<br>● Subordinate CA or private certificates: no longer than 20 years |
| start_from | No | Integer | Start time. The options are as follows:<br>● The value is a timestamp in milliseconds. For example, 1645146939688 indicates 2022-02-18 09:15:39.<br>● The value of **start_from** cannot be earlier than the result of the value of **current_time** minus 5 minutes. |

**Table 4-174** SubjectAlternativeName

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| type | Yes | String | Type of the alternative name. Currently, only **DNS**, **IP**, **DNS**, and **URI** are allowed.<br>● **DNS**<br>● **IP**<br>● **EMAIL**<br>● **URI** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| value | Yes | String | Value of the corresponding alternative name type.<br>● DNS type. Length range: 0 to 253 characters<br>● IP address type. Length range: 0 to 39 characters<br>● EMAIL type. Length range: 0 to 256 characters<br>● URI address type. Length range: 0 to 253 characters |

## Response Parameters

**Status code: 200**

**Table 4-175** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| certificate_id | String | ID of the certificate being issued.<br>Minimum: **36**<br>Maximum: **36** |

**Status code: 400**

**Table 4-176** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-177** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-178** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-179** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-180** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>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.ap-southeast-3.myhuaweicloud.com/v1/private-certificates/csr

{
  "csr" : "-----BEGIN CERTIFICATE REQUEST-----\
\nMIICyTCCAbECAQAwXjELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB3NpY2hhdW4xEDAO\
\nBgNVBAcTB2NoZW5nZHUxCzAJBgNVBAoTAkhXMQswCQYDVQQLEwJJVDERMA8GA1UE\
\nAxMIdGVzdC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCZ4q5z\\nxqK/L/
FC9x2jESeUW5GB6zS5rVxT0WLTCTv9d1LtWBLsRIinATYTYiP1pNo4/pBq\
\nHlM3IiUDkc896CJerYlNzOIjTaV4GjCZvPrxSHU5toJvIDflBsY+gnzbT1ol/y0r\\n3yb9dx7eeF5rPR+U8RTw+Ov/
ZNRb+0CY30hrXMdrWjp5dtLGTlr5EFYxlKNOPCkR\\n
+6BGyJnC9PWSuqwsykFbgMRkcBaNAxa59dRhMF50pvx2Vs929vFrMi+ofDELUOqz\
\n1vyjaEA3pn3AGJGXZgrGNbSfz12ixgGLes4cQD21GCIAWgnBQ7b1ru2V8ImUfyh0\\nyvTEyHJTuFbQ
+257AgMBAAGgJjAkBgkqhkiG9w0BCQ4xFzAVMBMGA1UdEQQMMAqC\
\nCHRlc3QuY29tMA0GCSqGSIb3DQEBCwUAA4IBAQBKfjZuYsz4s0wb1POIWn41eiAB\
\np53qb63QKWILN9z8dLktcdSl3lPfcfPZpXv++QPtn3LR9rJKBawusk6SPXbvOGgS\\n5J
+6eM8kVW2O3gHFgoaMcPYVtiO7ekG6o25qx6+Rj84wbFdmpOiCc8AwrLEBwzYV\
\np1zaprWQu6PxBulkYPa3FLcntDdi7B67r0YTpxVvo1K7vHYFboDvPz7xG57QIFIM\
\nwGd1OegariMT3N8gBOzLZc+jqLpxgo4xoNqBHMo6DEmKLdWdzU4ljpuGK9had99k\\nvQ5vft/
Qra3v1uq2lOm/G92b0uA9Y1t2bMHobtAnuXL0HmY9XcLdzpC3f8h8\\n-----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.

### URI

POST /v1/private-certificates/csr/parse

### Request Parameters

**Table 4-181** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

**Table 4-182** Request body parameters

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

### Response Parameters

**Status code: 200**

**Table 4-183** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| key_algorithm | String | Key algorithm. |
| key_algorithm_length | String | Length of the key algorithm, in bits. |
| signature_algorithm | String | Signature algorithm with a specific signature and hash algorithm, for example, **SHA256withRSA**. |

| Parameter | Type | Description |
|---|---|---|
| public_key | String | Public key content.<br>**NOTE**<br>The newline characters have been replaced with **\r\n**.<br>Minimum: **0**<br>Maximum: **4096** |
| distinguished_name | **DistinguishedName** object | Certificate name. For details, see data structure for the **DistinguishedName** field. |

**Table 4-184** DistinguishedName

| Parameter | Type | Description |
|---|---|---|
| common_name | String | Common certificate name (CN).<br>Minimum: **1**<br>Maximum: **64** |
| country | String | Country code, which must comply with the regular expression "**[A-Za-z]{2}**".<br>Minimum: **2**<br>Maximum: **2** |
| state | String | State or city name.<br>Minimum: **1**<br>Maximum: **128** |
| locality | String | Country/Region.<br>Minimum: **1**<br>Maximum: **128** |
| organization | String | Organization name.<br>Minimum: **1**<br>Maximum: **64** |
| organizational_unit | String | Organization Unit (OU).<br>Minimum: **1**<br>Maximum: **64** |

**Status code: 400**

**Table 4-185** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-186** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-187** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-188** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-189** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to parse a 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.ap-southeast-3.myhuaweicloud.com/v1/private-certificates/csr/parse

{
  "csr" : "-----BEGIN CERTIFICATE REQUEST-----\
\nMIICyTCCAbECAQAwXjELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB3NpY2hhdW4xEDAO\
\nBgNVBAcTB2NoZW5nZHUxCzAJBgNVBAoTAkhXMQswCQYDVQQLEwJJVDERMA8GA1UE\
\nAxMIdGVzdC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCZ4q5z\\nxqK/L/
FC9x2jESeUW5GB6zS5rVxT0WLTCTv9d1LtWBLsRIinATYTYiP1pNo4/pBq\
\nHlM3IiUDkc896CJerYlNzOIjTaV4GjCZvPrxSHU5toJvIDflBsY+gnzbT1ol/y0r\\n3yb9dx7eeF5rPR+U8RTw+Ov/
ZNRb+0CY30hrXMdrWjp5dtLGTlr5EFYxlKNOPCkR\\n
+6BGyJnC9PWSuqwsykFbgMRkcBaNAxa59dRhMF50pvx2Vs929vFrMi+ofDELUOqz\
\n1vyjaEA3pn3AGJGXZgrGNbSfz12ixgGLes4cQD21GCIAWgnBQ7b1ru2V8ImUfyh0\\nyvTEyHJTuFbQ
+257AgMBAAGgJjAkBgkqhkiG9w0BCQ4xFzAVMBMGA1UdEQQMMAqC\
\nCHRlc3QuY29tMA0GCSqGSIb3DQEBCwUAA4IBAQBKfjZuYsz4s0wb1POIWn41eiAB\
\np53qb63QKWILN9z8dLktcdSl3lPfcfPZpXv++QPtn3LR9rJKBawusk6SPXbvOGgS\\n5J
+6eM8kVW2O3gHFgoaMcPYVtiO7ekG6o25qx6+Rj84wbFdmpOiCc8AwrLEBwzYV\
\np1zaprWQu6PxBulkYPa3FLcntDdi7B67r0YTpxVvo1K7vHYFboDvPz7xG57QIFIM\
\nwGd1OegariMT3N8gBOzLZc+jqLpxgo4xoNqBHMo6DEmKLdWdzU4ljpuGK9had99k\\nvQ5vft/
Qra3v1uq2lOm/G92b0uA9Y1t2bMHobtAnuXL0HmY9XcLdzpC3f8h8\\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
\nU9UGOo8xCxux8k2dsXRnY+fxRiLWphiT2ij4CYURagETbKuRl9WOI+HFVkmIU/0p\r\n3FWqB0RdrRTEcAC
+S5fmW75E85rAMh9f65wa/6eWcM6vlnby4Bbm1mcJdR3olgKJ\r\nUQIDAQAB\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.

## URI

GET /v1/private-certificates/quotas

## Request Parameters

**Table 4-190** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 200**

**Table 4-191** Response body parameters

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

**Table 4-192** Quotas

| Parameter | Type | Description |
|---|---|---|
| resources | Array of **Resources** objects | Resource quota list. For details, see data structure for the **Resources** field. |

**Table 4-193** Resources

| Parameter | Type | Description |
|---|---|---|
| type | String | Certificate type<br>● **CERTIFICATE_AUTHORITY**: CA certificate.<br>● **CERTIFICATE**: private certificate. |
| used | Integer | Used quota |
| quota | Integer | Total quota<br>● **CERTIFICATE_AUTHORITY**: 100<br>● **CERTIFICATE**: 100,000 |

**Status code: 400**

**Table 4-194** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-195** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-196** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-197** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-198** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to query the private CA quota, 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.ap-southeast-3.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.

## URI

GET /v1/private-certificates/{certificate_id}

**Table 4-199** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate_id | Yes | String | ID of the private certificate you want to query.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-200** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 200**

**Table 4-201** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| certificate_id | String | ID of the private certificate<br>Minimum: **36**<br>Maximum: **36** |
| status | String | Certificate status:<br>● **ISSUED**: The certificate is issued.<br>● **EXPIRED**: The certificate expired.<br>● **REVOKED**: The certificate is revoked. |
| issuer_id | String | ID of the parent CA.<br>Minimum: **36**<br>Maximum: **36** |
| issuer_name | String | The name of the parent CA certificate.<br>Minimum: **1**<br>Maximum: **64** |
| key_algorithm | String | Key algorithm |
| signature_algorithm | String | Signature algorithm |

| Parameter | Type | Description |
|---|---|---|
| freeze_flag | Integer | Freezing tag:<br>- **0**: The certificate is not frozen.<br>- **Other values**: The certificate is frozen (The type of value is reserved). |
| gen_mode | String | Certificate generation method.<br>- **GENERATE**: The certificate is generated through the PCA system.<br>- **IMPORT**: The certificate is imported externally.<br>- **CSR**: The CSR is imported externally and issued by the internal CA. The private key is not managed in PCA. |
| serial_number | String | Serial number.<br>Minimum: **1**<br>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. |

**Table 4-202** DistinguishedName

| Parameter | Type | Description |
|---|---|---|
| common_name | String | Common certificate name (CN).<br>Minimum: **1**<br>Maximum: **64** |
| country | String | Country code, which must comply with the regular expression "**[A-Za-z]{2}**".<br>Minimum: **2**<br>Maximum: **2** |

| Parameter | Type | Description |
|---|---|---|
| state | String | State or city name.<br>Minimum: **1**<br>Maximum: **128** |
| locality | String | Country/Region.<br>Minimum: **1**<br>Maximum: **128** |
| organization | String | Organization name.<br>Minimum: **1**<br>Maximum: **64** |
| organizational_unit | String | Organization Unit (OU).<br>Minimum: **1**<br>Maximum: **64** |

**Status code: 400**

**Table 4-203** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-204** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-205** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-206** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-207** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to query details about a 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.

```
GET https://ccm.ap-southeast-3.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" : "20211015105754126608186 1",
  "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"
}
```

**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.

## URI

DELETE /v1/private-certificates/{certificate_id}

**Table 4-208** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate_id | Yes | String | ID of the private certificate you want to delete.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-209** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 400**

**Table 4-210** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-211** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-212** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-213** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-214** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to delete a 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.

```
DELETE https://ccm.ap-southeast-3.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. |
| 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**.

## 4.2.2.8 Exporting a Certificate

## Function

This API is used to export a certificate.

- 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**.
    - If **type** is set to **APACHE**, the compressed package contains three files: **server.key** (key file in PEM format), **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) and **server.pfx** (PFX certificate. The certificate and certificate chain are contained in the same file).
    - If **type** is set to **NGINX**, the compressed package contains two files: **server.key** (key file in PEM format) and **server.crt** (content in PEM format. The certificate and certificate chain are contained in the same file).
    - If **type**is set to **TOMCAT**, the compressed package contains two files: **keystorePass.txt** (keystore password) and **server.jks** (JKX certificate. The certificate and certificate chain are contained in the same file).
    - If **type** is set to **OTHER**, the compressed package contains three files: **server.key** (key file in PEM format), **chain.pem** (certificate chain), and **server.pem** (certificate).
  - If **is_compressed** is set to **false**, a certificate in JSON format is returned, including the following parameters:
    - 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**: indicates the certificate private key in PEM format.

- If **type** is set to "**IIS**" or "**TOMCAT**", it is not defined currently.

NOTE

Only certificates in the **Issued** status can be exported.

## URI

POST /v1/private-certificates/{certificate_id}/export

**Table 4-215** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate_id | Yes | String | ID of the private certificate you want to export.<br>Minimum: **36**<br>Maximum: **36** |

## 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**. |

**Table 4-217** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| is_compressed | Yes | String | Whether to compress.<br>● **true**<br>● **false** |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| type | Yes | String | Type of the server on which the certificate is installed. The options are as follows:<br>● **APACHE**: This parameter is recommended if you want to use the certificate for an Apache server.<br>● **NGINX**: This parameter is recommended if you want to use the certificate for an Nginx server.<br>● **IIS**: This parameter is recommended if you want to use the certificate for a Windows IIS server.<br>● **TOMCAT**: This parameter is recommended if you want to use the certificate for a Tomcat server.<br>● **OTHER**: This parameter is recommended if you want to download a certificate in PEM format. |

## Response Parameters

**Status code: 200**

**Table 4-218** 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 4-219** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-220** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-221** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-222** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-223** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to export a 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.ap-southeast-3.myhuaweicloud.com/v1/private-certificates/
6434f74f-2d13-4e6a-89eb-93ee313f1a43/export

{
  "type" : "other",
  "is_compressed" : false
}
```

## 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.

## URI

POST /v1/private-certificates/{certificate_id}/revoke

**Table 4-224** Path Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| certificate_id | Yes | String | ID of the private certificate you want to revoke.<br>Minimum: **36**<br>Maximum: **36** |

## Request Parameters

**Table 4-225** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

**Table 4-226** Request body parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| reason | No | String | Reason for revocation.The options are as follows:<br>● **UNSPECIFIED** : Default value. No reason is specified for revocation.<br>● **KEY_COMPROMISE** : The certificate key material has been leaked.<br>● **CERTIFICATE_AUTHORITY_COMPROMISE** : Key materials of the CA have been leaked in the certificate chain.<br>● **AFFILIATION_CHANGED** : The subject or other information in the certificate has been changed.<br>● **SUPERSEDED** : The certificate has been replaced.<br>● **CESSATION_OF_OPERATION** : The entity in the certificate or certificate chain has ceased to operate.<br>● **CERTIFICATE_HOLD** : The certificate should not be considered valid currently and may take effect in the future.<br>● **PRIVILEGE_WITHDRAWN** : This certificate no longer has permissions on the properties it claims.<br>● **ATTRIBUTE_AUTHORITY_COMPROMISE** : The authority which determines appropriate attributes for a Certificate may have been compromised.<br>NOTE<br>If you do not want to provide the revocation reason, set the request body to **{}**. Otherwise, an error will be reported. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| | | | Enumeration values:<br>- **UNSPECIFIED**<br>- **KEY_COMPROMISE**<br>- **CERTIFICATE_AUTHORITY_COMPROMISE**<br>- **AFFILIATION_CHANGED**<br>- **SUPERSEDED**<br>- **CESSATION_OF_OPERATION**<br>- **CERTIFICATE_HOLD**<br>- **PRIVILEGE_WITHDRAWN**<br>- **ATTRIBUTE_AUTHORITY_COMPROMISE** |

## Response Parameters

**Status code: 400**

**Table 4-227** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-228** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-229** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-230** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-231** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |

| Parameter | Type | Description |
|---|---|---|
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to revoke a 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.ap-southeast-3.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.

## URI

GET /v1/private-certificate-authorities/obs/agencies

## Request Parameters

**Table 4-232** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 200**

**Table 4-233** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| agency_granted | String | OBS agency status<br>- **true**<br>- **false** |

**Status code: 400**

**Table 4-234** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-235** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-236** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-237** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-238** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>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.ap-southeast-3.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.

## URI

POST /v1/private-certificate-authorities/obs/agencies

## Request Parameters

**Table 4-239** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

## Response Parameters

**Status code: 200**

**Table 4-240** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| agency_id | String | Authorization ID returned by IAM when an OBS agency is created. |

**Status code: 400**

**Table 4-241** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-242** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-243** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-244** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-245** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>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.ap-southeast-3.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.

### URI

GET /v1/private-certificate-authorities/obs/buckets

### Request Parameters

**Table 4-246** Request header parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| X-Auth-Token | Yes | String | User token. For details, see **Obtaining a User Token**. |

### Response Parameters

**Status code: 200**

**Table 4-247** 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. |

**Table 4-248** ObsBuckets

| Parameter | Type | Description |
|---|---|---|
| bucket_name | String | Bucket name<br>Minimum: **3**<br>Maximum: **63** |
| create_time | Long | Creation time. The value is a timestamp in milliseconds. |

**Status code: 400**

**Table 4-249** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 401**

**Table 4-250** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 403**

**Table 4-251** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 404**

**Table 4-252** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

**Status code: 500**

**Table 4-253** Response body parameters

| Parameter | Type | Description |
|---|---|---|
| error_code | String | Error code<br>Minimum: **3**<br>Maximum: **36** |
| error_msg | String | Error message<br>Minimum: **0**<br>Maximum: **1024** |

## Example Requests

When you use this API to query the list of OBS buckets, 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.ap-southeast-3.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**.

# 5 Examples

## 5.1 Example 1: Deleting an Expired SSL Certificate

### Scenario

This topic describes how to delete an expired SSL certificate using the SCM API.

NOTE

- This topic only describes how to delete an SSL certificate from Huawei Cloud. The certificate will still be valid and trusted by web browsers.
- After you submit a certificate deletion application, you cannot cancel it. Exercise caution when performing this operation.

### Involved APIs

- **Querying the certificate list**: Query all SSL certificates under your current account.
- **Deleting a certificate**: Delete a specific expired SSL certificate.

### Procedure

**Step 1** Query the certificate list.

- API information

  URI format: GET /v3/scm/certificates

  For details, see **Querying the Certificate List**.

- Example request

  GET: https://*{endpoint}*/v3/scm/certificates

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

```
{
   "limit": "2",
   "offset": "0"
}
```

- Example response

```
{
 "certificates" : [ {
  "id" : "scs1554192131150",
  "name" : "test",
  "domain" : "www.zx.com",
  "type" : "OV_SSL_CERT",
  "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
}
```

**Step 2** Delete a certificate.

- API information

  URI format: DELETE /v3/scm/certificates/{certificate_id}

  For details, see **Deleting a Certificate**.

- Example request

  DELETE: https://*{endpoint}*/v3/scm/certificates/scs1554192131150

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

```
{
 certificate_id:scs1554192131150
}
```

- Example response

```
{ }
```

or

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

**----End**

# 5.2 Example 2: Pushing Your External SSL Certificate to Other Services

## Scenario

This topic describes how to import your SSL certificates purchased on other platforms to SCM and push such certificates to your cloud services on Huawei Cloud, such as WAF and CDN, to keep your workloads secure.

## Involved APIs

- **Importing a certificate**: Import an SSL certificate not purchased on SCM into SCM for centralized management.
- **Querying the certificate list**: Query all certificates under your current account and obtain the ID of the certificate to be pushed.

- **Pushing a certificate**: Push an SSL certificate imported into SCM to other Huawei Cloud services.

## Procedure

**Step 1** Import the certificate.

- API information

  URI format: POST /v3/scm/certificates/import

  For details, see **Importing a Certificate**

- Example request

  POST: https://*{endpoint}*/v3/scm/certificates/import

  Obtain *{endpoint}* from **Regions and Endpoints**.

- Example response

```
{
  "certificate_id" : "scs1554192131150"
}
```

**Step 2** Query the certificate list.

- API information

  URI format: GET /v3/scm/certificates

  For details, see **Querying the Certificate List**.

- Example request

  GET: https://*{endpoint}*/v3/scm/certificates

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

```
{
    "limit": "2",
    "offset": "0"
}
```

- Example response

```
{
  "certificates" : [ {
    "id" : "scs1554192131150",
    "name" : "test",
    "domain" : "www.zx.com",
    "type" : "OV_SSL_CERT",
    "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
}
```

**Step 3** Push a certificate.

- API information

  URI format: POST /v3/scm/certificates/{certificate_id}/push

  For details, see **Pushing a Certificate**

- Example request

POST: https://*{endpoint}*/v3/scm/certificates/scs1554192131150/push

Obtain *{endpoint}* from **Regions and Endpoints**.

- Example response

```
{
  }
```

or

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

**----End**

# 5.3 Example 3: Pushing Your SSL Certificate Purchased Through CCM to Other Services

## Scenario

This topic describes how to push a certificate purchased and issued in CCM to WAF and CDN on Huawei Cloud to keep your workloads secure.

## Involved APIs

- **Querying the certificate list**: Query all certificates under your current account and obtain the ID of the certificate to be pushed.
- **Pushing a certificate**: Push an SSL certificate you have purchased in CCM to other Huawei Cloud services.

## Procedure

**Step 1** Query the certificate list.

- API information

  URI format: GET /v3/scm/certificates

  For details, see **Querying the Certificate List**.
- Example request

  GET: https://*{endpoint}*/v3/scm/certificates

  Obtain *{endpoint}* from **Regions and Endpoints**.

  Body:

```
{
    "limit": "2",
    "offset": "0"
}
```

- Example response

```
{
  "certificates" : [ {
    "id" : "scs1554192131150",
    "name" : "test",
    "domain" : "www.zx.com",
    "type" : "OV_SSL_CERT",
    "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
}
```

**Step 2** Push an SSL certificate to other services.

- API information

  URI format: POST /v3/scm/certificates/{certificate_id}/push

  For details, see **Pushing a Certificate**

- Example request

  POST: https://*{endpoint}*/v3/scm/certificates/scs1554192131150/push

  Obtain *{endpoint}* from **Regions and Endpoints**.

- Example response

  ```
  {
    }
  ```

  or

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

**----End**

# 6 Historical APIs

## 6.1 SCM APIs

### 6.1.1 Purchasing an SSL Certificate

#### Function

This API is used to purchase an SSL certificate.

NOTE

The request parameter **agree_privacy_protection** must be set to **true**. Otherwise, the certificate purchase application cannot be submitted.

#### URI

- URI format

  POST /v2/{project_id}/scm/cert/purchase

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |

#### Request

Request parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_brand | Yes | String | Certificate brand.<br>For example: GLOBALSIGN |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_type | Yes | String | Certificate type. Options:<br>- DV_SSL_CERT<br>- DV_SSL_CERT_BASIC<br>- EV_SSL_CERT<br>- EV_SSL_CERT_PRO<br>- OV_SSL_CERT<br>- OV_SSL_CERT_PRO |
| domain_type | Yes | String | Domain name type. Options:<br>- **SINGLE_DOMAIN**: single-domain name type.<br>- **MULTI_DOMAIN**: multi-domain name type.<br>- **WILDCARD**: wildcard domain name type. |
| effective_time | Yes | Integer | Certificate validity period, in years. Options:<br>- **1**: Purchase a certificate with a validity period of one year.<br>- **2**: Purchase a certificate with a validity period of two years. |
| domain_numbers | Yes | Integer | Number of domain names.<br>- If **domain_type** is set to **SINGLE_DOMAIN** or **WILDCARD**, the value of **domain_numbers** is **1**.<br>- If **domain_type** is set to **MULTI_DOMAIN**, the value of **domain_numbers** ranges from 2 to 100. |
| order_number | Yes | Integer | Number of purchased certificates. Value range: 1-1000. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| agree_privacy_protection | Yes | Boolean | Whether to agree with the privacy statement.<br>● **true**: Agree with the privacy statement.<br>● **false**: Disagree with the privacy statement.<br>You can purchase a certificate only when this parameter is set to **true**. |

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| order_id | Yes | String | Order ID. |
| cert | Yes | Array of cert objects | Certificate list. For details, see **Table 6-1**. |

**Table 6-1** cert

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_id | Yes | String | Certificate ID. |

## Example

The following describes how to purchase a multi-domain OV certificate issued by GlobalSign. Assume that the domain quantity is 5, and the validity period is one year.

- Example request
```
{
 "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 response
```
{
"order_id": "CS1803192259ROA8U"
"cert": [{
        "cert_id": "scs1481110651012",
    }]
}
```

or

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

## Status Codes

**Table 6-2** lists the normal status code returned by the API.

**Table 6-2** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error code, see **Error Codes**

# 6.1.2 Querying the Certificate List

## Function

This API is used to query the certificate list based on a certificate name or bound domain name.

NOTICE

This API will be discarded. You are advised to query certificates by referring to **Querying the Certificate Lists**.

## URI

- URI format

  GET /v2/{project_id}/scm/certlist?order_status=&content=&sort_key=&sort_dir=&limit=&offset=

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |

## Request

Request parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| order_status | No | String | Certificate status. Options:<br>- **PAID**: The certificate has been paid.<br>- **ISSUED**: The certificate has been issued.<br>- **CHECKING**: The certificate application is being reviewed.<br>- **CANCELCHECKING**: The certificate application cancellation is being reviewed.<br>- **UNPASSED**: The certificate application fails.<br>- **EXPIRED**: The certificate has expired.<br>- **REVOKING**: The certificate revocation application is being reviewed.<br>- **REVOKED**: The certificate has been revoked.<br>- **UPLOAD**: The certificate is being hosted.<br>- **SUPPLEMENTCHECKING**: Additional domain names to be added for a multi-domain certificate is being reviewed.<br>- **CANCELSUPPLEMENTING**: The cancellation on additional domain names to be added is being reviewed. |
| content | No | String | Keyword for search. |
| sort_key | No | String | Sorting criterion. Options:<br>- **certExpiredTime**: certificate expiration time.<br>- **certStatus**: certificate status.<br>- **certUpdateTime**: certificate update time. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| sort_dir | No | String | Sorting method. Sorting is performed based on the sorting parameter **sort_key**. Options:<br>• **ASC**: ascending order.<br>• **DESC**: descending order. |
| limit | No | Integer | Maximum number of pieces of certificate information to be displayed on each page. Options:<br>• **10**: Each page displays up to 10 pieces of certificate information.<br>• **20**: Each page displays up to 20 pieces of certificate information.<br>• **50**: Each page displays up to 50 pieces of certificate information. |
| offset | No | Integer | Offset. Value range: 1-30. |

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| total | Yes | Integer | Number of certificates in a list. |
| free_remain | Yes | Integer | Remaining quota of the free test certificate. |
| order_list | Yes | Array of order_list objects | Certificate list. For details, see **Table 6-3**. |

**Table 6-3** order_list

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_id | Yes | String | Certificate ID. |
| cert_name | Yes | String | Certificate name. |
| domain | Yes | String | Bound domain name. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_type | Yes | String | Certificate type. |
| cert_brand | Yes | String | Certificate brand. |
| domain_type | Yes | String | Domain name type. |
| purchase_period | Yes | Integer | Validity period. |
| expired_time | Yes | String | Certificate expiration time. |
| order_status | Yes | String | Certificate status. |
| domain_num | Yes | Integer | Number of domain names. |
| wildcard_number | Yes | Integer | Number of wildcard domain names. |
| cert_des | Yes | String | Certificate description. |

## Example

- Example request

  None

- Example response

```
{
"total": 1,
"free_remain":"19",
"order_list": [{
"cert_id": "scs1481110651012",
"cert_name": "scs-0001",
"domain": "*.example.com",
"cert_type": "GE00V01",
"cert_brand":"GLOBALSIGN",
"domain_type":" SINGLE_DOMAIN ",
"purchase_period":1,
"expired_time":"15051501510501",
"order_state":"completed ",
"domain_num":10,
"wildcard_number":2,
"cert_des":"************"
}]
}
```

  or

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

## Status Codes

Table 6-4 lists the normal status code returned by the API.

**Table 6-4** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error code, see **Error Codes**

## 6.1.3 Querying Details of a Certificate

### Function

This API is used to query details of a certificate.

NOTICE

This API will be discarded. You are advised to obtain certificate details by referring to **Obtaining Details of a Certificate**.

### URI

- URI format

  GET /v2/{project_id}/scm/cert/{cert_id}

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

### Request

Request parameters

None

### Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_id | Yes | String | Certificate ID. |
| order_id | Yes | String | Order ID. |
| cert_name | Yes | String | Certificate name. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_type | Yes | String | Certificate type.<br>Example: OV |
| cert_brand | Yes | String | Certificate brand.<br>Example: GLOBALSIGN |
| domain_type | Yes | String | Domain name type.<br>Example: MUILT_DOMAIN |
| domain_name | Yes | String | Domain name bound to a certificate.<br>Example: funnyzx.com;abc.com |
| domain_number | Yes | Integer | Number of domains.<br>Example: 3 |
| cert_describe | Yes | String | Certificate description. |
| push_support | Yes | String | Whether a certificate can be pushed. |
| revoke_reason | Yes | String | Reason for certificate revocation. |
| domain_name | Yes | String | Domain name bound to a certificate. Multiple domain names are separated by semicolons (;).<br>Example: www.example.com;www.example1.com;www.example2.com |
| company_name | Yes | String | Company name. |
| company_province | Yes | String | State or region where a company is located. |
| company_city | Yes | String | City where a company is located. |
| applicant_name | Yes | String | Name of a company contact. |
| applicant_phone | Yes | String | Phone number of a company contact. |
| applicant_email | Yes | String | Email of a company contact. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| contact_name | Yes | String | Name of a technical contact. |
| contact_phone | Yes | String | Phone number of a technical contact. |
| contact_email | Yes | String | Email of a technical contact. |
| status | Yes | String | Certificate status. |
| encrypt_type | Yes | String | Signature encryption algorithm. |
| country | Yes | String | Country code. |
| organization_unit | Yes | String | Company department. |
| DNS_push_status | Yes | String | DNS push status<br>● **ON**: indicates that the push is successful.<br>● **OFF**: indicates that the push fails.<br>● NONE: indicates that the push function is not enabled. |
| auth | Yes | Array of auth objects | Certificate authentication status. For details, see **Table 6-5**. |

**Table 6-5** auth

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| method | Yes | String | Authentication method. |
| status | Yes | String | Certificate authentication status. |
| domain_name | Yes | String | Domain name for DNS authentication. |
| host_record | Yes | String | Host record of DNS authentication. |
| record_type | Yes | String | Record type of DNS authentication. |
| record | Yes | String | Record value of DNS authentication. |

## Example

- Example request

  None

- Example response

```
{
"cert_id": "scs1481110651012",
"order_id ": "CS1803192259ROA8U",
"cert_name": "test",
"cert_type": "OV",
"cert_brand": "GEOTRUST",
"domain_type": "MUILT_DOMAIN",
"domain_name": "funnyzx.com;abc.com",
"domain_number": 3,
"cert_describe": "XXXXXXXXX",
"push_support": "on",
"revoke_reason":"xxxxxxxxxxx",
"domain_name": " www.test.com;*.example1.com;*.example2.com",
"company_name": "Huawei Technologies Co., Ltd.",
"company_province": "Guangdong",
"company_city": "Shenzhen",
"applicant_name": "Tom",
"applicant_phone": "13087654321",
"applicant_email": "example@xx.com",
"contact_name": "Jacky",
"contact_phone": "13087654321",
"contact_email": "example@xx.com",
"status": "PAID",
"encrypt_type": "SHA256withRSA2048",
"country": "CN",
"organization_unit": "unit",
"DNS_push_status": "ON",
"auth": [{
"method": "DNS",
"status": " checking ",
"domain_name": "www.test.com",
"host_record": "dnsauth",
"record_type": "TXT",
"record": "201803272148qwedginciog08"
 }]
}
```

  or

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

## Status Codes

**Table 6-6** lists the normal status code returned by the API.

**Table 6-6** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error code, see **Error Codes**

## 6.1.4 Modifying a Certificate

### Function

This API is used to change the name or description of a certificate.

### URI

- URI format
  PUT /v2/{project_id}/scm/cert/{cert_id}
- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

### Request

Request parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| modify_key | Yes | String | Change key. The value can be **CERT_NAME** or **DESCRIPTION**.<br>● **CERT_NAME**: indicates the name of a certificate to be modified.<br>● **DESCRIPTION**: indicates the description of a certificate to be modified. |
| modify_value | Yes | String | Modification details.<br>● If the change key is **CERT_NAME**, the value can contain only digits, letters, and hyphens (-). The value is a string of 0 to 63 characters and cannot be null.<br>● When the change key is **DESCRIPTION**, the value is a string of 0 to 255 characters and can be null. |

### Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| response_info | Yes | String | Request result. |

## Examples

The following describes how to change the certificate name to **sssaaaa**.

- Example request

```
{
"modify_key":"CERT_NAME",
"modify_value": "sssaaaa"
}
```

- Example response

```
{
"response_info":"success"
}
```

  or

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

## Status Codes

**Table 6-7** lists the normal status code returned by the API.

**Table 6-7** Status Code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error code, see **Error Codes**

# 6.1.5 Querying the Product Type of a Certificate

## Function

This API is used to query information about all products that are being sold on SCM.

## URI

- URI format

  GET /v2/{project_id}/scm/cert/product

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |

## Request

Request parameters

None

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| type_list | Yes | Array of type_list objects | Product type list. For details, see **Table 6-8**. |

**Table 6-8** type_list

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_type | Yes | String | Certificate type.<br>• **OV_SSL_CERT**: Organization Validation (OV) SSL certificate.<br>• **EV_SSL_CERT**: Extended Validation (EV) SSL certificate. |
| cert_brand | Yes | String | Certificate brand.<br>**GLOBALSIGN**: GlobalSign brand. |
| domain_type | Yes | String | Domain name type.<br>• **SINGLE_DOMAIN**: single-domain name type.<br>• **MULTI_DOMAIN**: multi-domain name type.<br>• **WILDCARD**: wildcard domain name type. |
| product_id | Yes | String | Product ID. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| effective_time | Yes | Integer | Certificate validity period (year).<br>● **1**: The validity period of the certificate is one year.<br>● **2**: The validity period of the certificate is two years. |
| product_name | Yes | String | Product name. |

## Example

- Example request

  None

- Example response

```
{
"type_list": [{
"cert_type": "OV_SSL_CERT",
"cert_brand":"GLOBALSIGN",
"domain_type":"SINGLE_DOMAIN",
"product_id":"00301-106005-0--0",
"effective_time":1,
"product_name ":"globalsign.single.ov.2"
}]
}
```

  or

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

## Status Codes

**Table 6-9** lists the normal status code returned by the API.

**Table 6-9** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error code, see **Error Codes**

# 6.1.6 Querying the Product Details of a Certificate

## Function

This API is used to query details about a specified certificate.

## URI

- URI format

  GET /v2/{project_id}/scm/product/{product_id}
- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| product_id | Yes | String | Product ID. |

## Request

Request parameters

None

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_type | Yes | String | Certificate type.<br>● **OV_SSL_CERT**: Organization Validation (OV) SSL certificate.<br>● **EV_SSL_CERT**: Extended Validation (EV) SSL certificate. |
| cert_brand | Yes | String | Certificate brand.<br>**GLOBALSIGN**: GlobalSign brand. |
| domain_type | Yes | String | Domain name type.<br>● **SINGLE_DOMAIN**: single-domain name type.<br>● **MULTI_DOMAIN**: multi-domain name type.<br>● **WILDCARD**: wildcard domain name type. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| effective_time | Yes | Integer | Certificate validity period, in years.<br>● **1**: The validity period of the certificate is one year.<br>● **2**: The validity period of the certificate is two years. |

## Example

- Example request

  None

- Example response

```
{
"cert_type": "OV_SSL_CERT",
"cert_brand":"GLOBALSIGN",
"domain_type":"SINGLE_DOMAIN",
"effective_time":1
}
```

  or

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

## Status Codes

**Table 6-10** lists the normal status code returned by the API.

**Table 6-10** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.7 Applying for a Certificate

## Function

This API is used to complete certificate application information, such as the domain name bound to a certificate and the applicant's detailed information.

NOTE

The request parameter **agree_privacy_protection** must be set to **true**. Otherwise, the certificate application information cannot be submitted.

## URI

- URI format
  POST /v2/{project_id}/scm/cert/{cert_id}/complete
- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| domain | Yes | String | Domain name bound to a certificate.<br>● If the certificate to be purchased is a single-domain or wildcard domain name certificate, enter the single-domain or wildcard domain name.<br>● If the certificate to be purchased is a multi-domain certificate, select one domain name as the primary domain name.<br>Example: www.example.com |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| sans | No | String | Additional domain name of the certificate that is bound to a multi-domain certificate.<br>Set this parameter only when the certificate to be purchased is a multi-domain certificate and the number of additional domain names can be increased.<br>Multiple domain names must be separated by semicolons (;).<br>Example: www.example.com;www.example1.com;www.example2.com |
| csr | No | String | Certificate CSR, which must match the domain name. |
| company_name | Yes | String | Company name. This parameter is mandatory for certificates of the OV and EV types.<br>The value must contain 0 to 63 characters. |
| company_unit | No | String | Department name. This parameter is optional for certificates of the OV and EV types.<br>The value must contain 0 to 63 characters. |
| company_province | Yes | String | State or region where a company is located. This parameter is mandatory for certificates of the OV and EV types.<br>The value must contain 0 to 63 characters. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| company_city | Yes | String | City where a company is located. This parameter is mandatory for certificates of the OV and EV types.<br>The value must contain 0 to 63 characters. |
| country | Yes | String | Country code.<br>● **CN**: China<br>● **US**: United States |
| applicant_name | Yes | String | Applicant name.<br>The value must contain 0 to 63 characters. |
| applicant_phone | Yes | String | Phone number of an applicant.<br>Example: 13212345678 |
| applicant_email | Yes | String | Email of an applicant.<br>Example: example.huawei.com |
| contact_name | No | String | Name of a technical contact.<br>The value must contain 0 to 63 characters. |
| contact_phone | No | String | Phone number of a technical contact.<br>Example: 13212345678 |
| contact_email | No | String | Email of a technical contact.<br>Example: example.huawei.com |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| auto_dns_auth | No | Boolean | Whether to push DNS authentication information to HUAWEI CLOUD DNS.<br>● **true**: DNS authentication information is pushed to HUAWEI CLOUD DNS.<br>● **false**: DNS authentication information is not pushed to HUAWEI CLOUD DNS. |
| agree_privacy_protection | Yes | Boolean | Whether to agree with the privacy statement.<br>● **true**: Agree with the privacy statement.<br>● **false**: Disagree with the privacy statement.<br>You can submit your certificate application only when this parameter is set to **true**. |

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| request_info | Yes | String | Request result. |

## Example

The following describes how to supplement information about a certificate.

- Example request

```
{
   "domain":"www.xzz.com",
    "company_name": "Huawei Chengdu branch",
   "company_province": "Sichuan",
  "company_city": "Chengdu",
   "applicant_name": "Tom",
   "applicant_phone":"13212345678",
   "applicant_email":"9997342346@qq.com",
   "csr":"",
   "sans":"",
   "country":"CN",
   "company_unit": "Human Resource Dept",
   "contact_name": "Jacky",
   "contact_phone":"13512345678",
   "contact_email":"jk@jk.ff",
   "auto_dns_auth":false,
   "agree_privacy_protection":true
}
```

- Example response

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

or

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

## Status Codes

Table 6-11 lists the normal status code returned by the API.

**Table 6-11** Status Codes

| Status Codes | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.8 Verifying a CSR

## Function

This API is used to verify a certificate signing request (CSR) and resolve the domain name.

## URI

- URI format

  POST /v2/{project_id}/scm/check-csr

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |

## Request

Request parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| csr | Yes | String | Certificate signing request. |

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| domain_name | Yes | String | Domain name in the CSR. |

## Example

The following describes how to verify a CSR.

- Example request

```
{
    "csr":"-----BEGIN NEW CERTIFICATE REQUEST-----******-----END NEW CERTIFICATE REQUEST-----"
}
```

- Example response

```
{
    "domain": "a.example1.com"
}
```

or

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

## Status Codes

**Table 6-12** lists the normal status code returned by the API.

**Table 6-12** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.9 Saving Certificate Information

## Function

This API is used to save certificate information entered during certificate application.

NOTE

The request parameter **agree_privacy_protection** must be set to **true**. Otherwise, certificate information cannot be saved.

## URI

- URI format
  POST /v2/{project_id}/scm/cert/{cert_id}/save
- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| domain | Yes | String | Domain name bound to a certificate. |
| sans | No | String | Additional domain names of a multi-domain certificate. Multiple domain names are separated by semicolons (;). |
| csr | No | String | Certificate csr string, which must match the domain name. |
| company_name | Yes | String | Company name. This parameter is mandatory for certificates of the OV and EV types.<br>The value must contain 0 to 63 characters. |
| company_unit | No | String | Department name. This parameter is optional for certificates of the OV and EV types.<br>The value must contain 0 to 63 characters. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| company_province | Yes | String | State or region where a company is located. This parameter is mandatory for certificates of the OV and EV types.<br>The value must contain 0 to 63 characters. |
| company_city | Yes | String | City where a company is located. This parameter is mandatory for certificates of the OV and EV types.<br>The value must contain 0 to 63 characters. |
| country | Yes | String | Country code. |
| applicant_name | Yes | String | Applicant name.<br>The value must contain 0 to 63 characters. |
| applicant_phone | Yes | String | Phone number of an applicant.<br>Example: 13212345678 |
| applicant_email | Yes | String | Email of an applicant.<br>Example: example.huawei.com |
| contact_name | No | String | Name of a technical contact.<br>The value must contain 0 to 63 characters. |
| contact_phone | No | String | Phone number of a technical contact.<br>Example: 13212345678 |
| contact_email | No | String | Email of a technical contact.<br>Example: example.huawei.com |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| agree_privacy_protection | Yes | Boolean | Whether to agree with the privacy statement.<br>- **true**: Agree with the privacy statement.<br>- **false**: Disagree with the privacy statement.<br>You can save certificate information only when this parameter is set to **true**. |

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| request_info | Yes | String | Request result. |

## Example

The following describes how to save supplemented information about a certificate.

- Example request

```
{
   "domain":"www.xzz.com",
    "company_name": "Huawei Chengdu branch",
   "company_province": "Sichuan",
  "company_city": "Chengdu",
   "applicant_name": "Tom",
   "applicant_phone":"13212345678",
   "applicant_email":"9997342346@qq.com",
   "csr":"",
   "sans":"",
   "country":"CN",
   "company_unit": "Human Resource Dept",
   "contact_name": "Jacky",
   "contact_phone":"13512345678",
   "contact_email":"jk@jk.ff",
   "agree_privacy_protection":true
}
```

- Example response

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

or

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

## Status Codes

Table 6-13 lists the normal status code returned by the API.

**Table 6-13** Status codes

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.10 Reading the Information Entered When Applying for a Certificate

## Function

This API is used to read the saved information about a certificate.

## URI

- URI format

  POST /v2/{project_id}/scm/cert/{cert_id}/read
- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

None

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| domain_name | Yes | String | Domain name bound to a certificate.<br>Example: www.domain.com |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| sans | Yes | String | Additional domain names of a multi-domain certificate. Multiple domain names are separated by semicolons (;).<br>If a single-domain or wildcard domain certificate is applied for, the value of this parameter is empty. |
| CSR | Yes | String | Certificate signing request. |
| country | Yes | String | Country code. Example:<br>● **CN**: China<br>● **US**: United States |
| company_name | Yes | String | Company name. |
| company_unit | Yes | String | Department name |
| company_province | Yes | String | State or region where a company is located.<br>Example: Sichuan |
| company_city | Yes | String | City where a company is located.<br>Example: Chengdu |
| applicant_name | Yes | String | Applicant name.<br>Example: Tom |
| applicant_phone | Yes | String | Phone number of an applicant.<br>Example: 13412345678 |
| applicant_email | Yes | String | Email of an applicant.<br>Example: example.huawei.com |
| contact_name | Yes | String | Name of a technical contact. |
| contact_phone | Yes | String | Phone number of a technical contact. |
| contact_email | Yes | String | Email of a technical contact. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| bl | Yes | String | Whether the picture of bank account opening permit has been uploaded.<br>● **0**: The picture of bank account opening permit has not been uploaded.<br>● **1**: The picture of bank account opening permit has been uploaded. |
| tl | Yes | String | Whether the business license of the company has been uploaded.<br>**0**: The business license of the company has not been uploaded.<br>**1**: The business license of the company has been uploaded. |

## Example

- Example request

  None

- Example response

```
{
    "domain_name": "www.xzz.com",
    "sans": "",
    "CSR": null,
    "country": "CN",
    "company_unit": "Human Resource Dept",
     "company_name": "Huawei Chengdu branch",
    "company_province": "Sichuan",
   "company_city": "Chengdu",
    "applicant_name": "Tom",
    "applicant_phone": "13245678932",
    "applicant_email": "1027342346@qq.com",
    "contact_name": "Jacky",
    "contact_phone": "13526456325",
    "contact_email": "jk@jk.ff",
    "bl": "0",
    "tl": "1"
}
```

  or

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

## Status Codes

**Table 6-14** lists the normal status code returned by the API.

**Table 6-14** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.11 Canceling an Application

## Function

This API is used to cancel an application of certificate reviewing.

## URI

- URI format
  POST /v2/{project_id}/scm/cert/{cert_id}/cancel-cert
- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

None

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_id | Yes | String | Certificate ID. |
| message | Yes | String | Request result. |

## Example

- Example request
  None

- Example response
  ```
  {
     "cert_id": " scs1481110651012",
     "message": "success"
  }
  ```
  or
  ```
  {
    "error_code": "SCM.XXXX",
    "error_msg": "XXXX"
   }
  ```

## Status Codes

**Table 6-15** lists the normal status code returned by the API.

**Table 6-15** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.12 Deleting a Certificate

## Function

This API is used to delete a certificate, that is, delete a certificate from HUAWEI CLOUD.

NOTICE

This API will be discarded. You are advised to delete a certificate by referring to **Deleting a Certificate**.

## URI

- URI format
  DELETE /v2/{project_id}/scm/cert/{cert_id}
- Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

None

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| message | Yes | String | Request result. |

## Example

- Example request

  None

- Example response

```
{
    "message": "success"
}
```

or

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

## Status Codes

**Table 6-16** lists the normal status code returned by the API.

**Table 6-16** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.13 Uploading Authentication Information

## Function

This API is used to upload the authentication information picture required for certificate review.

## URI

- URI format

  POST /v2/{project_id}/scm/cert/{cert_id}/info/{type}/upload_authentication

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| type | Yes | String | Type of the content to be uploaded.<br>● **BL**: bank account opening permit.<br>● **TL**: business license of a company. |
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

None

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| request_info | Yes | String | Request result. |

## Example

- Example request

```
{
    <Upload content>
}
```

- Example response

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

or

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

## Status Codes

**Table 6-17** lists the normal status code returned by the API.

**Table 6-17** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.14 Downloading a Certificate

## Function

This API is used to download a certificate.

NOTICE

This API will be discarded. You are advised to export a certificate by referring to **Exporting a Certificate**.

## URI

- URI format

  GET /v2/{project_id}/scm/cert/{cert_id}/cert_file
- Parameter description

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

## Requests

Request parameters

None

## Responses

Certificate file, which is a compressed package with the .rar extension.

## Examples

- Example request

  None
- Example response

```
{
   <Object Content>
}
```

or

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

## Status Codes

Table 6-18 lists the normal status code returned by the API.

**Table 6-18** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.15 Uploading a Certificate

## Function

This API is used to upload a certificate to SCM.

## URI

- URI format

  POST /v2/{project_id}/scm/cert/upload

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |

## Request

Request parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_name | Yes | String | Certificate name.<br>The value is a string of 0 to 63 characters. |
| cert | Yes | String | Certificate chain content. |
| private_key | Yes | String | Private key of a certificate. |

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_id | Yes | String | Certificate ID. |

## Example

The following describes how to upload a certificate named **test**.

- Example request
```
{
   "cert_name":"test",
   "cert":"-----BEGIN CERTIFICATE----- *** -----END CERTIFICATE-----",
   "private_key": "-----BEGIN RSA PRIVATE KEY----- *** -----END RSA PRIVATEKEY-----"
}
```
- Example response
```
{
   "cert_id": " scs1481110651012"
}
```
  or
```
{
  "error_code": "SCM.XXXX",
  "error_msg": "XXXX"
 }
```

## Status Codes

**Table 6-19** lists the normal status code returned by the API.

**Table 6-19** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.16 Revoking a Certificate

## Function

This API is used to revoke a certificate.

## URI

- URI format

  POST /v2/{project_id}/scm/cert/{cert_id}/revoke
- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| reason | Yes | String | Reason for revoking a certificate.<br>The value is a string of 0 to 63 characters. |

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| message | Yes | String | Revocation request result. |

## Examples

The following uses the certificate revocation reason "certificate information filled incorrectly" as an example.

- Example request
```
{
   "reason": "certificate information filled incorrectly",
}
```
- Example response
```
{
   "message":"success"
}
```
  or
```
{
  "error_code": "SCM.XXXX",
  "error_msg": "XXXX"
 }
```

## Status Codes

**Table 6-20** lists the normal status code returned by the API.

**Table 6-20** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

## 6.1.17 Pushing a Certificate

### Function

This API is used to push an SSL certificate to other HUAWEI CLOUD services, such as Web Application Firewall (WAF) and Content Delivery Network (CDN).

NOTICE

This API will be discarded. You are advised to push a certificate by referring to **Pushing a Certificate**.

### URI

- URI format

  POST /v2/{project_id}/scm/cert/{cert_id}/push

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

### Request

Request parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| service_type | Yes | String | Type of the service to which a certificate is pushed. Options:<br>**CDN** and **WAF** |
| remote_project | Yes | String | Region where the target service to which a certificate is pushed. |

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| message | Yes | String | Request result. |

## Example

The following describes how to push a certificate to WAF in region **ap-southeast-1**.

- Example request

```
{
    "service_type":"WAF",
    "remote_project":"ap-southeast-1"
}
```

- Example response

```
{
    "message":"success"
}
```

  or

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

## Status Codes

**Table 6-21** lists the normal status code returned by the API.

**Table 6-21** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.18 Querying Push Records

## Function

This API is used to query the last 10 certificate push records, which are to be pushed to another HUAWEI CLOUD service.

## URI

- URI format

  GET /v2/{project_id}/scm/cert/{cert_id}/push-history

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

None

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| push_history_list | Yes | Array of push_history_list objects | Push record list. For details, see **Table 6-22**. |

**Table 6-22** push_history_list

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| push_time | Yes | String | Push time, in milliseconds. |
| push_remote_project | Yes | String | Push project. |
| push_service | Yes | String | Push service type.<br>● **WAF**: A certificate is pushed to WAF.<br>● **CDN**: A certificate is pushed to CDN. |

## Example

- Example request

  None

- Example response

```
{
    "push_history_list": [
        {
            "push_time": "1556257820000",
            "push_remote_project": null,
            "push_service": "CDN"
    },
    {
      "push_time": "1556257447000",
      "push_remote_project": "ap-southeast-1",
      "push_service": "WAF"
    }
  ]
}
```

or

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

## Status Codes

**Table 6-23** lists the normal status code returned by the API.

**Table 6-23** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.19 Canceling Authorization for Privacy Information

## Function

This API is used to cancel authorization for privacy information and delete the privacy data saved in SCM.

## URI

- URI format

  DELETE /v2/{project_id}/scm/privacy-protection/{cert_id}

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

None

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| message | Yes | String | Request result. |

## Example

- Example request

  None

- Example response

```
{
   "message":"success"
}
```

or

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

## Status Codes

**Table 6-24** lists the normal status code returned by the API.

**Table 6-24** Status code

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.20 Adding an Additional Domain Name

## Function

This API is used to add an additional domain name. If you have a multi-domain SSL certificate and available quota for additional domain names, you can add additional domain names for the certificate after it is issued.

## URI

- URI format

  POST /v2/{project_id}/scm/cert/{cert_id}/supplement

- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| ori_sans | Yes | String | Additional domain name bound to a multi-domain certificate.<br>If multiple domain names are displayed, the domain names are separated by semicolons (;).<br>Example: example.domain.com;example.domain1.com |
| add_sans | No | String | Additional domain name to be added for a multi-domain certificate.<br>If multiple domain names need to be entered, separate the domain names by semicolons (;).<br>Example: example.domain2.com;example.domain3.com |
| email | No | String | Email of a contact. |

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| request_info | Yes | String | Request result. |

## Example

The following describes how to add an additional domain name **example.domain.com**.

- Example request

```
{
    "ori_sans": "abc.com;xyz.com",
    "add_sans": "example.domain.com",
    "email": "example@xx.com"
}
```

- Example response

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

or

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

## Status Codes

**Table 6-25** lists the normal status code returned by the API.

**Table 6-25** Status codes

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 6.1.21 Querying Domain Name Verification Information

## Function

This API is used to query domain name verification details.

## URI

- URI format
  GET /v2/{project_id}/scm/cert/{cert_id}/domain-verify
- Parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| project_id | Yes | String | Project ID. |
| cert_id | Yes | String | Certificate ID. |

## Request

Request parameters

None.

## Response

Response parameters

| Parameter | Mandatory | Type | Description |
|---|---|---|---|
| domain_name | Yes | String | Domain name for ownership verification. |
| domain_email | Yes | String | Email address used for domain name verification. |
| record_name | Yes | String | Host record |
| record_value | Yes | String | DNS record |
| record_type | Yes | String | Record type |
| domain_method | Yes | String | Verification method |
| applicant_email | Yes | String | Email of the applicant. |
| auto_dns_auth | Yes | boolean | Whether the domain name ownership is verified in an automated manner. |

## Example

```
{
 "domain_name": "huawei.com",
  "domain_email": null,
  "record_name": "_dnsauth. huawei.com",
  "record_value": "202305150000002aurxma1tun2fgzz0jbs9h5lsekf8gloq57mbs78m9jist465m",
  "record_type": "TXT",
  "domain_method": "DNS",
  "applicant_email": "huawei@huawei.com",
  "auto_dns_auth": true
}
```

## Status Code

**Table 6-26** lists the normal status code returned by the API.

**Table 6-26** Status code

| Status Code | Code | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |

For details about error codes, see **Error Codes**

# 7 Permissions and Supported Actions

## 7.1 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 roles and policies 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 of the permissions required to call all APIs, but IAM users must have the required permissions specifically assigned. 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:

- **SSL Certificate Manager (SCM)**
- **Private Certificate Authority (PCA)**

# 7.2 SSL Certificate Manager (SCM)

## Authorization information of APIs (v3)

| Permission | API | Action | Dependent Permission | IAM Project (Project) | Enterprise Project (Enterprise Project) |
|---|---|---|---|---|---|
| Querying the certificate list | GET /v3/scm/certificates | scm:cert:list | - | √ | x |
| Obtaining details of a certificate | GET /v3/scm/certificates/{certificate_id} | scm:cert:get | - | √ | x |
| Deleting a certificate | DELETE /v3/scm/certificates/{certificate_id} | scm:cert:delete | - | √ | x |

| Permission | API | Action | Dependent Permission | IAM Project<br>(Project) | Enterprise Project<br>(Enterprise Project) |
|---|---|---|---|---|---|
| Pushing a certificate | POST /v3/scm/certificates/{certificate_id}/push | scm:cert:push | The following action needs to be added when a certificate is to be pushed to CDN:<br>cdn:configuration:queryHttpsConf | √ | x |
| Importing a certificate | POST /v3/scm/certificates/import | scm:cert:upload | - | √ | x |
| Exporting a certificate | POST /v3/scm/certificates/{certificate_id}/export | scm:cert:download | - | √ | x |

## Authorization information of APIs (v2)

| Permission | API | Action | Dependent Permission | IAM Project (Project) | Enterprise Project (Enterprise Project) |
|---|---|---|---|---|---|
| Querying the certificate list | GET /v2/{project_id}/scm/certlist | scm:cert:list | - | √ | x |
| Querying the certificate details | GET /v2/{project_id}/scm/cert/{cert_id} | scm:cert:get | - | √ | x |
| Querying the certificate type | GET /v2/{project_id}/scm/cert/product | scm:certType:get | - | √ | x |
| Querying the certificate details | GET /v2/{project_id}/scm/product/{product_id} | scm:certProduct:get | - | √ | x |
| Modifying a certificate | PUT /v2/{project_id}/scm/cert/{cert_id} | scm:cert:edit | - | √ | x |
| Deleting a certificate | DELETE /v2/{project_id}/scm/cert/{cert_id} | scm:cert:delete | - | √ | x |

| Permission | API | Action | Dependent Permission | IAM Project (Project) | Enterprise Project (Enterprise Project) |
|---|---|---|---|---|---|
| Pushing a certificate | POST /v2/{project_id}/scm/cert/{cert_id}/push | scm:cert:push | The following action needs to be added when a certificate is to be pushed to CDN:<br>cdn:configuration:queryHttpsConf | √ | x |
| Querying push records | GET /v2/{project_id}/scm/cert/{cert_id}/push-history | scm:pushHistory:list | - | √ | x |
| Uploading a certificate | POST /v2/{project_id}/scm/cert/upload | scm:cert:upload | - | √ | x |

# 7.3 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 |

| Permission | API | Action |
|---|---|---|
| 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 |
| 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 |

| Permission | API | Action |
|---|---|---|
| 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 |
| 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 Code to SCM APIs

| Status Code | Status | Description |
|---|---|---|
| 200 | OK | Request processed successfully. |
| 202 | Accept | The job was successfully delivered. However, it will be postponed because the system is busy currently. |
| 204 | No Content | The request is processed successfully and no content is returned. |
| 300 | multiple choices | The requested resource has multiple available responses. |
| 400 | Bad Request | The request parameter is incorrect. |
| 401 | Unauthorized | A username and password are required. |
| 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. |
| 405 | Method Not Allowed | The method specified in the request is not allowed. |
| 406 | Not Acceptable | The response generated by the server cannot be accepted by the client. |
| 407 | Proxy Authentication Required | You must use the proxy server for authentication. Then, the request can be processed. |

| Status Code | Status | Description |
|---|---|---|
| 408 | Request Timeout | The request timed out. |
| 409 | Conflict | The request cannot be processed due to a conflict. |
| 500 | Internal Server Error | Internal service error. |
| 501 | Not Implemented | Failed to complete the request. The server does not support the requested function. |
| 502 | Bad Gateway | Failed to complete the request, because the server receives an invalid request. |
| 503 | Service Unavailable | Failed to complete the request because the system is temporarily abnormal. |
| 504 | Gateway Timeout | A gateway timeout error occurs. |

### 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.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. |
| 400 | SCM.0085 | Required param phone is null or empty. | Required param phone is null or empty. | Please enter nonNull filed. |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 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. |
| 400 | SCM.0201 | Failed to push to ELB. | Failed to push to ELB. Eerror message returned. | Contact the customer service. |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 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. Eerror 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. |
| 400 | SCM.0306 | Tag key is invalid. | Tag key is invalid. | Please enter valid tag key. |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 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.0403 | Encrypt cert is not sm2 signature algorithm. | Encrypt cert is not sm2 signature algorithm. | Please input valid cert. |
| 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. |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 400 | SCM.0502 | The certificate ID list cannot be empty. | The certificate ID list cannot be empty. | Please enter nonNull certificate ID list. |
| 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. |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 401 | SCM.1009 | Your account is restricted. | The account is restricted | Contact the administrator for unfreezing. |
| 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. |
| 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-xxxxxxxxxxxx format. | Invalid CA ID. Valid CA IDs use a hexadecimal xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx 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-xxxxxxxxxxxx format. | Invalid certificate ID. Valid certificate IDs use a hexadecimal xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx 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:<br>1. The format should be correct. When requesting through API, you need to use " " or "\r " instead of line feed;<br>2. The certificate chain should be complete. Some intermediate CA certificates cannot be missing. The order is: intermediate CA >... > Root ca. |
| 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. |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 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:<br>1. Check whether the token is obtained according to the interface provided by the Identity and Access Management(IAM);<br>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. |
| 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. |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 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:<br>1. Disable CA: CA status must be in "ACTIVED" or "EXPIRED" status;<br>2. Enable CA: CA status must be in "DISABLED" status;<br>3. Delete CA: CA status must be in "PENDING" or "DISABLED" status;<br>4. Restore CA: CA status needs to be in "DELETED" status;<br>5. Export the CSR of the CA: the CA status needs to be in the "PENDING" state;<br>6. Export CA certificate: CA status needs to be in "ACTIVED" or "EXPIRED" status;<br>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;<br>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.00030202 | CA or certificate frozen. Contact administrator. | CA or certificate frozen. Contact administrator. | Please contact technical support. |
| 403 | PCA.00030301 | 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.00030102 | CA or certificate is not found. | CA or certificate is not found. | Please confirm that the CA or certificate already exists. |

| Status Code | Error Codes | Error Message | Description | Solution |
|---|---|---|---|---|
| 404 | PCA.00030103 | 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". |
| 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

## Obtaining a Project ID by Calling an API

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

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

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

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

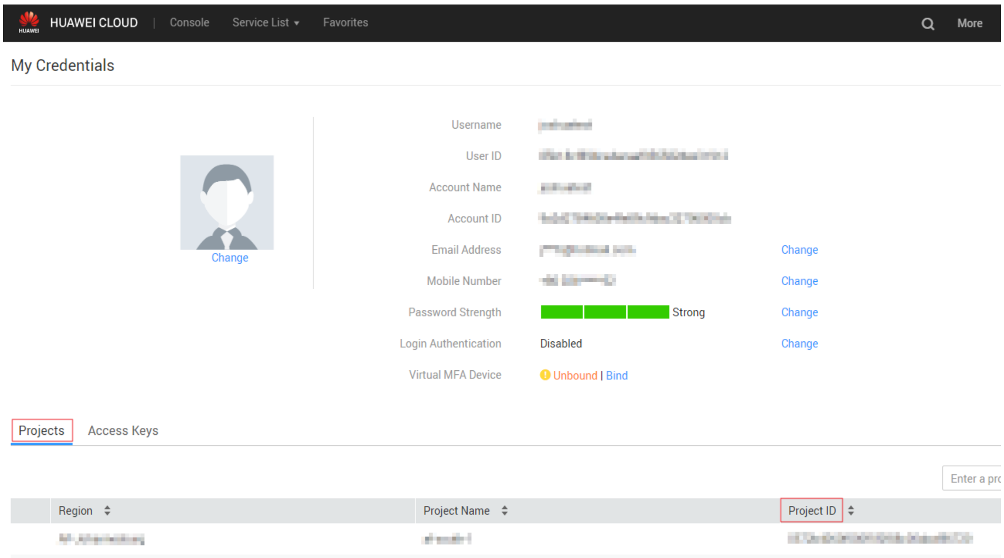
## Obtaining a Project ID from the Console

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

1. Log in to the management console.
2. Click the username and choose **Basic Information** from the drop-down list.
3. On the **Account Info** page, click **Manage** next to **Security Credentials**.

   On the **My Credentials** page, view project IDs in the project list.

**Figure A-1** Viewing project IDs



My Credentials

Username [redacted]
User ID [redacted]
Account Name [redacted]
Account ID [redacted]
Email Address [redacted] Change
Mobile Number [redacted] Change
Password Strength Strong Change
Login Authentication Disabled Change
Virtual MFA Device Unbound | Bind

| Region | Project Name | Project ID |
|---|---|---|
| [redacted] | [redacted] | [redacted] |

# B Change History

| Released On | Description |
|---|---|
| 2023-05-16 | This issue is the third official release.<br>Added **Querying Domain Name Verification Information**. |
| 2022-08-24 | This issue is the second official release.<br>Updated the error codes for private certificates. |
| 2022-03-24 | This issue is the first official release. |