Cloud Certificate Manager

API Reference

Issue	01
Date	2022-12-15

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

Cloud Certificate Manager (CCM) is a private CA and certificate management platform. You can use CCM to set up a complete CA hierarchy and use it to issue and manage private certificates for your organization. It is used to authenticate application identities and encrypt and decrypt data within your organization.

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. Endpoints vary depending on services and regions. For the endpoints of all services, see **Regions and Endpoints**.

1.4 Concepts

- Account

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

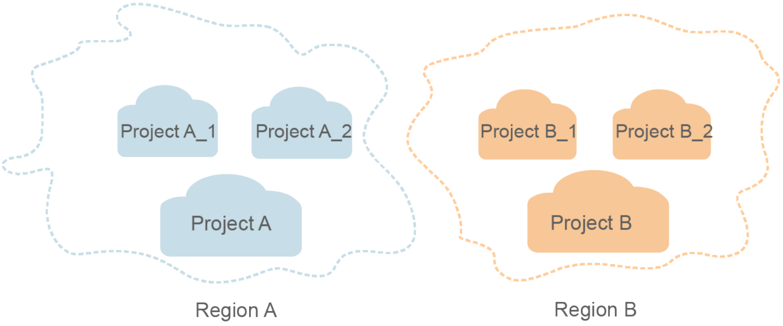
- Availability Zone (AZ)

  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.

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 the **ae-ad-1** region is **iam.ae-ad-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**:

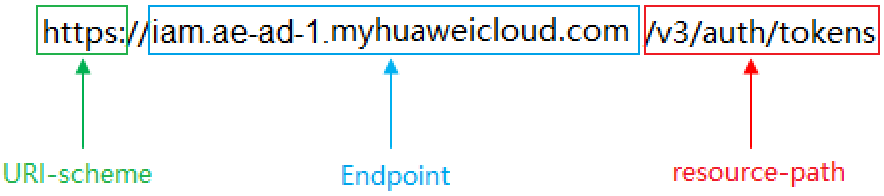
  Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of "Parameter name=Parameter value". For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in the **ae-ad-1** region, obtain the endpoint of IAM (**iam.ae-ad-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.ae-ad-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.ae-ad-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.ae-ad-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**.

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.ae-ad-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.ae-ad-1.myhuaweicloud.com/v3/auth/tokens
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**.

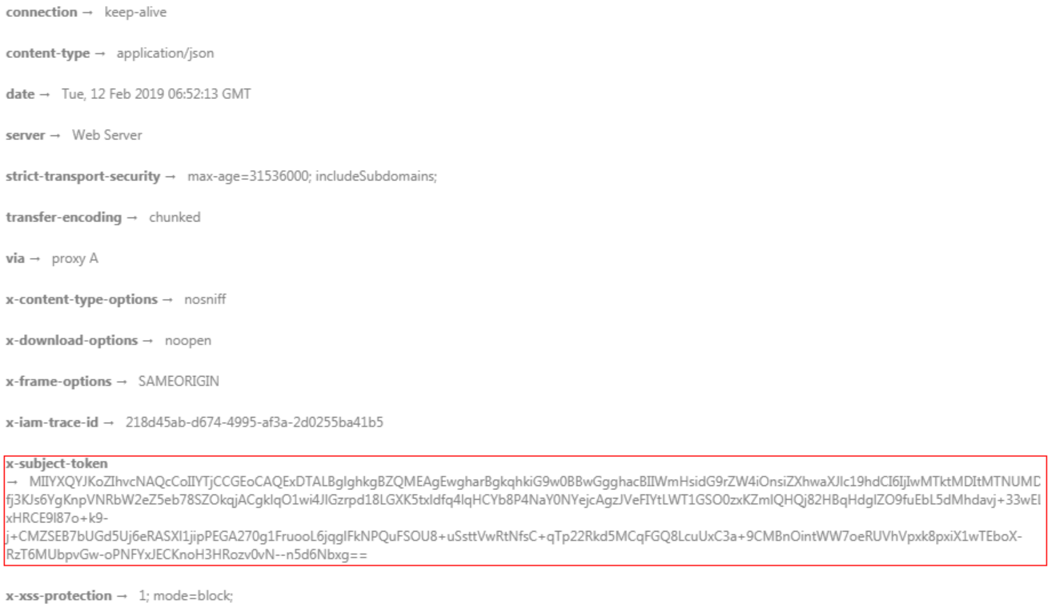
For example, if status code **201** is returned for calling the API used to **obtain a user token**, the request is successful.

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
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkqjACgklqO1wi4JIGzrpd18LGXK5txldfq4lqHCYb8P4NaY0NYejcAgzJVeFIYtLWT1GSO0zxKZmIQHQj82HBqHdglZO9fuEbL5dMhdavj+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.

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 Private Certificates

4.1.1 Private CA Management

4.1.1.1 Querying the CA List

Function

This API is used to query the CA list.

URI

GET /v1/private-certificate-authorities

Table 4-1 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	The number of returned records. The default value is **10**. Minimum: **0** Maximum: **1000**
name	No	String	The CA certificate name (**CN**) filter. This parameter is used to obtain the set of CA certificates whose names contain a specific value. Minimum: **1** Maximum: **64**

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**. Minimum: **0**
status	No	String	The CA certificate status. You can search CA certificates by status. ● **PENDING**: The CA certificate is to be activated. A CA certificate in this status cannot issue certificates. ● **ACTIVED**: The CA certificate is activated. A CA certificate in this status can issue certificates. ● **DISABLED**: The CA certificate is disabled. A CA certificate in this status cannot issue certificates. ● **DELETED**: The CA certificate is to be deleted as scheduled. A CA certificate in this status cannot issue certificates. ● **EXPIRED**: The CA certificate has expired. A CA certificate in this status cannot issue certificates.
type	No	String	CA certificate types: ● **ROOT**: a root CA certificate ● **SUBORDINATE**: a subordinate CA certificate

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

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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-3 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 4-4 CertificateAuthorities

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

Parameter	Type	Description
signature_algorithm	String	Signature hash algorithm
freeze_flag	Integer	Freezing tag: ● **0**: The certificate is not frozen. ● **Other values**: The certificate is frozen (The type of value is reserved).
gen_mode	String	Certificate generation method. ● **GENERATE**: The certificate is generated through the PCA system. ● **IMPORT**: The certificate is imported externally. ● **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 Minimum: **1** Maximum: **64**
create_time	Long	Time the certificate was created. The value is a timestamp in milliseconds.
delete_time	Long	Time the certificate was deleted. The value is a timestamp in milliseconds.
not_before	Long	Time the certificate was created. The value is a timestamp in milliseconds.
not_after	Long	Time the certificate expires. The value is a timestamp in milliseconds.
distinguished_name	**DistinguishedName** object	Certificate name. For details, see data structure for the **DistinguishedName** field.
crl_configuration	**ListCrlConfiguration** object	Certificate CRL. For details, see data structure for the **ListCrlConfiguration** field.

Table 4-5 DistinguishedName

Parameter	Type	Description
common_name	String	Common certificate name (CN). Minimum: **1** Maximum: **64**

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

Table 4-6 ListCrlConfiguration

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

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

Status code: 400

Table 4-7 Response body parameters

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

Status code: 401

Table 4-8 Response body parameters

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

Status code: 403

Table 4-9 Response body parameters

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

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

Status code: 404

Table 4-10 Response body parameters

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

Status code: 500

Table 4-11 Response body parameters

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

Example Requests

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

```
GET https://ccm.ae-ad-1.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" : "your country abbreviation",
      "state" : "your state",
      "locality" : "your locality",
      "organization" : "your organization",
      "organizational_unit" : "your unit",
      "common_name" : "your CN"
    },
    "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" : "your country abbreviation",
      "state" : "your state",
      "locality" : "your locality",
      "organization" : "your organization",
      "organizational_unit" : "your unit",
      "common_name" : "your CN"
    },
    "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**.

4.1.1.2 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 4-12 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-Auth-Token** in the response header is the user token.

Table 4-13 Request body parameters

Parameter	Mandatory	Type	Description
type	Yes	String	Type of the CA you want to create: - **ROOT**: a root CA - **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: ● **RSA2048**: RSA algorithm with the key length of 2048 bits ● **RSA4096**: RSA algorithm with the key length of 4096 bits ● **EC256**: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 256 bits ● **EC384**: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 384 bits
validity	No	**Validity** object	Validity period of a certificate. The options are as follows: ● If you want to create a root CA, this parameter is mandatory. ● If you want to create a subordinate CA and activate it, this parameter is mandatory. ● If you want to create a subordinate CA but not activate it immediately, this parameter is not required. You can specify this parameter when activating the subordinate CA. **NOTE** 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: ● 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. ● If you want to create a subordinate CA and activate it, this parameter is mandatory. ● If you want to create a subordinate CA but not activate it immediately, this parameter is not required. You can specify this parameter when activating the subordinate CA. Minimum: **36** Maximum: **36**

Parameter	Mandatory	Type	Description
path_length	No	Integer	Length of the CA certificate path. The options are as follows: ● If you want to create a root CA, this parameter is not required by default. This means CA path length is not limited and you can expand the CA hierarchies. To limit the CA hierarchies, you can specify this parameter when creating a subordinate CA. ● If you want to create a subordinate CA and activate it, specify this parameter based on your need. Default value: **0** ● 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. Minimum: **0** Maximum: **6**

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

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

Table 4-14 DistinguishedName

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

Table 4-15 Validity

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

Table 4-16 CrlConfiguration

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

Parameter	Mandatory	Type	Description
obs_bucket_name	No	String	OBS bucket name. **NOTE** To enable the CRL release function: ● 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. ● The specified OBS bucket must exist. Otherwise, an error will be reported.
valid_days	No	Integer	CRL update interval, in days. This parameter is mandatory when the CRL release function is enabled. Minimum: **7** Maximum: **30**

Response Parameters

Status code: 200

Table 4-17 Response body parameters

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

Status code: 400

Table 4-18 Response body parameters

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

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

Status code: 401

Table 4-19 Response body parameters

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

Status code: 403

Table 4-20 Response body parameters

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

Status code: 404

Table 4-21 Response body parameters

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

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

Status code: 500

Table 4-22 Response body parameters

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

Example Requests

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

```
POST https://ccm.ae-ad-1.myhuaweicloud.com/v1/private-certificate-authorities

{
  "type" : "ROOT",
  "key_algorithm" : "RSA4096",
  "signature_algorithm" : "SHA512",
  "distinguished_name" : {
    "country" : "your country abbreviation",
    "state" : "your state",
    "locality" : "your locality",
    "organization" : "your organization",
    "organizational_unit" : "your unit",
    "common_name" : "your CN"
  },
  "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**.

4.1.1.3 Querying the CA Quota

Function

This API is used to query the CA quota.

URI

GET /v1/private-certificate-authorities/quotas

Request Parameters

Table 4-23 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-24 Response body parameters

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

Table 4-25 Quotas

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

Table 4-26 Resources

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

Status code: 400

Table 4-27 Response body parameters

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

Status code: 401

Table 4-28 Response body parameters

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

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

Status code: 403

Table 4-29 Response body parameters

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

Status code: 404

Table 4-30 Response body parameters

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

Status code: 500

Table 4-31 Response body parameters

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

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

Example Requests

When you 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.ae-ad-1.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**.

4.1.1.4 Querying CA Details

Function

This API is used to query details about a CA.

URI

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

Table 4-32 Path Parameters

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

Request Parameters

Table 4-33 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-34 Response body parameters

Parameter	Type	Description
ca_id	String	ID of the CA certificate Minimum: **36** Maximum: **36**
type	String	The CA type can be: ● **ROOT**: a root CA ● **SUBORDINATE**: a subordinate CA
status	String	CA certificate status: ● **PENDING**: The CA certificate is to be activated. A CA certificate in this status cannot issue certificates. ● **ACTIVED**: The CA certificate is activated. A CA certificate in this status can issue certificates. ● **DISABLED**: The CA certificate is disabled. A CA certificate in this status cannot issue certificates. ● **DELETED**: The CA certificate is to be deleted as scheduled. A CA certificate in this status cannot issue certificates. ● **EXPIRED**: The CA certificate has expired. A CA certificate in this status cannot issue certificates.

Parameter	Type	Description
path_length	Integer	CA path length. **NOTE** Note: The path length of the generated root CA certificate is not limited, but this field is set to **7** in the database. The path length of a subordinate CA is specified by you when you create the subordinate CA. The default value is **0**. Minimum: **0** Maximum: **6**
issuer_id	String	The ID of the CA certificate that issues the certificate. For a root CA, the value of this parameter is **null**. Minimum: **36** Maximum: **36**
issuer_name	String	The name of the parent CA certificate. For a root CA, the value of this parameter is **null**. Minimum: **1** Maximum: **64**
key_algorithm	String	Key algorithm
signature_algorithm	String	Signature hash algorithm
freeze_flag	Integer	Freezing tag: ● **0**: The certificate is not frozen. ● **Other values**: The certificate is frozen (The type of value is reserved).
gen_mode	String	Certificate generation method. ● **GENERATE**: The certificate is generated through the PCA system. ● **IMPORT**: The certificate is imported externally. ● **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 Minimum: **1** Maximum: **64**
create_time	Long	Time the certificate was created. The value is a timestamp in milliseconds.
delete_time	Long	Time the certificate was deleted. The value is a timestamp in milliseconds.

Parameter	Type	Description
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 4-35 DistinguishedName

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

Table 4-36 ListCrlConfiguration

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

Status code: 400

Table 4-37 Response body parameters

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

Status code: 401

Table 4-38 Response body parameters

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

Status code: 403

Table 4-39 Response body parameters

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

Status code: 404

Table 4-40 Response body parameters

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

Status code: 500

Table 4-41 Response body parameters

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

Example Requests

When you use this API to query 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.ae-ad-1.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" : "your IT Root CA",
  "not_after" : 1647567892000,
  "not_before" : 1645148632000,
  "status" : "ACTIVED",
  "freeze_flag" : 0,
  "gen_mode" : "CSR",
  "serial_number" : "202202180143522338893611",
  "distinguished_name" : {
    "country" : "your country abbreviation",
    "state" : "your state",
    "locality" : "your locality",
    "organization" : "your organization",
    "organizational_unit" : "your unit",
    "common_name" : "your CN"
  },
  "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**.

4.1.1.5 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 4-42 Path Parameters

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

Table 4-43 Query Parameters

Parameter	Mandatory	Type	Description
pending_days	Yes	String	Delayed deletion time, in days Minimum: **7** Maximum: **30**

Request Parameters

Table 4-44 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 400

Table 4-45 Response body parameters

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

Status code: 401

Table 4-46 Response body parameters

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

Status code: 403

Table 4-47 Response body parameters

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

Status code: 404

Table 4-48 Response body parameters

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

Status code: 500

Table 4-49 Response body parameters

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

Example Requests

When you use this API to 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.ae-ad-1.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**.

4.1.1.6 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 4-50 Path Parameters

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

Request Parameters

Table 4-51 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-Auth-Token** in the response header is the user token.

Table 4-52 Request body parameters

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

Table 4-53 Validity

Parameter	Mandatory	Type	Description
type	Yes	String	Validity period type, which is mandatory. The options are as follows: ● **YEAR**: Year (12 months) ● **MONTH**: Month (31 days) ● **DAY**: Day ● **HOUR**: Hour
value	Yes	Integer	The certificate validity period. The value of this parameter varies depending on the value of **type**: ● Root CA certificates: no longer than 30 years ● Subordinate CA or private certificates: no longer than 20 years
start_from	No	Integer	Start time. The options are as follows: ● The value is a timestamp in milliseconds. For example, 1645146939688 indicates 2022-02-18 09:15:39. ● 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 4-54 Response body parameters

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

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

Status code: 401

Table 4-55 Response body parameters

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

Status code: 403

Table 4-56 Response body parameters

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

Status code: 404

Table 4-57 Response body parameters

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

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

Status code: 500

Table 4-58 Response body parameters

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

Example Requests

When you use this API to 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.ae-ad-1.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**.

4.1.1.7 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 4-59 Path Parameters

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

Request Parameters

Table 4-60 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-61 Response body parameters

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

Status code: 400

Table 4-62 Response body parameters

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

Status code: 401

Table 4-63 Response body parameters

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

Status code: 403

Table 4-64 Response body parameters

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

Status code: 404

Table 4-65 Response body parameters

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

Status code: 500

Table 4-66 Response body parameters

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

Example Requests

When you use this API to 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.ae-ad-1.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**.

4.1.1.8 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 4-67 Path Parameters

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

Request Parameters

Table 4-68 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 400

Table 4-69 Response body parameters

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

Status code: 401

Table 4-70 Response body parameters

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

Status code: 403

Table 4-71 Response body parameters

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

Status code: 404

Table 4-72 Response body parameters

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

Status code: 500

Table 4-73 Response body parameters

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

Example Requests

When you use this API to 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.ae-ad-1.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**.

4.1.1.9 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 4-74 Path Parameters

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

Request Parameters

Table 4-75 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 400

Table 4-76 Response body parameters

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

Status code: 401

Table 4-77 Response body parameters

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

Status code: 403

Table 4-78 Response body parameters

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

Status code: 404

Table 4-79 Response body parameters

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

Status code: 500

Table 4-80 Response body parameters

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

Example Requests

When you use this API to 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.ae-ad-1.myhuaweicloud.com/v1/private-certificate-authorities/4c0e772e-a30c-4029-b929-b7acb04143f7/enable
```

Example Responses

Status code: 400

Invalid request parameters.

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

Status code: 401

Token required for the requested page.

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

Status code: 403

Authentication failed.

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

Status code: 404

No resources available or found.

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

Status code: 500

Internal service error.

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

Status Codes

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

Error Codes

See **Error Codes**.

4.1.1.10 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 4-81 Path Parameters

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

Request Parameters

Table 4-82 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-83 Response body parameters

Parameter	Type	Description
certificate	String	Certificate content. **NOTE** ● If you use an API to obtain the certificate, the newline characters in it have been replaced with **\r\n**. ● If you export the certificate from the console, the certificate is in PEM format. Minimum: **1** Maximum: **4096**
certificate_chain	String	The content of the certificate chain. The sequence of the certificate chain (from top to bottom) is as follows: intermediate certificate >... > root certificate. **NOTE** ● If you use an API to obtain the certificate chain, the newline characters in it have been replaced with **\r\n**. ● If you export the certificate chain from the console, the certificate chain is in PEM format. Minimum: **1** Maximum: **2097152**

Status code: 400

Table 4-84 Response body parameters

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

Status code: 401

Table 4-85 Response body parameters

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

Status code: 403

Table 4-86 Response body parameters

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

Status code: 404

Table 4-87 Response body parameters

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

Status code: 500

Table 4-88 Response body parameters

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

Example Requests

When you use this API to 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.ae-ad-1.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.
404	No resources available or found.
500	Internal service error.

Error Codes

See **Error Codes**.

4.1.1.11 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 4-89 Path Parameters

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

Request Parameters

Table 4-90 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-Auth-Token** in the response header is the user token.

Table 4-91 Request body parameters

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

Response Parameters

Status code: 400

Table 4-92 Response body parameters

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

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

Status code: 401

Table 4-93 Response body parameters

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

Status code: 403

Table 4-94 Response body parameters

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

Status code: 404

Table 4-95 Response body parameters

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

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

Status code: 500

Table 4-96 Response body parameters

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

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.ae-ad-1.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**.

4.1.1.12 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 4-97 Path Parameters

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

Request Parameters

Table 4-98 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 400

Table 4-99 Response body parameters

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

Status code: 401

Table 4-100 Response body parameters

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

Status code: 403

Table 4-101 Response body parameters

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

Status code: 404

Table 4-102 Response body parameters

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

Status code: 500

Table 4-103 Response body parameters

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

Example Requests

When you use this API to 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.ae-ad-1.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**.

4.1.1.13 Revoking a subordinate CA

Function

This API is used to revoke a subordinate CA

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-certificate-authorities/{ca_id}/revoke

Table 4-104 Path Parameters

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

Request Parameters

Table 4-105 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-Auth-Token** in the response header is the user token.

Table 4-106 Request body parameters

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

Response Parameters

Status code: 400

Table 4-107 Response body parameters

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

Status code: 401

Table 4-108 Response body parameters

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

Status code: 403

Table 4-109 Response body parameters

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

Status code: 404

Table 4-110 Response body parameters

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

Status code: 500

Table 4-111 Response body parameters

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

Example Requests

When you use this API to 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.ae-ad-1.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**.

4.1.2 Private Certificate Management

4.1.2.1 Querying the List of Private Certificates

Function

This API is used to query the private certificate list.

URI

GET /v1/private-certificates

Table 4-112 Query Parameters

Parameter	Mandatory	Type	Description
limit	No	Integer	The number of returned records. The default value is **10**. Minimum: **0** Maximum: **1000**
name	No	String	The name of the private certificate. The set of certificates whose names contain the name field is returned. Minimum: **1** Maximum: **64**
offset	No	Integer	Index position. The query starts from the next data record indexed by this parameter. Minimum: **0**
status	No	String	The private certificate status. You can query private certificates by status. ● **ISSUED**: The certificate is issued. ● **REVOKED**: The certificate is revoked. ● **EXPIRED**: The certificate expired.

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

Request Parameters

Table 4-113 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-114 Response body parameters

Parameter	Type	Description
total	Integer	Total number of private certificates. Minimum: **0** Maximum: **1000000**

Parameter	Type	Description
certificates	Array of **Certificates** objects	For details, see data structure for the **Certificates** field.

Table 4-115 Certificates

Parameter	Type	Description
certificate_id	String	ID of the private certificate Minimum: **36** Maximum: **36**
status	String	Certificate status: ● **ISSUED**: The certificate is issued. ● **EXPIRED**: The certificate expired. ● **REVOKED**: The certificate is revoked.
issuer_id	String	ID of the parent CA. Minimum: **36** Maximum: **36**
issuer_name	String	The name of the parent CA certificate. Minimum: **1** Maximum: **64**
key_algorithm	String	Key algorithm
signature_algorithm	String	Signature algorithm
freeze_flag	Integer	Freezing tag: ● **0**: The certificate is not frozen. ● **Other values**: The certificate is frozen (The type of value is reserved).
gen_mode	String	Certificate generation method. ● **GENERATE**: The certificate is generated through the PCA system. ● **IMPORT**: The certificate is imported externally. ● **CSR**: The CSR is imported externally and issued by the internal CA. The private key is not managed in PCA.

Parameter	Type	Description
serial_number	String	Serial number. Minimum: **1** Maximum: **64**
create_time	Long	Time the certificate was created. The value is a timestamp in milliseconds.
delete_time	Long	Time the certificate was deleted. The value is a timestamp in milliseconds.
not_before	Long	Time the certificate was created. The value is a timestamp in milliseconds.
not_after	Long	Time the certificate expires. The value is a timestamp in milliseconds.
distinguished_name	**DistinguishedName** object	Certificate name. For details, see data structure for the **DistinguishedName** field.

Table 4-116 DistinguishedName

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

Parameter	Type	Description
organizational_unit	String	Organization Unit (OU). Minimum: **1** Maximum: **64**

Status code: 400

Table 4-117 Response body parameters

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

Status code: 401

Table 4-118 Response body parameters

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

Status code: 403

Table 4-119 Response body parameters

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

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

Status code: 404

Table 4-120 Response body parameters

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

Status code: 500

Table 4-121 Response body parameters

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

Example Requests

When you use this API to query the 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.ae-ad-1.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" : "your country abbreviation",
      "state" : "your state",
      "locality" : "your locality",
      "organization" : "your organization",
      "organizational_unit" : "your unit",
      "common_name" : "your CN"
    },
    "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" : "your country abbreviation",
      "state" : "your state",
      "locality" : "your locality",
      "organization" : "your organization",
      "organizational_unit" : "your unit",
      "common_name" : "your CN"
    },
    "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.
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**.

4.1.2.2 Applying for a Certificate

Function

This API is used to apply for a certificate.

URI

POST /v1/private-certificates

Request Parameters

Table 4-122 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-Auth-Token** in the response header is the user token.

Table 4-123 Request body parameters

Parameter	Mandatory	Type	Description
issuer_id	Yes	String	ID of the parent CA. Minimum: **36** Maximum: **36**
key_algorithm	Yes	String	Key algorithm. The options are as follows: • **RSA2048**: RSA algorithm with the key length of 2048 bits • **RSA4096**: RSA algorithm with the key length of 4096 bits • **EC256**: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 256 bits • **EC384**: Elliptic Curve Digital Signature Algorithm (ECDSA) with the key length of 384 bits
signature_algorithm	Yes	String	Signature hash algorithm. The options are as follows: • **SHA256** • **SHA384** • **SHA512**
distinguished_name	Yes	**CertDistinguishedName** object	Certificate name. For details, see data structure for the **CertDistinguishedName** field.

Parameter	Mandatory	Type	Description
validity	Yes	**Validity** object	Certificate validity. For details, see data structure for the **Validity** field.
key_usages	No	Array of strings	Key usage. For details, see **4.2.1.3** in RFC 5280. ● **digitalSignature**: The key is used as a digital signature. ● **nonRepudiation**: The key can be used for non-repudiation. ● **keyEncipherment**: The key can be used for key encryption. ● **dataEncipherment**: The key can be used for data encryption. ● **keyAgreement**: The key can be used for key negotiation. ● **keyCertSign**: The key can issue a certificate. ● **cRLSign**: The key can issue a certificate revocation list (CRL). ● **encipherOnly**: The key is used only for encryption. ● **decipherOnly**: The key is used only for decryption.
subject_alternative_names	No	Array of **SubjectAlternativeName** objects	Alternative name for the subject. For details, see data structure for the **SubjectAlternativeName** field. ● 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 4-124 CertDistinguishedName

Parameter	Mandatory	Type	Description
common_name	Yes	String	Common certificate name (CN). Minimum: **1** 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. Minimum: **2** Maximum: **2**
state	No	String	State or city name.If not passed in, the value corresponding to the parent CA is inherited by default. Minimum: **1** Maximum: **128**
locality	No	String	Country/Region.If not passed in, the value corresponding to the parent CA is inherited by default. Minimum: **1** Maximum: **128**
organization	No	String	Organization name.If not passed in, the value corresponding to the parent CA is inherited by default. Minimum: **1** Maximum: **64**
organizational_unit	No	String	Organization Unit (OU).If not passed in, the value corresponding to the parent CA is inherited by default. Minimum: **1** Maximum: **64**

Table 4-125 Validity

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

Table 4-126 SubjectAlternativeName

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

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

Table 4-127 ExtendedKeyUsage

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

Parameter	Mandatory	Type	Description
email_protection	No	Boolean	Email protection. The OID is 1.3.6.1.5.5.7.3.4. ● **true** ● **false** **NOTE** The default value is false. Default: **false**
time_stamping	No	Boolean	Binding the hash of an object to a time. The OID is 1.3.6.1.5.5.7.3.8 ● **true** ● **false** **NOTE** The default value is false. Default: **false**

Table 4-128 CustomizedExtension

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

Response Parameters

Status code: 200

Table 4-129 Response body parameters

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

Status code: 400

Table 4-130 Response body parameters

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

Status code: 401

Table 4-131 Response body parameters

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

Status code: 403

Table 4-132 Response body parameters

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

Status code: 404

Table 4-133 Response body parameters

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

Status code: 500

Table 4-134 Response body parameters

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

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.ae-ad-1.myhuaweicloud.com/v1/private-certificates

{
  "key_algorithm" : "RSA2048",
  "distinguished_name" : {
    "country" : "your country abbreviation",
    "state" : "your state",
    "locality" : "your locality",
    "organization" : "your organization",
    "organizational_unit" : "your unit",
    "common_name" : "your CN"
  },
  "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" ],
  "customized_extension" : {
    "object_identifier" : "1.3.6.1.4.1.2011.4.1",
    "value" : "This is custom extensions."
  }
}
```

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**.

4.1.2.3 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 4-135 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-Auth-Token** in the response header is the user token.

Table 4-136 Request body parameters

Parameter	Mandatory	Type	Description
issuer_id	Yes	String	ID of the parent CA. Minimum: **36** 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. Maximum: **5120**
validity	Yes	**Validity** object	Certificate validity. For details, see data structure for the **Validity** field.
type	No	String	Certificate type. This parameter is used to distinguish subordinate CA certificates from private certificates. ● **ENTITY_CERT**: A private certificate is issued. It is the default value. ● **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. Minimum: **0** Maximum: **6**
subject_alternative_names	No	Array of **SubjectAlternativeName** objects	The alternative name for the subject (This parameter is reserved and ignored at the backend). For details, see data structure for the **SubjectAlternativeName** field.

Table 4-137 Validity

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

Table 4-138 SubjectAlternativeName

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

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

Response Parameters

Status code: 200

Table 4-139 Response body parameters

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

Status code: 400

Table 4-140 Response body parameters

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

Status code: 401

Table 4-141 Response body parameters

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

Status code: 403

Table 4-142 Response body parameters

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

Status code: 404

Table 4-143 Response body parameters

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

Status code: 500

Table 4-144 Response body parameters

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

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.ae-ad-1.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**.

4.1.2.4 Parsing a CSR

Function

This API is used to parse a CSR.

URI

POST /v1/private-certificates/csr/parse

Request Parameters

Table 4-145 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-Auth-Token** in the response header is the user token.

Table 4-146 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. Maximum: **5120**

Response Parameters

Status code: 200

Table 4-147 Response body parameters

Parameter	Type	Description
key_algorithm	String	Key algorithm.
key_algorithm_length	String	Length of the key algorithm, in bits.

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

Table 4-148 DistinguishedName

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

Status code: 400

Table 4-149 Response body parameters

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

Status code: 401

Table 4-150 Response body parameters

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

Status code: 403

Table 4-151 Response body parameters

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

Status code: 404

Table 4-152 Response body parameters

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

Status code: 500

Table 4-153 Response body parameters

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

Example Requests

When you 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.ae-ad-1.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" : "your country abbreviation",
    "state" : "your state",
    "locality" : "your locality",
    "organization" : "your organization",
    "organizational_unit" : "your unit",
    "common_name" : "your CN"
  },
  "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**.

4.1.2.5 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 4-154 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-155 Response body parameters

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

Table 4-156 Quotas

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

Table 4-157 Resources

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

Status code: 400

Table 4-158 Response body parameters

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

Status code: 401

Table 4-159 Response body parameters

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

Status code: 403

Table 4-160 Response body parameters

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

Status code: 404

Table 4-161 Response body parameters

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

Status code: 500

Table 4-162 Response body parameters

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

Example Requests

When you use this API to query the 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.ae-ad-1.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**.

4.1.2.6 Querying Certificate Details

Function

This API is used to query details about a certificate.

URI

GET /v1/private-certificates/{certificate_id}

Table 4-163 Path Parameters

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

Request Parameters

Table 4-164 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-165 Response body parameters

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

Parameter	Type	Description
signature_algorithm	String	Signature algorithm
freeze_flag	Integer	Freezing tag: - **0**: The certificate is not frozen. - **Other values**: The certificate is frozen (The type of value is reserved).
gen_mode	String	Certificate generation method. - **GENERATE**: The certificate is generated through the PCA system. - **IMPORT**: The certificate is imported externally. - **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. Minimum: **1** Maximum: **64**
create_time	Long	Time the certificate was created. The value is a timestamp in milliseconds.
delete_time	Long	Time the certificate was deleted. The value is a timestamp in milliseconds.
not_before	Long	Time the certificate was created. The value is a timestamp in milliseconds.
not_after	Long	Time the certificate expires. The value is a timestamp in milliseconds.
distinguished_name	**DistinguishedName** object	Certificate name. For details, see data structure for the **DistinguishedName** field.

Table 4-166 DistinguishedName

Parameter	Type	Description
common_name	String	Common certificate name (CN). Minimum: **1** Maximum: **64**

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

Status code: 400

Table 4-167 Response body parameters

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

Status code: 401

Table 4-168 Response body parameters

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

Status code: 403

Table 4-169 Response body parameters

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

Status code: 404

Table 4-170 Response body parameters

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

Status code: 500

Table 4-171 Response body parameters

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

Example Requests

When you use this API to query 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.ae-ad-1.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" : "your CA name",
  "not_after" : 1665539214000,
  "not_before" : 1634295475000,
  "status" : "ISSUED",
  "freeze_flag" : 0,
  "gen_mode" : "GENERATE",
  "serial_number" : "20211015105754126608186l",
  "distinguished_name" : {
    "country" : "your country abbreviation",
    "state" : "your state",
    "locality" : "your locality",
    "organization" : "your organization",
    "organizational_unit" : "your unit",
    "common_name" : "your CN"
  },
  "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**.

4.1.2.7 Deleting a Certificate

Function

This API is used to delete a certificate.

URI

DELETE /v1/private-certificates/{certificate_id}

Table 4-172 Path Parameters

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

Request Parameters

Table 4-173 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 400

Table 4-174 Response body parameters

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

Status code: 401

Table 4-175 Response body parameters

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

Status code: 403

Table 4-176 Response body parameters

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

Status code: 404

Table 4-177 Response body parameters

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

Status code: 500

Table 4-178 Response body parameters

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

Example Requests

When you use this API to 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.ae-ad-1.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.
500	Internal service error.

Error Codes

See **Error Codes**.

4.1.2.8 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 4-179 Path Parameters

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

Request Parameters

Table 4-180 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-Auth-Token** in the response header is the user token.

Table 4-181 Request body parameters

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

Response Parameters

Status code: 200

Table 4-182 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 4-183 Response body parameters

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

Status code: 401

Table 4-184 Response body parameters

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

Status code: 403

Table 4-185 Response body parameters

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

Status code: 404

Table 4-186 Response body parameters

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

Status code: 500

Table 4-187 Response body parameters

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

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.ae-ad-1.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**.

4.1.2.9 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 4-188 Path Parameters

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

Request Parameters

Table 4-189 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-Auth-Token** in the response header is the user token.

Table 4-190 Request body parameters

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

Response Parameters

Status code: 400

Table 4-191 Response body parameters

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

Status code: 401

Table 4-192 Response body parameters

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

Status code: 403

Table 4-193 Response body parameters

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

Status code: 404

Table 4-194 Response body parameters

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

Status code: 500

Table 4-195 Response body parameters

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

Example Requests

When you use this API to 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.ae-ad-1.myhuaweicloud.com/v1/private-certificates/
6434f74f-2d13-4e6a-89eb-93ee313f1a43/revoke

{
  "reason" : "private key lost"
}
```

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**.

4.1.3 Certificate Revocation

4.1.3.1 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 4-196 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-197 Response body parameters

Parameter	Type	Description
agency_granted	String	OBS agency status ● **true** ● **false**

Status code: 400

Table 4-198 Response body parameters

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

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

Status code: 401

Table 4-199 Response body parameters

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

Status code: 403

Table 4-200 Response body parameters

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

Status code: 404

Table 4-201 Response body parameters

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

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

Status code: 500

Table 4-202 Response body parameters

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

Example Requests

When you use this API to check whether PCA has the OBS agency permission (for accessing OBS buckets and updating the CRL), a token is required in the **X-Auth-Token** field in the request header, and the token must have the permission to access the API and the **secu_admin** permission.

```
GET https://ccm.ae-ad-1.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.
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**.

4.1.3.2 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 4-203 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-204 Response body parameters

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

Status code: 400

Table 4-205 Response body parameters

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

Status code: 401

Table 4-206 Response body parameters

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

Status code: 403

Table 4-207 Response body parameters

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

Status code: 404

Table 4-208 Response body parameters

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

Status code: 500

Table 4-209 Response body parameters

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

Example Requests

When you use this API to create an OBS agency (for accessing OBS buckets and updating the CRL) for PCA, a token is required in the **X-Auth-Token** field in the request header, and the token must have the permission to access the API and the **secu_admin** permission.

```
POST https://ccm.ae-ad-1.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**.

4.1.3.3 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 4-210 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-Auth-Token** in the response header is the user token.

Response Parameters

Status code: 200

Table 4-211 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 4-212 ObsBuckets

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

Status code: 400

Table 4-213 Response body parameters

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

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

Status code: 401

Table 4-214 Response body parameters

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

Status code: 403

Table 4-215 Response body parameters

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

Status code: 404

Table 4-216 Response body parameters

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

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

Status code: 500

Table 4-217 Response body parameters

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

Example Requests

When you use this API to query the 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.ae-ad-1.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 Permissions and Supported Actions

5.1 Introduction to Permissions Policies and Supported Actions

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

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

Permissions are classified into 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:

- **Private Certificate Authority (PCA)**

5.2 Private Certificate Authority (PCA)

Authorization information about APIs related to private CAs

Permission	API	Action
Creating a CA	POST /v1/private-certificate-authorities	pca:ca:create
Canceling the scheduled deletion of a CA	POST /v1/private-certificate-authorities/{ca_id}/restore	pca:ca:restore
Querying details about a private CA	GET /v1/private-certificate-authorities/{ca_id}	pca:ca:get
Querying CSR details about a private CA	GET /v1/private-certificate-authorities/{ca_id}/csr	pca:ca:getCsr
Querying the private CA quota	GET /v1/private-certificate-authorities/quotas	pca:ca:quota
Exporting a private CA	POST /v1/private-certificate-authorities/{ca_id}/export	pca:ca:export
Deleting a private CA	DELETE /v1/private-certificate-authorities/{ca_id}	pca:ca:delete

Permission	API	Action
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
Querying the private certificate quota	GET /v1/private-certificates/quotas	pca:cert:quota
Creating a private certificate	POST /v1/private-certificates	pca:ca:issueCert
Deleting a private certificate	DELETE /v1/private-certificates/{certificate_id}	pca:ca:delete
Revoking a private certificate	POST /v1/private-certificates/{certificate_id}/revoke	pca:cert:revoke

Permission	API	Action
Creating a private certificate through a CSR	POST /v1/private-certificates/csr	pca:ca:issueCertThroughCSR
Querying the list of private certificates	GET /v1/private-certificates	pca:cert:list

A Appendix

A.1 Status Codes

Statues Codes to Private Certificate Management APIs

Status Codes	Status	Description
200	OK	Request processed successfully.
201	Created	Resource created.
204	NO Content	Request succeeded. No response body is returned.
400	Bad Request	The request parameter is incorrect.
401	Unauthorized	Incorrect or illegal client authentication information.
403	Forbidden	The server understood the request, but is refusing to fulfill it.
404	Not Found	The requested resource does not exist or not found.
500	Internal Server Error	Internal service error.

A.2 Error Codes

A.2.1 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.
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.

Status Code	Error Codes	Error Message	Description	Solution
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.
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].

Status Code	Error Codes	Error Message	Description	Solution
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.
400	PCA. 00020401	Incorrect certificate signature request.	Incorrect certificate signature request.	Please check that the certificate signing request is correct.
400	PCA. 00020402	Incorrect certificate. Please contact technical support.	Incorrect certificate. Please contact technical support.	Please contact technical support.
400	PCA. 00020403	Incorrect certificate chain.	Incorrect certificate chain.	Please confirm that the certificate chain entered meets the requirements: 1. The format should be correct. When requesting through API, you need to use " " or "\r " instead of line feed; 2. The certificate chain should be complete. Some intermediate CA certificates cannot be missing. The order is: intermediate CA >... > Root ca.

Status Code	Error Codes	Error Message	Description	Solution
400	PCA. 00020404	Invalid status. The status can only be Pending activation, Activated, Disabled, Pending deletion, or Expired.	Invalid status. The current support status is PENDING, ACTIVED, DISABLED, DELETED, and EXPIRED.	Please enter a valid status value. The currently supported status values are: PENDING, ACTIVED, DISABLED, DELETED, EXPIRED.
401	PCA. 00000101	Access Denied. No permissions granted for this OBT.	Access Denied. No permissions granted for this OBT.	Please apply for public beta permission.
401	PCA. 00010001	Incorrect X-Auth-Token in the request header.	Incorrect X-Auth-Token in the request header.	Please check: 1. Check whether the token is obtained according to the interface provided by the Identity and Access Management(IAM); 2. Check whether the token has expired. If the problem is not solved after checking the above conditions, please contact technical support.
401	PCA. 00010002	Account frozen. Please contact technical support.	Account frozen. Please contact technical support.	Please contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
401	PCA. 00010003	Access denied. Real-name authenticatio n failed or account in arrears.	Access denied. Real-name authenticatio n failed or account in arrears.	Please confirm whether the account has been authenticated by real name and whether it is in arrears. If it is still not resolved, please contact technical support.
401	PCA. 00010004	Insufficient permissions. Contact administrator.	Insufficient permissions. Contact administrator.	Please contact the account administrator to confirm the account permissions. If the problem is still not resolved, please contact technical support.
403	PCA. 00000006	Obtaining OBS buckets failed. Please contact technical support.	Obtaining OBS buckets failed. Please contact technical support.	Please contact technical support.
403	PCA. 00030001	CA or certificate quantity exceeds quota.	CA or certificate quantity exceeds quota.	Please check whether the number of CAs that have been created or the number of certificates that have been applied for has reached the maximum value. If you need to increase the quota, please contact technical support.

Status Code	Error Codes	Error Message	Description	Solution
403	PCA. 00030201	Operation not allowed in the current status.	Operation not allowed in the current status.	There are restrictions on the operations that the CA or certificate is allowed to perform in different states, please check the conditions of the operations: 1. Disable CA: CA status must be in "ACTIVED" or "EXPIRED" status; 2. Enable CA: CA status must be in "DISABLED" status; 3. Delete CA: CA status must be in "PENDING" or "DISABLED" status; 4. Restore CA: CA status needs to be in "DELETED" status; 5. Export the CSR of the CA: the CA status needs to be in the "PENDING" state; 6. Export CA certificate: CA status needs to be in "ACTIVED" or "EXPIRED" status; 7. Activate CA: The CA status needs to be in the "PENDING" state;

Status Code	Error Codes	Error Message	Description	Solution
				8. Applying for a certificate: The issuing CA status needs to be in the "ACTIVED" status; 9. Export certificate: The certificate status needs to be in the "ISSUED" status. If the problem is not resolved after checking the operating conditions, please contact technical support.
403	PCA. 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 IAM API used to query project information based on the specified criteria.

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

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

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

Obtaining a Project ID from the Console

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

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

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

B Change History

Released On	Description
2022-12-15	This issue is the first official release.