组织成员帐号

API 参考

文档版本 01

发布日期 2024-02-29

华为技术有限公司

版权所有 © 华为技术有限公司 2024。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

 版权所有 © 华为技术有限公司

目 录

 版权所有 © 华为技术有限公司

1 使用前必读

1.1 概述

组织成员帐号OrgID是面向企业提供组织管理、企业成员帐号管理以及SaaS应用授权管理能力的云服务。OrgID通过将Huawei ID扩展到组织内部应用领域，实现对组织部门、用户、帐号、应用、认证源的统一管理。

在调用OrgID的API之前，请确保已经充分了解OrgID相关概念，详细信息请参见**OrgID**。

1.2 调用说明

OrgID提供了REST（Representational State Transfer）风格API，支持通过HTTPS请求调用。

调用方法请参见**如何调用API**。

1.3 终端节点

终端节点即调用API的请求地址，不同服务不同区域的终端节点不同。

使用OrgID服务API无需关注终端节点，需要使用OrgID的公网访问域名，OrgID的公网访问域名为“orgid.huaweiapaas.cn”。

版权所有 © 华为技术有限公司

2 API 概览

OrgID服务提供了多个API接口，包含获取Access Token、获取用户信息等的接口，如**表2-1**所示。

OrgID服务提供的具体API如**表1**所示。

表 2-1 接口说明

API	说明
获取AccessToken	获取Access Token，Access Token可用于调用获取用户信息API。
获取用户信息	获取用户信息。
验证票据	CAS 3.0方式的应用验证票据，可以获取用户属性信息。

版权所有 © 华为技术有限公司

3 如何调用 API

3.1 构造请求

本节介绍REST API请求的组成，并以调用**获取Access Token**接口说明如何调用API，该API获取用户的Token，Token可以用于调用其他API。

您还可以通过这个视频教程了解如何构造请求调用API：**https://bbs.huaweicloud.com/videos/102987** 。

请求 URI

请求URI由如下部分组成：

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

尽管请求URI包含在请求消息头中，但大多数语言或框架都要求您从请求消息中单独传递它，所以在此单独强调。

表 3-1 请求 URI

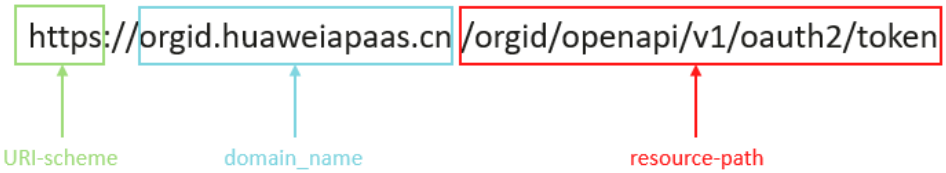
参数	说明
URI-scheme	表示用于传输请求的协议，当前所有API均采用HTTPS协议。
domain_name	使用OrgID的公网访问域名，OrgID的公网访问域名为“orgid.huaweiapaas.cn”。
resource-path	资源路径，也即API访问路径。从具体API的URI模块获取，例如“获取Access Token”API的resource-path为“/orgid/openapi/v1/oauth2/token”，其中“/orgid/openapi”可省略。
query-string	查询参数，是可选部分，并不是每个API都有查询参数。查询参数前面需要带一个“?”，形式为“参数名=参数取值”，例如“?limit=10”，表示查询不超过10条数据。

版权所有 © 华为技术有限公司

例如您需要获取用户访问OrgID的Access Token，则需使用OrgID的公网访问域名（orgid.huaweiapaas.cn），并在获取Access Token的URI部分找到resource-path（/v3/auth/tokens），拼接起来如下所示。

```
https://orgid.huaweiapaas.cn/orgid/openapi/v1/oauth2/token
```

图 3-1 URI 示意图



说明

为查看方便，在每个具体API的URI部分，只给出resource-path部分，并将请求方法写在一起。这是因为URI-scheme都是HTTPS，而domain_name在同一个区域也相同，所以简洁起见将这两部分省略。

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务您正在请求什么类型的操作。

表 3-2 HTTP 方法

方法	说明
GET	请求服务器返回指定资源。
PUT	请求服务器更新指定资源。
POST	请求服务器新增资源或执行特殊操作。
DELETE	请求服务器删除指定资源，如删除对象等。
HEAD	请求服务器资源头部。
PATCH	请求服务器更新资源的部分内容。 当资源不存在的时候，PATCH可能会去创建一个新的资源。

在获取Access Token的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://orgid.huaweiapaas.cn/orgid/openapi/v1/oauth2/token
```

请求消息头

附加请求头字段，如指定的URI和HTTP方法所要求的字段。例如定义消息体类型的请求头“Content-Type”，请求鉴权信息等。

需要添加到请求中的公共消息头如表3-3所示。

版权所有 © 华为技术有限公司

表 3-3 公共请求消息头

参数名	说明	是否必选	示例
Content-type	消息体的类型（格式），默认取值为“application/x-www-form-urlencoded”。	是	application/x-www-form-urlencoded

对于获取Access Token接口，由于不需要认证，所以只添加“Content-Type”即可，添加消息头后的请求如下所示。

```
POST https://orgid.huaweiapaas.cn/orgid/openapi/v1/oauth2/token
Content-Type: application/x-www-form-urlencoded
```

请求消息体

请求消息体通常以结构化格式发出，与请求消息头中Content-type对应，传递除请求消息头之外的内容。若请求消息体中参数支持中文，则中文字符必须为UTF-8编码。

每个接口的请求消息体内容不同，也并不是每个接口都需要有请求消息体（或者说消息体为空），GET、DELETE操作类型的接口就不需要消息体，消息体具体内容需要根据具体接口而定。

对于获取Access Token接口，您可以从接口的请求部分看到所需的请求参数及参数说明。将消息体加入后的请求如下所示，加粗的斜体字段需要根据实际值填写，***client_id***为创建应用后OrgID提供的client_id，***client_secret***为创建应用后OrgID提供的client_secret，***redirect_uri***为创建自建应用时配置的首页URL，***code***为OrgID给用户颁发的code，可以在创建应用后应用的“登录配置”页面该应用的首页URL中获取。

```
POST https://orgid.huaweiapaas.cn/orgid/openapi/v1/oauth2/token
Content-Type: application/x-www-form-urlencoded

{
  grant_type:authorization_code
  client_id:client_id
  client_secret:client_secret
  redirect_uri:redirect_uri
  code:code
}
```

到这里为止这个请求需要的内容就具备齐全了，您可以使用**curl**、**Postman**或直接编写代码等方式发送请求调用API。对于获取Access Token接口，返回的响应消息体中“access_token”就是需要获取的Access Token。有了Token之后，您就可以使用Token认证调用其他API。

3.2 返回结果

请求发送以后，会收到响应，包含：状态码、响应消息头和响应消息体。

版权所有 © 华为技术有限公司

状态码

状态码是一组从1xx到5xx的数字代码，状态码表示了请求响应的状态，完整的状态码列表请参见**状态码**。

对于获取Access Token接口，如果调用后返回状态码为“200”，则表示请求成功。

响应消息头

该部分可选。

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于Access Token接口，不返回响应消息头。

响应消息体

该部分可选。响应消息体通常以结构化格式（如JSON或XML）返回，与响应消息头中Content-Type对应，传递除响应消息头之外的内容。

对于获取Access Token接口，返回如下消息体。

```
{
   "access_token": "3AkJTad**************************0P6JBHQX8ipoG",
   "refresh_token": "Bd0k_ek******************BPVBTGLlMjb-vyjHu0nZYx",
   "scope": "phone profile email",
   "token_type": "Bearer",
   "expires_in": 7200
}
```

当接口调用出错时，会返回错误码及错误信息说明，错误响应的Body体格式如下所示。

```
{
   "error_code": "AS.0001",
   "error_msg": "The format of message is error"
}
```

其中，error_code或error表示错误码，error_msg或error_description表示错误描述信息。

版权所有 © 华为技术有限公司

4 API

4.1 基于 OAuth 的应用认证集成

4.1.1 获取 AccessToken

功能介绍

获取Access Token，Access Token可用于调用获取用户信息API。

URI

POST /orgid/openapi/v1/oauth2/token

请求参数

表 4-1 FormData 参数

参数	是否必选	参数类型	描述
grant_type	是	String	授权方式，该参数为固定值authorization_code。
code	是	String	授权码，基于OAuth协议，OrgID给用户颁发的code。
client_id	是	String	应用标识，创建应用后OrgID提供的client_id。
client_secret	是	String	应用密钥，创建应用后OrgID提供的client_secret。
redirect_uri	是	String	回调地址，即code的接收地址，与创建自建应用时配置的首页URL一致。

版权所有 © 华为技术有限公司

参数	是否必选	参数类型	描述
access_type	否	String	接入模式，默认为在线模式，可不填，如需设置为离线模式，可设置为“offline”，设置后会返回refresh_token。

响应参数

状态码： 200

表 4-2 响应 Body 参数

参数	参数类型	描述
access_token	String	用户级token，授权服务器返回给第三方应用的访问令牌。
refresh_token	String	用户级刷新token，离线模式适用，用于客户端主动刷新用户token。
scope	String	授权信息范围。
token_type	String	访问令牌类型。固定值“Bearer”，消息头传入token时前缀填入方式。
expires_in	Long	访问令牌的有效期，以秒为单位。

状态码： 400

表 4-3 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误描述。
error	String	错误码（兼容原开放接口字段）。
error_description	String	错误描述（兼容原开放接口字段）。

状态码： 401

版权所有 © 华为技术有限公司

表 4-4 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误描述。
error	String	错误码（兼容原开放接口字段）。
error_description	String	错误描述（兼容原开放接口字段）。

状态码： 500

表 4-5 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误描述。
error	String	错误码（兼容原开放接口字段）。
error_description	String	错误描述（兼容原开放接口字段）。

请求示例

```
POST https://orgid.huaweiapaas.cn/orgid/openapi/v1/oauth2/token
Content-Type: application/x-www-form-urlencoded

{
  grant_type: authorization_code
  client_id: 85d6fafdb128582dfaa312f25a9630fd0f32
  client_secret: 11edba361e6a0965206f14304
  redirect_uri: http=//123456789.com
  code:-hp8fzV3Bzk**********kO_g7ZjbGftCHuR
}
```

响应示例

状态码： 200

正常响应。

```
{
    "access_token": "SetPuNNPf49RlT16Y0fvmqetHYmndhXLI7e8lq-4zOJAsKfPmD",
    "refresh_token": "PMBlkkSHDqFtxyNSQrHJfyxdJyNoqiq2_EdhMqRrlQKcbObFeWD",
    "scope": "phone profile email",
    "token_type": "Bearer",
    "expires_in": 7200
}
```


版权所有 © 华为技术有限公司

状态码

状态码	描述
200	正常响应。
400	参数错误响应。
401	权限错误响应。
500	系统错误响应。

错误码

请参见**错误码**。

4.1.2 获取用户信息

功能介绍

获取用户信息。

URI

GET /orgid/openapi/v1/oauth2/userinfo

请求参数

表 4-6 请求 Header 参数

参数	是否必选	参数类型	描述
X-OrgID-Authorization	是	String	用户访问凭证，即Bearer {access_token}。

响应参数

状态码： 200

表 4-7 响应 Body 参数

参数	参数类型	描述
tenant	String	租户code，即企业code。
name	String	用户名。
mobile	String	手机号。
user_name	String	用户登录账号。

版权所有 © 华为技术有限公司

参数	参数类型	描述
user_id	String	用户外部id。
email	String	邮箱。
role	String	角色，枚举：user或admin。

状态码： 400

表 4-8 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误描述。
error	String	错误码（兼容原开放接口字段）。
error_description	String	错误描述（兼容原开放接口字段）。

状态码： 401

表 4-9 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误描述。
error	String	错误码（兼容原开放接口字段）。
error_description	String	错误描述（兼容原开放接口字段）。

状态码： 500

表 4-10 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误描述。
error	String	错误码（兼容原开放接口字段）。

版权所有 © 华为技术有限公司

参数	参数类型	描述
error_description	String	错误描述（兼容原开放接口字段）。

请求示例

```
GET https://orgid.huaweiapaas.cn/orgid/openapi/v1/oauth2/userinfo
--header 'Authorization': Bearer 0s2tzzP4K7ragzUrj-***GqQDxuv9S3vDHYtFCb5GxcDv
```

响应示例

状态码： 200

正常响应。

```
{
  "tenant_name" : "dddd",
  "role" : "admin",
  "login_type" : "saml",
  "user_name" : "wss2111",
  "mobile" : "176****0802",
  "employee_code" : "00001",
  "domain_id" : "46fdb8041e7444a4aef1435bf5f93b72",
  "user_id" : "1008600000062741768",
  "name" : "176******02",
  "email" : "l***@huawei.com",
  "tenant" : "9190086000001301818"
}
```

状态码

状态码	描述
200	正常响应。
400	参数错误响应。
401	权限错误响应。
500	系统错误响应。

错误码

请参见**错误码**。

4.2 基于 CAS 的应用认证集成

4.2.1 验证票据

功能介绍

CAS3.0方式应用验证票据，并获取用户属性信息。

版权所有 © 华为技术有限公司

URI

GET /orgid/openapi/v1/cas/p3/serviceValidate

表 4-11 Query 参数

参数	是否必选	参数类型	描述
service	是	String	登录时携带的回调地址。 最大长度：**1024**
ticket	是	String	登录时系统返回的ticket。 最大长度：**128**

请求参数

```
GET https://orgid.huaweiapaas.cn/orgid/openapi/v1/cas/p3/serviceValidate?service=http://123456789.com&ticket=ST-******OwBG
```

响应参数

状态码： 200

表 4-12 响应 Body 参数

参数	参数类型	描述
serviceResponse	**ServiceResponse** object	业务响应

表 4-13 ServiceResponse

参数	参数类型	描述
authenticationFailure	**CasServiceResponseAuthenticationFailure** object	失败响应
authenticationSuccess	**CasServiceResponseAuthenticationSuccess** object	成功响应

表 4-14 CasServiceResponseAuthenticationFailure

参数	参数类型	描述
code	String	错误码

版权所有 © 华为技术有限公司

参数	参数类型	描述
description	String	错误描述

表 4-15 CasServiceResponseAuthenticationSuccess

参数	参数类型	描述
user	String	用户标识
proxyGrantingTicket	String	代理授权凭据
proxies	Array of strings	代理
attributes	**CasAuthenticationSuccessAttributes** object	属性

表 4-16 CasAuthenticationSuccessAttributes

参数	参数类型	描述
authenticationDate	String	认证时间
longTermAuthenticationRequestTokenUsed	Boolean	true/false
isFromNewLogin	Boolean	true/false
token	String	获取用户信息的token
logo	String	用户头像URL
displayName	String	用户显示名
uid	String	华为账号uid

请求示例

无

响应示例

状态码： 200

版权所有 © 华为技术有限公司

CAS3.0票据校验响应。


```
{
  "serviceResponse" : {
    "authenticationFailure" : null,
    "authenticationSuccess" : {
      "user" : "wss2111",
      "proxyGrantingTicket" : null,
      "proxies" : null,
      "attributes" : {
        "user_name" : "wss2111",
        "name" : "176******02",
        "mobile" : "176****0802",
        "email" : "l***@huawei.com",
        "user_id" : "1008600000106085748"
      }
    }
  }
}
```


状态码

状态码	描述
200	CAS3.0票据校验响应。

错误码

请参见**错误码**。

版权所有 © 华为技术有限公司

5 附录

5.1 状态码

状态码如表5-1所示。

表 5-1 状态码

状态码	编码	说明
200	OK	正常响应。
400	Bad Request	参数错误响应。
401	Unauthorized	权限错误响应。
500	Internal Server Error	系统错误响应。

5.2 错误码

当您调用API时，如果遇到“APIGW”开头的错误码，请参见API网关错误码进行处理。

状态码	错误码	错误信息	描述	处理措施
400	无	invalid_grant	url clientId clientSecret错误。	检查调用参数或者联系运营开发人员定位。
401	OrgID.OAUTH.4000	invalid token	不合法的token。	检查是否正确的获取token或者重新生成token。
401	OrgID.OAUTH.4001	token expired	token过期。	重新生成token。

版权所有 © 华为技术有限公司

状态码	错误码	错误信息	描述	处理措施
401	OrgID.OAUTH.4006	token is not user token	非用户级token。	使用用户级token，不要使用应用级token。

版权所有 © 华为技术有限公司

6 修订记录

表 6-1 修订记录

发布日期	修订记录
2024-02-29	第一次正式发布。

版权所有 © 华为技术有限公司