应用身份管理服务

API 参考

文档版本 01

发布日期 2023-06-30

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 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

HUAWEI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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 使用前必读 1
1.1 概述 1
1.2 调用说明 1
1.3 终端节点 1
1.4 基本概念 1
1.5 获取用户访问域名 2
2 API 概览 3
3 API 5
3.1 管理类接口 5
3.1.1 如何调用 API 5
3.1.1.1 构造请求 5
3.1.1.2 返回结果 8
3.1.2 访问凭据 8
3.1.2.1 获取访问凭据 9
3.1.3 用户管理 10
3.1.3.1 创建用户 10
3.1.3.2 修改用户 16
3.1.3.3 删除用户 20
3.1.3.4 启用用户 21
3.1.3.5 禁用用户 23
3.1.3.6 修改用户密码 24
3.1.3.7 校验原密码修改用户密码 26
3.1.3.8 根据用户 id 查询用户详情 28
3.1.3.9 根据用户名查询用户详情 31
3.1.3.10 查询用户列表 34
3.1.3.11 用户授权应用帐号 37
3.1.3.12 查询用户所有授权的应用帐号 39
3.1.4 组织管理 41
3.1.4.1 创建组织 41
3.1.4.2 修改组织 43
3.1.4.3 删除组织 45
3.1.4.4 查询组织详情 47

3.1.4.5 查询组织列表.....48
3.1.5 应用机构管理.....51
3.1.5.1 新增应用机构.....51
3.1.5.2 修改应用机构.....53
3.1.5.3 删除应用机构.....55
3.1.5.4 查询应用机构详情.....57
3.1.5.5 查询应用机构列表.....59
3.1.6 应用帐号管理.....61
3.1.6.1 新增应用帐号.....61
3.1.6.2 更新应用帐号.....63
3.1.6.3 删除应用帐号.....65
3.1.6.4 查询应用帐号详情.....67
3.1.6.5 查询应用帐号列表.....70
3.1.6.6 启用应用帐号.....73
3.1.6.7 禁用应用帐号.....75
3.1.7 应用侧角色管理.....77
3.1.7.1 新增应用侧角色.....77
3.1.7.2 修改应用侧角色信息.....79
3.1.7.3 删除应用侧角色.....81
3.1.7.4 查询应用侧角色详情.....82
3.1.7.5 查询应用侧角色列表.....84
3.1.7.6 新增应用侧角色成员.....87
3.1.7.7 删除应用侧角色成员.....89
3.1.7.8 查询应用侧角色成员列表.....91
3.2 用户类接口.....94
3.2.1 如何调用 API.....94
3.2.1.1 构造请求.....94
3.2.1.2 返回结果.....97
3.2.2 系统接口.....97
3.2.2.1 获取服务器时间.....97
3.2.2.2 获取公钥.....99
3.2.3 注册.....101
3.2.3.1 使用手机号和短信验证码注册.....102
3.2.4 验证码.....105
3.2.4.1 获取图形验证码.....105
3.2.4.2 校验图形验证码.....108
3.2.4.3 获取国际区号.....111
3.2.4.4 发送短信验证码.....114
3.2.5 登录登出.....116
3.2.5.1 用户名密码登录.....117
3.2.5.2 手机短信验证码登录.....120
3.2.5.3 微信登录.....123

3.2.5.4 支付宝登录 125
3.2.5.5 退出登录 128
3.2.6 社交帐号 130
3.2.6.1 社交帐号登录绑定手机号 130
3.2.6.2 社交帐号注册并绑定手机号 133
3.2.6.3 获取用户已绑定的社交帐号列表 136
3.2.6.4 社交帐号解绑 139
3.2.7 密码管理 141
3.2.7.1 跳过强制修改密码 141
3.2.7.2 密码过期强制修改密码 144
3.2.7.3 通过手机号找回密码 147
3.2.8 二次认证 149
3.2.8.1 通过 state_Token 获取手机号 149
3.2.8.2 手机号短信验证码二次认证 151
3.2.9 个人信息管理 154
3.2.9.1 查询个人信息 154
3.2.9.2 修改个人信息 156
3.2.10 SSO 159
3.2.10.1 通过 session_token 获取 sso_ticket 159
3.2.10.2 通过 sso_ticket 获取用户信息 162
3.2.10.3 刷新 session_token 165
3.2.11 id_token 管理 167
3.2.11.1 通过 session_token 生成 id_token 167
3.3 应用集成接口 169
3.3.1 如何调用 API 169
3.3.1.1 构造请求 170
3.3.1.2 返回结果 172
3.3.2 基于 CAS 的应用认证集成 173
3.3.2.1 认证登录 173
3.3.2.2 验证票据(CAS3.0) 174
3.3.2.3 注销登录 176
3.3.2.4 验证票据(CAS1.0) 177
3.3.2.5 验证票据(CAS2.0) 178
3.3.3 基于 SAML2.0 的应用认证集成 180
3.3.3.1 IdP-initiated 单点登录 180
3.3.3.2 获取 IdP 元数据 metadata 181
3.3.4 基于 OAuth2.0 的应用认证集成 181
3.3.4.1 认证登录获取授权码 182
3.3.4.2 获取 AccessToken 183
3.3.4.3 获取用户信息 186
3.3.4.4 刷新 Access Token 188
3.3.5 基于 OIDC 的应用认证集成 190

3.3.5.1 认证登录获取授权码 190
3.3.5.2 获取 ID Token 191
3.3.5.3 刷新 Access Token 193
3.3.5.4 隐式授权 196
3.3.5.5 获取 OIDC metadata 197
3.3.6 退出登录 198
3.3.6.1 全局退出 200
4 附录 202
4.1 session token 签名 202
4.2 对 OIDC 协议中的 id_token 进行验证 204
4.3 错误码 204

1 使用前必读

1.1 概述

欢迎使用应用身份管理服务OneAccess。OneAccess提供集中式的身份管理、身份认证、身份授权服务，保证合法用户以适当的权限访问受信任的云端和本地应用系统。

您可以使用本文档提供的API对OneAccess进行相关操作，包括：

- 管理类接口：提供给管理员进行用户、组织、应用等管理操作的接口。
- 用户类接口：提供给普通用户进行登录登出、密码管理等操作的接口。
- 应用集成接口：提供给下游应用进行单点登录等操作的接口。

在调用应用身份管理服务的API之前，请确保已经充分了解应用身份管理服务的相关概念，详细信息请参见产品介绍。

1.2 调用说明

应用身份管理服务提供了REST（Representational State Transfer）风格API，支持您通过HTTPS请求调用。

1.3 终端节点

终端节点即调用API的**请求地址**，不同服务在不同区域的终端节点不同。

OneAccess是全局级服务，使用OneAccess服务API无需关注终端节点，需要使用用户访问域名，获取方法请参见获取用户访问域名。

1.4 基本概念

- 企业管理员

  企业管理员包括主账号或拥有OneAccess管理权限的用户。企业管理员在OneAccess管理门户负责用户（组）、组织、应用及API等实体的管理。
- 系统管理员

版权所有 © 华为云计算技术有限公司

系统管理员由企业管理员在统一身份认证服务中创建，拥有对企业所有组织结构、用户、应用及除创建管理员以外其他管理门户菜单的管理权限。

- 普通用户

  普通用户是企业应用使用者，包含企业员工、合作伙伴、客户等。普通用户可以登录OneAccess用户门户访问和操作应用。

1.5 获取用户访问域名

操作场景

在调用接口时，请求头中需要填入用户访问域名{domain_name}，需要获取此域名。

获取用户访问域名

该域名需由创建人在应用身份管理服务控制台获取。步骤如下：

步骤1 管理员登录应用身份管理服务控制台。

步骤2 单击**用户访问域名**后的复制，获取**用户访问域名**。

图 1-1 获取用户访问域名

----结束

版权所有 © 华为云计算技术有限公司

2 API 概览

应用身份管理服务为您提供管理类、用户类和应用集成相关接口。

表 2-1 OneAccess 接口说明

接口分类	接口类型	接口说明
管理类接口	访问认证	包括获取访问凭据。
	用户管理	包括创建、修改、删除用户以及为用户授权、查询用户信息等。
	组织管理	包括创建、修改、删除组织以及查询组织等。
	应用机构管理	包括更新、删除、新增应用机构以及查询应用机构等。
	应用帐号管理	包括更新、禁用、启用、删除、新增应用帐号以及查询应用帐号等。
	应用侧角色管理	包括更新、删除、新增应用侧角色和应用侧角色成员以及查询应用侧角色、角色成员等。
用户类接口	系统接口	包括获取服务器时间、获取公钥。
	注册接口	包括使用手机号和短信验证码注册。
	验证码	包括获取图形验证码、校验图形验证码、获取国际区号、发送短信验证码等。
	登录登出	包括用户密码登录、手机短信验证码登录、微信登录、支付宝登录、退出登录等。
	社交帐号	包括社交帐号登录绑定手机号、社交帐号注册并绑定手机号、获取用户已绑定的社交帐号列表、社交帐号解绑等。
	密码管理	包括跳过强制修改密码、密码过期强制修改密码、查询是否设置个人密码、通过手机号找回密码等。
	二次认证	包括通过state_Token获取手机号和手机号短信验证码二次认证。

版权所有 © 华为云计算技术有限公司

接口分类	接口类型	接口说明
	个人信息管理	包括查询个人信息、修改个人信息和修改个人手机号。
	SSO	包括通过session_token获取sso_ticket、通过sso_ticket获取用户信息和刷新session_token。
	id_token管理	包括通过session_token生成id_token。
应用集成接口	基于CAS的应用认证集成	包括基于CAS协议进行应用认证集成的接口，如认证登录、验证票据、注销登录等。
	基于SAML2.0的应用认证集成	包括基于SAML2.0协议进行应用认证集成的接口，如获取IdP元数据等。
	基于OAuth2.0的应用认证集成	包括基于OAuth2.0协议进行应用认证集成的接口，如认证登录获取授权码、获取AccessToken、获取用户信息等。
	基于OIDC的应用认证集成	包括基于OIDC协议进行应用认证集成的接口，如隐式授权、认证登录获取授权码等。
	统一退出	包括全局退出接口，用于注销会话退出登录应用。

版权所有 © 华为云计算技术有限公司

3 API

3.1 管理类接口

3.1.1 如何调用 API

3.1.1.1 构造请求

本节介绍API请求的组成，并以调用OneAccess管理类接口必须的“获取访问凭据”为例接口说明如何调用API，获取访问凭证后，可用于调用其他管理类API。

前提条件

调用API前，管理员在OneAccess管理门户中需参考**授权API**授权API，并且获取管理员在OneAccess管理门户中已添加应用的**通用信息**中的ClientId以及ClientSecret，用以调用API实现相关接口功能。

请求 URI

OneAccess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 URI 中的参数说明

参数	描述
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OneAccess服务API需要使用用户访问域名，获取方法请参见**获取用户访问域名**。

参数	描述
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“获取访问凭证”API的resource-path为“/api/v2/tenant/token”。
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。

例如您需要获取用户访问域名为“abcdefg.huaweioneaccess.com”的实例Access Token，则需使用用户访问域名“abcdefg.huaweioneaccess.com”，并在获取访问凭据的URI部分找到resource-path（/api/v2/tenant/token），拼接起来如下所示。

```
https://abcdefg.huaweioneaccess.com/api/v2/tenant/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在同一个实例也相同，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。

在获取访问凭据的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://abcdefg.huaweioneaccess.com/api/v2/tenant/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。

详细的公共请求消息头字段请参见**表3-3**。

表 3-3 公共请求消息头

名称	描述	是否必选	示例
Content-Type	消息体的类型（格式）。默认取值为“application/json”，有其他取值时会在具体接口中专门说明。	是	application/json
Accept	接受响应类型。推荐用户使用默认值application/json，有其他取值时会在具体接口中专门说明。	否	application/json
Content-Length	请求body长度，单位为Byte。	否	3495
Authorization	认证凭据。如获取用户信息接口，值为Bearer {access_token}。	否	Bearer {access_token}

对于获取访问凭据接口，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://{domain_name}/api/v2/tenant/token
Content-Type: application/x-www-form-urlencoded
```

请求消息体（可选）

该部分可选。请求消息体通常以结构化格式（如JSON或XML）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。若请求消息体中的参数支持中文，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。

对于获取访问凭据接口，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，其中***ClientId***

为注册应用后分配的接口认证凭证ID，***ClientSecret***为注册应用后分配的接口认证凭证密钥。

```
POST https://{domain_name}/api/v2/tenant/token
Content-Type: application/x-www-form-urlencoded

client_id=ClientId&
client_secret=ClientSecret&
grant_type=client_credentials
```

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。对于获取访问凭据接口，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。

3.1.1.2 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

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。

对于获取访问凭据接口，如果调用后返回状态码为“200”，则表示请求成功。

响应消息头（可选）

该部分可选。

对应请求消息头，响应同样也有消息头，如“Content-type”。

对于获取访问凭据接口，不返回响应消息头。

响应消息体（可选）

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。

对于获取访问凭据接口，返回如下消息体。

```
{
  "access_token" : "334**********************************140...",
  "token_type" : "Bearer",
  "expires_in" : 1719,
  "scope" : "all",
  "id_token" : "eyJ*****************************************************************************pYW..."
}
```

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": "invalid_client",
  "error_description": "Bad client credentials"
}
```

其中，error表示错误类型，error_description表示错误描述信息。

3.1.2 访问凭据

3.1.2.1 获取访问凭据

功能介绍

获取应用的API访问凭据。Token的有效期默认为30分钟，可在管理门户-设置-服务配置-API认证配置中设置过期时间修改。建议进行缓存，避免频繁调用。使用Token前请确保Token离过期有足够的时间，防止调用API的过程中Token过期导致调用API失败。重新获取Token，不影响已有Token有效性。

URI

POST /api/v2/tenant/token

请求参数

表 3-4 FormData 参数

参数	是否必选	参数类型	描述
grant_type	是	String	授权类型，固定值：client_credentials。
client_id	是	String	应用标识，注册应用后，分配的ClientId。
client_secret	是	String	应用密钥，注册应用后，分配的ClientSecret。

响应参数

状态码： 200

表 3-5 响应 Body 参数

参数	参数类型	描述
access_token	String	认证凭据，用于调用管理API。
token_type	String	认证凭据类型。固定值：Bearer。
expires_in	Integer	过期时间。单位为秒，默认1800s。
scope	String	获取的Access Token授权访问范围。
id_token	String	授权访问id_token。

状态码： 400

表 3-6 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

获取凭据，根据应用的clientid以及clientsecret获取接口鉴权token。

```
POST https://{domain_name}/api/v2/tenant/token

Content-Type: application/x-www-form-urlencoded

client_id=ONtQq2igSggfFClyGgzmuXR8ubWEP...&
client_secret=XdqUmJpG19hNEHz3472XsPcwvfe...&
grant_type=client_credentials
```

响应示例

状态码： 200

请求成功。

```
{
  "access_token" : "334******140",
  "token_type" : "Bearer",
  "expires_in" : 1719,
  "scope" : "all",
  "id_token" : "ey******Is.ey******Yo.EL******YW"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3 用户管理

3.1.3.1 创建用户

功能介绍

创建用户。

URI

POST /api/v2/tenant/users

请求参数

表 3-7 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-8 请求 Body 参数

参数	是否必选	参数类型	描述
user_name	是	String	用户名，用户唯一标识，企业内唯一。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性。
password	否	String	密码，需要满足企业定义的格式。
mobile	是	String	手机号，企业内唯一。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性
org_code	否	String	主组织的组织编码，填写企业中存在的组织编码。为空时组织在第一个根组织下。
name	否	String	姓名，为空值时设置为user_name。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性。
email	否	String	邮箱。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性。
employee_id	否	String	员工id。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性。

参数	是否必选	参数类型	描述
first_name	否	String	名字。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性。
middle_name	否	String	中间名。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性。
last_name	否	String	姓氏。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性。
pwd_must_modify	否	Boolean	首次登录是否需要强制修改密码。 缺省值：**true**
attr_gender	否	String	性别。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性。 枚举值： ● **unknown：保密** ● **male：男** ● **female：女**
attr_birthday	否	String	生日，格式为yyyy-mm-dd。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性。
attr_nick_name	否	String	昵称。可在管理门户界面，用户菜单下的用户属性定义中修改必填属性。

参数	是否必选	参数类型	描述
attr_identity_type	否	String	证件类型。 枚举值： ● **id_card：居民身份证** ● **HongKong_Macau_Taiwan_residence_permit：港澳台居住证** ● **mainland_travel_permit_for_HongKong_Macao：港澳居民来往内地通行证** ● **mainland_travel_permit_for_Taiwan：台湾居民来往大陆通行证** ● **chinese_passport：中国护照** ● **overseas_passport：海外驾照** ● **overseas_driver_license：海外驾照** ● **officer_id：军官证** ● **foreigner_residence_permit：外国人居留证** ● **other：其他**
attr_identity_number	否	String	证件号码。
attr_area	否	String	国家或者地区的编码。
attr_city	否	String	城市。
attr_manager_id	否	String	直属上级。
attr_user_type	否	String	人员类型。 枚举值： ● **regular：正式** ● **intern：实习** ● **dispatch：劳务派遣** ● **outsourcing：劳务外包**
attr_hire_date	否	String	入职时间，格式为yyyy-MM-dd。
attr_work_place	否	String	工作地点。

参数	是否必选	参数类型	描述
user_org_relation_list	否	Array of **UserOrgRelationListOption** objects	用户组织关系集合。若填写，必须包含主组织的信息。
extension	否	Object	自定义扩展属性。

表 3-9 UserOrgRelationListOption

参数	是否必选	参数类型	描述
orgCode	是	String	组织编码
relationType	是	String	归属关系，同一用户只能有1个归属，最多9个挂靠。 枚举值： ● **0：挂靠** ● **1：归属**

响应参数

状态码： 201

表 3-10 响应 Body 参数

参数	参数类型	描述
user_id	String	用户id。

状态码： 400

表 3-11 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

创建一个用户，用户名zhangsan，手机号12345678901，邮箱zhangsan@example.com。

```
POST https://{domain_name}/api/v2/tenant/users
```

```
Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
{
    "user_name": "zhangsan",
    "password": "p******d",
    "org_code": "10000",
    "name": "zhangsan",
    "mobile": "12345678901",
    "email": "zhangsan@example.com",
    "employee_id": "123456789",
    "pwd_must_modify": false,
    "first_name": "F",
    "middle_name": "M",
    "last_name": "L",
    "attr_gender": "male",
    "attr_birthday": "1990-02-01",
    "attr_nick_name": "zhangsan",
    "attr_identity_type": "id_card",
    "attr_identity_number": "123456789",
    "attr_area": "CN",
    "attr_city": "xxx",
    "attr_manager_id": "123456789",
    "attr_user_type": "regular",
    "attr_hire_date": "2021-04-01",
    "attr_work_place": "xxx",
    "user_org_relation_list": [
     {
          "orgCode": "10000",
          "relationType": 1
     },
     {
          "orgCode": "TestOrg1",
          "relationType": 0
     },
     {
          "orgCode": "TestOrg2",
          "relationType": 0
     }
    ],
    "extension": {
       "age": "18"
    }
}
```

响应示例

状态码： 201

请求成功。

```
{
  "user_id" : "20210621095935811-5E16-6B3060..."
}
```

状态码

状态码	描述
201	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3.2 修改用户

功能介绍

修改用户。

URI

PUT /api/v2/tenant/users/{user_id}

表 3-12 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	用户id。

请求参数

表 3-13 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-14 请求 Body 参数

参数	是否必选	参数类型	描述
user_name	否	String	用户名，用户唯一标识，企业内唯一。
mobile	否	String	手机号，企业内唯一。
org_code	否	String	组织编码。
name	否	String	姓名。
email	否	String	邮箱。
employee_id	否	String	员工id。
first_name	否	String	名字。
middle_name	否	String	中间名。

参数	是否必选	参数类型	描述
last_name	否	String	姓氏。
pwd_must_modify	否	Boolean	首次登录是否需要强制修改密码。 缺省值：**true**
attr_gender	否	String	性别。 枚举值： ● **unknown：保密** ● **male：男** ● **female：女**
attr_birthday	否	String	生日，格式为yyyy-mm-dd。
attr_nick_name	否	String	昵称。
attr_identity_type	否	String	证件类型。 枚举值： ● **id_card：居民身份证** ● **HongKong_Macau_Taiwan_residence_permit：港澳台居住证** ● **mainland_travel_permit_for_HongKong_Macao：港澳居民来往内地通行证** ● **mainland_travel_permit_for_Taiwan：台湾居民来往大陆通行证** ● **chinese_passport：中国护照** ● **overseas_passport：海外驾照** ● **overseas_driver_license：海外驾照** ● **officer_id：军官证** ● **foreigner_residence_permit：外国人居留证** ● **other：其他**
attr_identity_number	否	String	证件号码。
attr_area	否	String	国家或者地区的编码。
attr_city	否	String	城市。

参数	是否必选	参数类型	描述
attr_manager_id	否	String	直属上级。
attr_user_type	否	String	人员类型。 枚举值： ● **regular：正式** ● **intern：实习** ● **dispatch：劳务派遣** ● **outsourcing：劳务外包**
attr_hire_date	否	String	入职时间，格式为yyyy-MM-dd。
attr_work_place	否	String	工作地点。
user_org_relation_list	否	**UserOrgRelationListOption** object	
extension	否	Object	自定义扩展属性。

表 3-15 UserOrgRelationListOption

参数	是否必选	参数类型	描述
orgCode	是	String	组织编码
relationType	是	String	归属关系，同一用户只能有1个归属，最多9个挂靠。 枚举值： ● **0：挂靠** ● **1：归属**

响应参数

状态码： 200

表 3-16 响应 Body 参数

参数	参数类型	描述
user_id	String	用户id。

状态码： 400

表 3-17 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

修改用户，用户名zhangsan，手机号12345678901，邮箱zhangsan@example.com。

```
PUT https://{domain_name}/api/v2/tenant/users/{user_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
    "user_name": "zhangsan",
    "org_code": "10000",
    "name": "zhangsan",
    "mobile": "12345678901",
    "email": "zhangsan@example.com",
    "employee_id": "123456789",
    "pwd_must_modify": false,
    "first_name": "F",
    "middle_name": "M",
    "last_name": "L",
    "attr_gender": "male",
    "attr_birthday": "1990-02-01",
    "attr_nick_name": "zhangsan",
    "attr_identity_type": "id_card",
    "attr_identity_number": "123456789",
    "attr_area": "CN",
    "attr_city": "xxx",
    "attr_manager_id": "123456789",
    "attr_user_type": "regular",
    "attr_hire_date": "2021-04-01",
    "attr_work_place": "xxx",
    "user_org_relation_list": [
     {
           "orgCode": "10000",
           "relationType": 1
      },
      {
           "orgCode": "TestOrg1",
           "relationType": 0
      },
      {
           "orgCode": "TestOrg2",
           "relationType": 0
      }
    ],
    "extension": {
       "age": "18"
    }
}
```

响应示例

状态码： 200

请求成功。

```
{
  "user_id" : "20210621095935811-5E16-6B3060..."
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3.3 删除用户

功能介绍

删除用户。

URI

DELETE /api/v2/tenant/users/{user_id}

表 3-18 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	用户id。

请求参数

表 3-19 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 400

表 3-20 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

删除用户，基于传入的user_id删除指定用户。

```
DELETE https://{domain_name}/api/v2/tenant/users/{user_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

无

状态码

状态码	描述
204	请求成功。
400	认证失败。

错误码

请参见错误码。

3.1.3.4 启用用户

功能介绍

启用用户。

URI

PUT /api/v2/tenant/users/{user_id}/enable

表 3-21 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	用户id。

请求参数

表 3-22 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-23 响应 Body 参数

参数	参数类型	描述
user_id	String	用户id。

状态码： 400

表 3-24 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

启用用户，根据传入的user_id启用用户。

```
PUT https://{domain_name}/api/v2/tenant/users/{user_id}/enable

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "user_id" : "20210621095935811-5E16-6B3060..."
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3.5 禁用用户

功能介绍

禁用用户。

URI

PUT /api/v2/tenant/users/{user_id}/disable

表 3-25 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	用户id。

请求参数

表 3-26 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-27 响应 Body 参数

参数	参数类型	描述
user_id	String	用户id。

状态码： 400

表 3-28 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

禁用用户，根据传入的user_id禁用用户。

```
PUT https://{domain_name}/api/v2/tenant/users/{user_id}/disable

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "user_id" : "20210621095935811-5E16-6B3060..."
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3.6 修改用户密码

功能介绍

修改用户密码。

URI

PUT /api/v2/tenant/users/{user_id}/change-password

表 3-29 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	用户id。

请求参数

表 3-30 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-31 请求 Body 参数

参数	是否必选	参数类型	描述
password	是	String	新密码。
pwd_must_modify	否	Boolean	首次登录是否需要修改密码。 缺省值：**true**

响应参数

状态码： 200

表 3-32 响应 Body 参数

参数	参数类型	描述
user_id	String	用户id。

状态码： 400

表 3-33 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

修改用户密码，用户新密码12345678，首次登录不强制修改密码。

```
PUT https://{domain_name}/api/v2/tenant/users/{user_id}/change-password

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
  "password":"12345678",
  "pwd_must_modify":false
}
```

响应示例

状态码： 200

请求成功。

```
{
  "user_id" : "20210621095935811-5E16-6B3060..."
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3.7 校验原密码修改用户密码

功能介绍

校验原密码修改用户密码。

URI

PUT /api/v2/tenant/users/{user_id}/change-password-verify

表 3-34 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	用户id。

请求参数

表 3-35 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-36 请求 Body 参数

参数	是否必选	参数类型	描述
password	是	String	新密码。
old_password	是	String	原密码。

响应参数

状态码： 200

表 3-37 响应 Body 参数

参数	参数类型	描述
user_id	String	用户id。

状态码： 400

表 3-38 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

校验原密码修改用户密码。

```
PUT https://{domain_name}/api/v2/tenant/users/{user_id}/change-password-verify

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
 "password":"N******8",
  "old_password":"O******4"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "user_id" : "20210621095935811-5E16-6B3060..."
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3.8 根据用户 id 查询用户详情

功能介绍

根据用户id查询用户详情。

URI

GET /api/v2/tenant/users/{user_id}

表 3-39 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	用户id。

请求参数

表 3-40 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-41 响应 Body 参数

参数	参数类型	描述
user_id	String	用户id。
org_id	String	用户所属组织。
user_name	String	用户名。
name	String	姓名。
mobile	String	手机号。
email	String	邮箱。
pwd_must_modify	Boolean	首次登录是否强制修改密码。
pwd_change_at	String	密码修改时间
created_at	String	创建时间。
updated_at	String	最后一次修改时间。
disabled	Boolean	是否禁用。
grade	Integer	可信等级。
locked	String	是否锁定。
extension	Object	自定义扩展属性。
user_org_relation_list	Array of **UserOrgRelationListResult** objects	用户组织关系集合。

表 3-42 UserOrgRelationListResult

参数	参数类型	描述
org_id	String	组织id。
relation_type	String	关系类型。

状态码： 400

表 3-43 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

查询用户详情，根据传入的user_id查询用户详情。

```
GET https://{domain_name}/api/v2/tenant/users/{user_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "user_id" : "20220413165737132-3BA0-91FCA2CB7",
  "org_id" : "20220117125622909-9346-35755733F",
  "user_name" : "zhangsan",
  "name" : "zhangsan",
  "mobile" : "12345678901",
  "email" : "zhangsan@example.com",
  "pwd_must_modify" : true,
  "pwd_change_at" : "2022-04-14 10:14:01.988",
  "created_at" : "2022-04-13 16:57:36.532",
  "updated_at" : "2022-04-14 10:14:01.979",
  "disabled" : false,
  "grade" : 1,
  "locked" : false,
  "extension" : { },
  "user_org_relation_list" : [ {
    "org_id" : "20220117125622909-9346-35755733F",
    "relation_type" : 1
  }, {
    "org_id" : "20220415103506608-AF59-5CC9081B9",
    "relation_type" : 0
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3.9 根据用户名查询用户详情

功能介绍

根据用户名查询用户详情。

URI

POST /api/v2/tenant/users/user-by-username

请求参数

表 3-44 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-45 请求 Body 参数

参数	是否必选	参数类型	描述
user_name	是	String	用户名称。

响应参数

状态码： 200

表 3-46 响应 Body 参数

参数	参数类型	描述
user_id	String	用户id。
org_id	String	用户所属组织。
user_name	String	用户名。
name	String	姓名。
mobile	String	手机号。
email	String	邮箱。
pwd_must_modify	Boolean	首次登录是否强制修改密码。
pwd_change_at	String	密码修改时间
created_at	String	创建时间。
updated_at	String	最后一次修改时间。
disabled	Boolean	是否禁用。
grade	Integer	可信等级。
locked	String	是否锁定。
extension	Object	自定义扩展属性。
user_org_relation_list	Array of **UserOrgRelationListResult** objects	用户组织关系集合。

表 3-47 UserOrgRelationListResult

参数	参数类型	描述
org_id	String	组织id。
relation_type	String	关系类型。

状态码： 400

表 3-48 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。

参数	参数类型	描述
error_msg	String	错误详情。

请求示例

根据用户名查询用户详情，用户名zhangsan。

```
POST https://{domain_name}/api/v2/tenant/users/user-by-username

{
  "user_name" : "zhangsan"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "user_id" : "20220413165737132-3BA0-91FCA2CB7",
  "org_id" : "20220117125622909-9346-35755733F",
  "user_name" : "zhangsan",
  "name" : "zhangsan",
  "mobile" : "12345678901",
  "email" : "zhangsan@example.com",
  "pwd_must_modify" : true,
  "pwd_change_at" : "2022-04-14 10:14:01.988",
  "created_at" : "2022-04-13 16:57:36.532",
  "updated_at" : "2022-04-14 10:14:01.979",
  "disabled" : false,
  "grade" : 1,
  "locked" : false,
  "extension" : { },
  "user_org_relation_list" : [ {
    "org_id" : "20220117125622909-9346-35755733F",
    "relation_type" : 1
  }, {
    "org_id" : "20220415103506608-AF59-5CC9081B9",
    "relation_type" : 0
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3.10 查询用户列表

功能介绍

查询用户列表。

URI

GET /api/v2/tenant/users

表 3-49 Query 参数

参数	是否必选	参数类型	描述
org_id	是	String	组织id，为空时查询所有用户。
offset	是	Integer	第几页。 最小值：**0**
limit	是	Integer	每页多少条。 最小值：**10** 最大值：**100**

请求参数

表 3-50 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-51 响应 Body 参数

参数	参数类型	描述
total	Long	用户总数。
users	Array of **UsersDetailsResult** objects	用户列表。

表 3-52 UsersDetailsResult

参数	参数类型	描述
user_id	String	用户id。
org_id	String	用户所属组织。
user_name	String	用户名。
name	String	姓名。
mobile	String	手机号。
email	String	邮箱。
pwd_must_modify	Boolean	首次登录是否强制修改密码。
pwd_change_at	String	密码修改时间
created_at	String	创建时间。
updated_at	String	最后一次修改时间。
disabled	Boolean	是否禁用。
grade	Integer	可信等级。
locked	String	是否锁定。
extension	Object	自定义扩展属性。
user_org_relation_list	Array of **UserOrgRelationListResult** objects	用户组织关系集合。

表 3-53 UserOrgRelationListResult

参数	参数类型	描述
org_id	String	组织id。
relation_type	String	关系类型。

状态码： 400

表 3-54 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。

参数	参数类型	描述
error_msg	String	错误详情。

请求示例

查询用户列表，查询前10条所有组织下的用户列表。

```
GET https://{domain_name}/api/v2/tenant/users?org_id=&offset=0&limit=10

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "total" : 1,
  "users" : [ {
    "extension" : { },
    "user_name" : "zhangsan",
    "mobile" : "12345678901",
    "created_at" : "2022-03-31 16:46:02.964",
    "pwd_must_modify" : false,
    "updated_at" : "2022-03-31 16:48:44.073",
    "user_id" : "20220331164602949-904C-D475B60AE",
    "org_id" : "20220331135144180-0FA5-EE3B69068",
    "grade" : 1,
    "name" : "zhangsan",
    "disabled" : false,
    "pwd_change_at" : "2022-03-31 16:47:51.481",
    "locked" : false,
    "user_org_relation_list" : [ {
      "org_id" : "20220331135144180-0FA5-EE3B69068",
      "relation_type" : 1
    }, {
      "org_id" : "20220415103506608-AF59-5CC9081B9",
      "relation_type" : 0
    } ]
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3.11 用户授权应用帐号

功能介绍

为用户授予应用访问权限，并在应用中创建用户对应的应用帐号。

URI

POST /api/v2/tenant/users/{user_id}/applications/{application_id}/accounts

表 3-55 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	用户id。
application_id	是	String	应用id。

请求参数

表 3-56 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-57 请求 Body 参数

参数	是否必选	参数类型	描述
account_name	否	String	对用户授权应用，在应用中创建的应用帐号名，可选参数，为空默认为用户名。

响应参数

状态码： 200

表 3-58 响应 Body 参数

参数	参数类型	描述
account_id	String	应用帐号id。

状态码： 400

表 3-59 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

用户授权应用帐号，在应用application_id中创建名为Test01的应用帐号。

```
POST https://{domain_name}/api/v2/tenant/users/{user_id}/applications/{application_id}/accounts

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
    "account_name":"Test01"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "account_id" : "20210621095931341-4CB3-122995..."
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.3.12 查询用户所有授权的应用帐号

功能介绍

查询用户所有授权的应用帐号。

URI

GET /api/v2/tenant/users/{user_id}/accounts

表 3-60 路径参数

参数	是否必选	参数类型	描述
user_id	是	String	用户id。

请求参数

表 3-61 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-62 响应 Body 参数

参数	参数类型	描述
total	Integer	总数。
accounts	Array of **Accounts** objects	应用帐号列表。

表 3-63 Accounts

参数	参数类型	描述
id	String	应用帐号id。
application_id	String	应用id。

参数	参数类型	描述
account_name	String	应用帐号名。
account_type	String	应用帐号类型。
name	String	应用帐号名称。
extension	Object	自定义扩展属性。

状态码： 400

表 3-64 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

查询用户所有授权的应用帐号，用户id为传入的user_id。

```
GET https://{domain_name}/api/v2/tenant/users/{user_id}/accounts

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "total" : 1,
  "accounts" : [ {
    "id" : "20210621095952398-57D5-B75A129DB",
    "account_name" : "Test01",
    "account_type" : "BASIC_ACCOUNT",
    "application_id" : "20210621095843929-CC99-9E7B3BC1F",
    "name" : "test",
    "extension" : { }
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.4 组织管理

3.1.4.1 创建组织

功能介绍

创建组织。

URI

POST /api/v2/tenant/organizations

请求参数

表 3-65 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-66 请求 Body 参数

参数	是否必选	参数类型	描述
code	是	String	组织编码，可输入中英文、数字、下划线和中划线。 最大长度：**64**
name	是	String	组织名称，所在层级下唯一，可输入中英文、数字、空格、中划线、下划线和&。 最大长度：**100**
parent_id	否	String	父组织id。创建父组织，不需要传递；创建子组织，需要传递。

参数	是否必选	参数类型	描述
category	否	String	组织类型。 缺省值：**department：部门** 枚举值： ● **department：部门** ● **company：公司** ● **unit：科** ● **group：组**

响应参数

状态码： 201

表 3-67 响应 Body 参数

参数	参数类型	描述
org_id	String	组织ID。

状态码： 400

表 3-68 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

创建组织，组织名子部门，组织编码1000001，父组织编码20210623103509267-6ABA-201FFC...，组织类型部门。

```
POST https://{domain_name}/api/v2/tenant/organizations

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
{
    "code": "1000001",
   "name": "子部门",
   "parent_id": "20210623103509267-6ABA-201FFC...",
      "category": "department"
}
```

响应示例

状态码： 201

创建成功。

```
{
  "org_id" : "20210623103509267-6ABA-201FFC..."
}
```

状态码

状态码	描述
201	创建成功。
400	参数无效。

错误码

请参见错误码。

3.1.4.2 修改组织

功能介绍

修改指定组织。

URI

PUT /api/v2/tenant/organizations/{org_id}

表 3-69 路径参数

参数	是否必选	参数类型	描述
org_id	是	String	组织id。

请求参数

表 3-70 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-71 请求 Body 参数

参数	是否必选	参数类型	描述
code	否	String	组织编码，组织编码为空时默认不修改，可输入中英文、数字、下划线和中划线。 最大长度：**64**
name	否	String	组织名称，组织名称为空时默认不修改，可输入中英文、数字、空格、中划线、下划线和&。 最大长度：**100**
parent_id	否	String	父组织id。
category	否	String	组织类型。 缺省值：**department：部门** 枚举值： ● **department：部门** ● **company：公司** ● **unit：科** ● **group：组**

响应参数

状态码： 200

表 3-72 响应 Body 参数

参数	参数类型	描述
org_id	String	组织ID。

状态码： 400

表 3-73 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

修改组织信息，组织编码为TestOrg，组织名为测试机构，父组织为根组织，组织类型为部门。

```
PUT https://{domain_name}/api/v2/tenant/organizations/{org_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
    "code": "TestOrg",
    "name": "测试机构",
    "parent_id": "",
    "category": "department"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "org_id" : "20210623103509267-6ABA-201FFC..."
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.4.3 删除组织

功能介绍

删除指定组织。

URI

DELETE /api/v2/tenant/organizations/{org_id}

表 3-74 路径参数

参数	是否必选	参数类型	描述
org_id	是	String	要删除的组织id（如果存在子组织无法删除）。

请求参数

表 3-75 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 400

表 3-76 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

删除组织，基于组织id删除指定组织。

```
DELETE https://{domain_name}/api/v2/tenant/organizations/{org_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

无

状态码

状态码	描述
204	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.4.4 查询组织详情

功能介绍

通过组织id查询组织详情。

URI

GET /api/v2/tenant/organizations/{org_id}

表 3-77 路径参数

参数	是否必选	参数类型	描述
org_id	是	String	组织id。

请求参数

表 3-78 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-79 响应 Body 参数

参数	参数类型	描述
org_id	String	组织id。
org_code	String	组织编号，全局唯一。
name	String	组织名称，所在层级下唯一。
parent_id	String	父组织id。
category	String	组织类型。

状态码： 400

表 3-80 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

查询组织详情，基于组织id查询指定组织详情。

```
GET https://{domain_name}/api/v2/tenant/organizations/{org_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "org_id" : "20220412142914549-1E50-B49C521A4",
  "parent_id" : "20220412105608948-3B83-D566C6D94",
  "name" : "测试机构",
  "category" : "department",
  "org_code" : "TestOrg"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.4.5 查询组织列表

功能介绍

查询指定组织及其下的子组织列表。

URI

GET /api/v2/tenant/organizations

表 3-81 Query 参数

参数	是否必选	参数类型	描述
all_child	否	Boolean	是否获取所有层级子组织。 缺省值：**false**
limit	是	Integer	每页多少条。 最小值：**10** 最大值：**100**
offset	是	Integer	第几页。 最小值：**0**
org_id	否	String	组织id。 当org_id=空，all_child=false，返回所有根组织（最高层级的组织）列表信息； 当org_id=空，all_child=true，返回除了根组织外，其他所有子组织列表信息； 当org_id=orgId，all_child=true，返回该组织以及该组织下所有层级子组织列表信息； 当org_id=orgId，all_child=false，返回该组织以及该组织的下一级组织列表信息。

请求参数

表 3-82 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-83 响应 Body 参数

参数	参数类型	描述
total	Long	组织总数。

参数	参数类型	描述
organizations	Array of **ResponseOrgInfo** objects	组织列表。

表 3-84 ResponseOrgInfo

参数	参数类型	描述
org_id	String	组织id。
org_code	String	组织编号，全局唯一。
name	String	组织名称，所在层级下唯一。
parent_id	String	父组织id。
category	String	组织类型。

状态码： 400

表 3-85 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

以分页形式查询组织列表，返回除了根组织外，其他所有子组织列表信息的前100条，不满100条时，则返回实际数量的信息结果。

```
GET https://{domain_name}/api/v2/tenant/organizations?org_id=&all_child=true&offset=0&limit=100

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "total" : 2,
  "organizations" : [ {
    "org_code" : "1000000",
    "org_id" : "20210619175242949-6040-CA7ECF...",
    "name" : "总部",
    "category" : "department",
    "parent_id" : null
```

```
 }, {
   "org_code" : "1000001",
   "org_id" : "20210623103509267-6ABA-201FFC...",
   "name" : "子部门",
   "category" : "department",
   "parent_id" : "20210619175242949-6040-CA7ECF..."
 } ]
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.5 应用机构管理

3.1.5.1 新增应用机构

功能介绍

新增应用机构。

URI

POST /api/v2/tenant/applications/{application_id}/organizations

表 3-86 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。

请求参数

表 3-87 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-88 请求 Body 参数

参数	是否必选	参数类型	描述
org_code	是	String	应用机构编码，可输入中英文、数字、下划线和中划线。 最大长度：**64**
name	是	String	应用机构名称，可输入中英文、数字、空格、中划线、下划线和&。 最大长度：**100**
parent_id	否	String	创建应用根机构不需要传，创建应用子机构需要传父机构id。

响应参数

状态码： 201

表 3-89 响应 Body 参数

参数	参数类型	描述
org_id	String	应用机构id。

状态码： 400

表 3-90 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

- 新增根机构，机构编码为10000，机构名称为总部。

```
POST https://{domain_name}/api/v2/tenant/applications/{application_id}/organizations
```

```
Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
  "org_code":"10000",
  "name":"总部",
  "parent_id": ""
}
```

- 新增子机构，机构编码为10001，机构名称为开发组，父机构id为20210623103520050-C5AF-DD1A97...。

```
POST https://{domain_name}/api/v2/tenant/applications/{application_id}/organizations

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
  "org_code":"10001",
  "name":"开发组",
  "parent_id":"20210623103520050-C5AF-DD1A97..."
}
```

响应示例

状态码： 201

请求成功。

```
{
  "org_id" : "20210623103520050-C5AF-DD1A97..."
}
```

状态码

状态码	描述
201	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.5.2 修改应用机构

功能介绍

修改应用机构。

URI

PUT /api/v2/tenant/applications/{application_id}/organizations/{org_id}

表 3-91 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。
org_id	是	String	机构id。

请求参数

表 3-92 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-93 请求 Body 参数

参数	是否必选	参数类型	描述
name	否	String	机构名称，为空时默认不修改，可输入中英文、数字、空格、中划线、下划线和&。 最大长度：**100**
parent_id	否	String	父机构id。

响应参数

状态码： 200

表 3-94 响应 Body 参数

参数	参数类型	描述
org_id	String	应用机构id。

状态码： 400

表 3-95 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和机构id修改机构属性，名称为开发组，父机构id为20201027162527852-B712-D040F4...。

```
PUT https://{domain_name}/api/v2/tenant/applications/{application_id}/organizations/{org_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
  "name":"开发组",
  "parent_id":"20201027162527852-B712-D040F4..."
}
```

响应示例

状态码： 200

请求成功。

```
{
  "org_id" : "20210623103520050-C5AF-DD1A9770E"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.5.3 删除应用机构

功能介绍

删除应用机构。

URI

DELETE /api/v2/tenant/applications/{application_id}/organizations/{org_id}

表 3-96 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。
org_id	是	String	应用机构id。

请求参数

表 3-97 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 400

表 3-98 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和机构id删除指定的应用机构。

```
DELETE https://{domain_name}/api/v2/tenant/applications/{application_id}/organizations/{org_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

无

状态码

状态码	描述
204	请求成功。

状态码	描述
400	参数无效。

错误码

请参见错误码。

3.1.5.4 查询应用机构详情

功能介绍

查询应用机构详情。

URI

GET /api/v2/tenant/applications/{application_id}/organizations/{org_id}

表 3-99 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。
org_id	是	String	应用机构id。

请求参数

表 3-100 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-101 响应 Body 参数

参数	参数类型	描述
org_id	String	应用机构id。

参数	参数类型	描述
org_code	String	应用机构编码。
name	String	应用机构名。
parent_id	String	父机构id。

状态码： 400

表 3-102 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和机构id查询指定机构的详情。

```
GET https://{domain_name}/api/v2/tenant/applications/{application_id}/organizations/{org_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "org_id" : "20210623103520050-C5AF-DD1A97...",
  "org_code" : "10000",
  "name" : "总部",
  "parent_id" : null
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.5.5 查询应用机构列表

功能介绍

查询一个应用被授权访问的机构列表

URI

GET /api/v2/tenant/applications/{application_id}/organizations

表 3-103 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。

表 3-104 Query 参数

参数	是否必选	参数类型	描述
offset	是	Integer	第几页。 最小值：**0**
limit	是	Integer	每页多少条。 最小值：**10** 最大值：**100**

请求参数

表 3-105 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-106 响应 Body 参数

参数	参数类型	描述
total	Long	应用机构总数。
organizations	Array of **ApplicationOrg** objects	机构列表。

表 3-107 ApplicationOrg

参数	参数类型	描述
org_id	String	应用机构id。
org_code	String	应用机构编码。
name	String	应用机构名。
parent_id	String	父机构id。

状态码： 400

表 3-108 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id分页查询应用中的机构列表中的前100条数据，如不满100条，则返回实际数量的数据。

```
GET https://{domain_name}/api/v2/tenant/applications/{application_id}/organizations?offset=0&limit=100

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "total" : 1,
  "organizations" : [ {
    "org_id" : "20210623103520050-C5AF-DD1A97...",
    "org_code" : "10000",
    "name" : "总部",
```

```
    "parent_id" : null
  }, {
    "org_id" : "20210619175409400-BFA4-63FA63...",
    "org_code" : "10001",
    "name" : "开发组",
    "parent_id" : "20210623103520050-C5AF-DD1A97..."
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.6 应用帐号管理

3.1.6.1 新增应用帐号

功能介绍

为用户创建应用帐号并授权。

URI

POST /api/v2/tenant/applications/{application_id}/accounts/basic-account

表 3-109 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。

请求参数

表 3-110 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-111 请求 Body 参数

参数	是否必选	参数类型	描述
user_id	是	String	应用帐号关联的授权用户id。
account_name	否	String	应用帐号名，为空默认为用户名。
name	否	String	应用帐号名称。
org_code	否	String	应用机构编码。
password	否	String	应用帐号密码。
disabled	否	Boolean	应用帐号是否禁用，为空默认为非禁用。
extension	否	Object	自定义扩展属性，需要在应用“对象模型”—“应用帐号模型”自定义。

响应参数

状态码： 201

表 3-112 响应 Body 参数

参数	参数类型	描述
account_id	String	应用帐号id。

状态码： 400

表 3-113 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

创建指定应用的应用账号并关联指定用户，账号名为zhangshan，账号名称为zs，关联用户的user_id为20220331164602949-904C-D475B60AE，应用账号为启用状态。

```
POST https://{domain_name}/api/v2/tenant/applications/{application_id}/accounts/basic-account

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
    "account_name":"zhangsan",
    "user_id":"20220331164602949-904C-D475B60AE",
    "name":"zs",
    "org_code":"",
    "password":"",
    "disabled":false,
    "extension":{}
}
```

响应示例

状态码： 201

请求成功。

```
{
  "account_id" : "20210517100458591-6F1C-965A4C..."
}
```

状态码

状态码	描述
201	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.6.2 更新应用帐号

功能介绍

更新应用帐号。

URI

PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}

表 3-114 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。

参数	是否必选	参数类型	描述
account_id	是	String	应用帐号id。

请求参数

表 3-115 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-116 请求 Body 参数

参数	是否必选	参数类型	描述
account_name	否	String	应用帐号名。
name	否	String	姓名。
org_code	否	String	应用机构编码。
password	否	String	密码。
disabled	否	Boolean	是否禁用。
extension	否	Object	自定义扩展属性，需要在应用“对象模型”—“应用帐号模型”自定义。

响应参数

状态码： 200

表 3-117 响应 Body 参数

参数	参数类型	描述
account_id	String	应用帐号id。

状态码： 400

表 3-118 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和应用账号id修改指定应用账号信息，应用账号名为Test02，姓名为Example，所属应用机构编码为10000，状态为启用。

```
PUT https://{domain_name}/api/v2/tenant/applications/{application_id}/accounts/{account_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
  "account_name": "Test02",
  "name":"Example",
  "org_code":"10000",
  "disabled":false
}
```

响应示例

状态码： 200

请求成功。

```
{
  "account_id" : "20210515151018087-2F92-6DBCA6..."
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.6.3 删除应用帐号

功能介绍

删除应用帐号。

URI

DELETE /api/v2/tenant/applications/{application_id}/accounts/{account_id}

表 3-119 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。
account_id	是	String	应用帐号id。

请求参数

表 3-120 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 400

表 3-121 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和应用账号id删除指定应用账号。

```
DELETE https://{domain_name}/api/v2/tenant/applications/{application_id}/accounts/{account_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

无

状态码

状态码	描述
204	请求成功。

状态码	描述
400	参数无效。

错误码

请参见错误码。

3.1.6.4 查询应用帐号详情

功能介绍

查询应用帐号详情。

URI

GET /api/v2/tenant/applications/{application_id}/accounts/{account_id}

表 3-122 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。
account_id	是	String	应用帐号id。

请求参数

表 3-123 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-124 响应 Body 参数

参数	参数类型	描述
id	String	应用帐号id。

参数	参数类型	描述
account_name	String	应用帐号名。
account_type	String	应用帐号类型。
name	String	姓名。
disabled	Boolean	是否禁用。
org_id	String	应用机构id。
roles	Array of **RolesInfo** objects	角色信息。
extension	Object	自定义扩展属性。

表 3-125 RolesInfo

参数	参数类型	描述
role_id	String	角色id。
role_code	String	角色代码。
role_name	String	角色名称。
privileges	Array of **PrivilegeInfo** objects	权限集合。

表 3-126 PrivilegeInfo

参数	参数类型	描述
privilege_id	String	权限ID。
privilege_code	String	权限代码。
privilege_name	String	权限名称。
resource_items	Array of **ResourceItem** objects	资源条目集合。

表 3-127 ResourceItem

参数	参数类型	描述
item_id	String	条目ID。
item_code	String	条目代码。
item_name	String	条目名称。
item_parentid	String	父条目ID。

状态码： 400

表 3-128 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和应用账号id查询指定应用账号详情。

```
GET https://{domain_name}/api/v2/tenant/applications/{application_id}/accounts/{account_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "id" : "5C00-C91355BC0",
  "account_name" : "example01",
  "name" : "示例1",
  "account_type" : "BASIC_ACCOUNT",
  "org_id" : "20201027162527852-B712-D040F4C71",
  "disabled" : false,
  "extension" : {
    "age" : "18"
  },
  "roles" : [ {
    "role_id" : "20220210090626329-AFAE-EB2862B3A",
    "role_code" : "admin",
    "role_name" : "管理员",
    "privileges" : [ {
      "privilege_id" : "20220210135202250-92C8-D89EC88C6",
      "privilege_code" : "demo_privilege",
      "privilege_name" : "示例权限",
      "resource_items" : [ {
        "item_id" : "20201027161283642-R582-7230F4E84",
        "item_code" : "demo_item",
        "item_name" : "示例条目",
```

```
      "item_parentid" : null
    } ]
  } ]
} ]
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.6.5 查询应用帐号列表

功能介绍

查询一个应用被授权访问的帐号列表。

URI

GET /api/v2/tenant/applications/{application_id}/accounts

表 3-129 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。

表 3-130 Query 参数

参数	是否必选	参数类型	描述
account_type	否	String	帐号类型，固定值，普通应用帐号（BASIC_ACCOUNT），孤儿帐号（ORPHAN_ACCOUNT），公共帐号（PUBLIC_ACCOUNT），不填查询所有。
offset	是	Integer	第几页。 最小值：**0**

参数	是否必选	参数类型	描述
limit	是	Integer	每页多少条。 最小值：**10** 最大值：**100**

请求参数

表 3-131 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-132 响应 Body 参数

参数	参数类型	描述
total	Long	应用帐号总数。
accounts	Array of **AccountDetail** objects	响应的用户列表。

表 3-133 AccountDetail

参数	参数类型	描述
id	String	应用帐号id。
account_name	String	应用帐号名。
account_type	String	应用帐号类型。
name	String	姓名。
disabled	Boolean	是否禁用。
org_id	String	应用机构id。

参数	参数类型	描述
roles	Array of **RolesInfo** objects	角色信息。
extension	Object	自定义扩展属性。

表 3-134 RolesInfo

参数	参数类型	描述
role_id	String	角色id。
role_code	String	角色代码。
role_name	String	角色名称。
privileges	Array of **PrivilegeInfo** objects	权限集合。

表 3-135 PrivilegeInfo

参数	参数类型	描述
privilege_id	String	权限ID。
privilege_code	String	权限代码。
privilege_name	String	权限名称。
resource_items	Array of **ResourceItem** objects	资源条目集合。

表 3-136 ResourceItem

参数	参数类型	描述
item_id	String	条目ID。
item_code	String	条目代码。
item_name	String	条目名称。
item_parentid	String	父条目ID。

状态码： 400

表 3-137 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id分页查询应用下的普通应用账号列表，返回查询结果的前100条数据，如不满100条，则返回实际数量的结果。

```
GET https://{domain_name}/api/v2/tenant/applications/{application_id}/accounts?
account_type=BASIC_ACCOUNT&offset=0&limit=100

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "total" : 1,
  "accounts" : [ {
    "id" : "20210621095850460-5A8A-03D94B540",
    "account_name" : "Test01",
    "account_type" : "BASIC_ACCOUNT",
    "name" : "Example01",
    "disabled" : false,
    "org_id" : "20210621095942194-560B-57E3CC...",
    "extension" : { }
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.6.6 启用应用帐号

功能介绍

启用应用帐号。

URI

PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}/enable

表 3-138 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。
account_id	是	String	应用帐号id。

请求参数

表 3-139 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-140 响应 Body 参数

参数	参数类型	描述
account_id	String	应用帐号id。

状态码： 400

表 3-141 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和应用账号id启用指定应用账号。

```
PUT https://{domain_name}/api/v2/tenant/applications/{application_id}/accounts/{account_id}/enable

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "account_id" : "20210515151018087-2F92-6DBCA6..."
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.6.7 禁用应用帐号

功能介绍

禁用应用帐号。

URI

PUT /api/v2/tenant/applications/{application_id}/accounts/{account_id}/disable

表 3-142 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。
account_id	是	String	应用帐号id。

请求参数

表 3-143 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-144 响应 Body 参数

参数	参数类型	描述
account_id	String	应用帐号id。

状态码： 400

表 3-145 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和应用账号id禁用指定应用账号。

```
PUT https://{domain_name}/api/v2/tenant/applications/{application_id}/accounts/{account_id}/disable

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "account_id" : "20210515151018087-2F92-6DBCA6..."
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.1.7 应用侧角色管理

3.1.7.1 新增应用侧角色

功能介绍

新增应用侧角色。

URI

POST /api/v2/tenant/applications/{application_id}/role

表 3-146 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。

请求参数

表 3-147 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-148 请求 Body 参数

参数	是否必选	参数类型	描述
code	是	String	角色代码，应用内唯一。 最大长度：**50**
name	否	String	角色名称。 最大长度：**32**

响应参数

状态码： 200

表 3-149 响应 Body 参数

参数	参数类型	描述
role_id	String	角色id。

状态码： 400

表 3-150 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id新增应用侧角色，角色代码为admin1,角色名称为管理员1。

```
POST https://{domain_name}/api/v2/tenant/applications/{application_id}/role

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
    "code": "admin1",
    "name": "管理员1"
}
```

响应示例

状态码： 200

角色id。

```
{
  "role_id" : "20220420140745089-23E4-DFF0A1900"
}
```

状态码

状态码	描述
200	角色id。
400	请求失败。

错误码

请参见错误码。

3.1.7.2 修改应用侧角色信息

功能介绍

修改应用侧角色信息。

URI

PUT /api/v2/tenant/applications/{application_id}/role/{role_id}

表 3-151 路径参数

参数	是否必选	参数类型	描述
role_id	是	String	角色id。
application_id	是	String	应用id。

请求参数

表 3-152 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-153 请求 Body 参数

参数	是否必选	参数类型	描述
name	是	String	应用侧角色名称

响应参数

状态码： 200

表 3-154 响应 Body 参数

参数	参数类型	描述
role_id	String	角色id。

状态码： 400

表 3-155 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和角色id修改应用侧角色，修改角色名称为管理员2。

```
PUT  https://{domain_name}/api/v2/tenant/applications/{application_id}/role/{role_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
  "name": "管理员2"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "role_id" : "20220420140745089-23E4-DFF0A1900"
}
```

状态码

状态码	描述
200	请求成功。
400	请求失败。

错误码

请参见错误码。

3.1.7.3 删除应用侧角色

功能介绍

删除应用侧角色。

URI

DELETE /api/v2/tenant/applications/{application_id}/role/{role_id}

表 3-156 路径参数

参数	是否必选	参数类型	描述
role_id	是	String	角色id。
application_id	是	String	应用id。

请求参数

表 3-157 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 400

表 3-158 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和角色id删除指定应用侧角色。

```
DELETE https://{domain_name}/api/v2/tenant/applications/{application_id}/role/{role_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

无

状态码

状态码	描述
200	请求成功。
400	请求失败。

错误码

请参见错误码。

3.1.7.4 查询应用侧角色详情

功能介绍

查询应用侧角色详情。

URI

GET /api/v2/tenant/applications/{application_id}/role/{role_id}

表 3-159 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。
role_id	是	String	角色id。

请求参数

表 3-160 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-161 响应 Body 参数

参数	参数类型	描述
id	String	角色id
code	String	角色code
name	String	角色名称
createdAt	String	创建时间
updatedAt	String	修改时间

状态码： 400

表 3-162 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和角色id查询指定应用侧角色详情。

```
GET https://{domain_name}/api/v2/tenant/applications/{application_id}/role/{role_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "id" : "20220210090626329-AFAE-EB2862B3A",
  "code" : "admin",
  "name" : "管理员",
  "createdAt" : "2022-02-10 09:06:26.333",
  "updatedAt" : "2022-02-10 09:06:26.333"
}
```

状态码

状态码	描述
200	请求成功。
400	请求失败。

错误码

请参见错误码。

3.1.7.5 查询应用侧角色列表

功能介绍

查询应用侧角色列表。

URI

GET /api/v2/tenant/applications/{application_id}/role-list

表 3-163 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。

表 3-164 Query 参数

参数	是否必选	参数类型	描述
offset	否	Integer	第几页。
limit	是	Integer	每页多少条。 最小值：**10** 最大值：**100**

请求参数

表 3-165 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

响应参数

状态码： 200

表 3-166 响应 Body 参数

参数	参数类型	描述
total	Integer	总数
offset	Integer	第几页
limit	Integer	每页多少条
roles	Array of **RoleInfoResult** objects	角色信息集合

表 3-167 RoleInfoResult

参数	参数类型	描述
id	String	角色id
code	String	角色code
name	String	角色名称
createdAt	String	创建时间
updatedAt	String	修改时间

状态码： 400

表 3-168 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id分页查询应用侧角色列表，返回查询结果的前10条，如不满10条，则返回实际数量的结果。

```
GET https://{domain_name}/api/v2/tenant/applications/{application_id}/role-list?offset=0&limit=10

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
```

响应示例

状态码： 200

请求成功。

```
{
  "total" : 3,
  "offset" : 0,
  "limit" : 10,
  "roles" : [ {
    "id" : "20220415170305200-EF22-C2404E358",
    "code" : "role1",
    "name" : "role1",
    "createdAt" : "2022-04-15 17:03:05.200",
    "updatedAt" : null
  }, {
    "id" : "20220415170305223-7193-A01122B37",
    "code" : "role2",
    "name" : "role2",
    "createdAt" : "2022-04-15 17:03:05.223",
    "updatedAt" : null
  }, {
    "id" : "20220420144449385-C66D-E8C1D1D79",
    "code" : "admin",
    "name" : "管理员",
    "createdAt" : "2022-04-20 14:44:49.385",
    "updatedAt" : null
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	请求失败。

错误码

请参见错误码。

3.1.7.6 新增应用侧角色成员

功能介绍

新增应用侧角色成员。

URI

POST /api/v2/tenant/applications/{application_id}/role-member

表 3-169 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。

请求参数

表 3-170 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-171 请求 Body 参数

参数	是否必选	参数类型	描述
role_id	是	String	角色id。
account_Ids	是	Array of strings	应用帐号id集合，最大50条。

响应参数

状态码： 200

表 3-172 响应 Body 参数

参数	参数类型	描述
success_list	Array of strings	成功列表
fail_list	Array of strings	失败列表

状态码： 400

表 3-173 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id新增应用侧角色成员，角色id为20220420144449385-C66D-E8C1D1D79，应用账号id集合为["20220415171558023-84A4-ED5C390B8", "20220414163425614-2FD6-CA9B208BE"]。

```
POST https://{domain_name}/api/v2/tenant/applications/{application_id}/role-member

{
  "role_id" : "20220420144449385-C66D-E8C1D1D79",
  "account_Ids" : [ "20220415171558023-84A4-ED5C390B8", "20220414163425614-2FD6-CA9B208BE" ]
}
```

响应示例

状态码： 200

应用帐号id列表。

```
{
  "success_list" : [ "20220415171558023-84A4-ED5C390B8", "20220414163425614-2FD6-CA9B208BE" ],
  "fail_list" : [ ]
}
```

状态码

状态码	描述
200	应用帐号id列表。
400	请求失败。

错误码

请参见错误码。

3.1.7.7 删除应用侧角色成员

功能介绍

删除应用侧角色成员。

URI

DELETE /api/v2/tenant/applications/{application_id}/role-member

表 3-174 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。

请求参数

表 3-175 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-176 请求 Body 参数

参数	是否必选	参数类型	描述
role_id	是	String	角色id。
account_Ids	是	Array of strings	应用帐号id集合，最大50条。

响应参数

状态码： 200

表 3-177 响应 Body 参数

参数	参数类型	描述
success_list	Array of strings	成功列表
fail_list	Array of strings	失败列表

状态码： 400

表 3-178 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id删除应用侧角色成员，应用侧角色id为20220420144449385-C66D-E8C1D1D79，应用账号id集合为["20220415171558023-84A4-ED5C390B8", "20220414163425614-2FD6-CA9B208BE"]。

```
DELETE https://{domain_name}/api/v2/tenant/applications/{application_id}/role-member

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
  "role_id": "20220420144449385-C66D-E8C1D1D79",
  "account_Ids": [
    "20220415171558023-84A4-ED5C390B8",
    "20220414163425614-2FD6-CA9B208BE"
  ]
}
```

响应示例

状态码： 200

应用帐号id列表。

```
{
  "success_list" : [ "20220415171558023-84A4-ED5C390B8", "20220414163425614-2FD6-CA9B208BE" ],
  "fail_list" : [ ]
}
```

状态码

状态码	描述
200	应用帐号id列表。

状态码	描述
400	请求失败。

错误码

请参见错误码。

3.1.7.8 查询应用侧角色成员列表

功能介绍

查询应用侧角色成员列表。

URI

GET /api/v2/tenant/applications/{application_id}/role-member-list/{role_id}

表 3-179 路径参数

参数	是否必选	参数类型	描述
application_id	是	String	应用id。
role_id	是	String	角色id。

请求参数

表 3-180 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。

表 3-181 请求 Body 参数

参数	是否必选	参数类型	描述
offset	是	Integer	第几页。 最小值：**0**

参数	是否必选	参数类型	描述
limit	是	Integer	每页多少条。 最小值：**10** 最大值：**100**

响应参数

状态码： 200

表 3-182 响应 Body 参数

参数	参数类型	描述
total	Integer	总数
offset	Integer	第几页
limit	Integer	每页多少条
role_members	Array of **RoleMemberInfo** objects	角色成员信息集合

表 3-183 RoleMemberInfo

参数	参数类型	描述
id	String	应用帐号id
account_name	String	应用帐号名
name	String	应用帐号名称
org_id	String	应用机构id
disabled	Boolean	是否禁用
account_type	String	应用帐号类型
extension	Object	自定义扩展属性

状态码： 400

表 3-184 响应 Body 参数

参数	参数类型	描述
error_code	String	错误编号。
error_msg	String	错误详情。

请求示例

根据应用id和角色id分页查询应用侧角色成员列表，返回查询结果前10条数据，如不满10条，则返回实际数量的结果。

```
GET https://{domain_name}/api/v2/tenant/applications/{application_id}/role-member-list/{role_id}

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...

{
  "offset": "0",
  "limit": "10",
}
```

响应示例

状态码： 200

请求成功。

```
{
  "total" : 1,
  "offset" : 0,
  "limit" : 10,
  "role_members" : [ {
    "id" : "20220210090626329-AFAE-EB2862B3A",
    "account_name" : "adminAcc",
    "account_type" : "1",
    "name" : "管理员",
    "org_id" : "20220210135202250-92C8-D89EC88C6",
    "disabled" : false,
    "extension" : null
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	请求失败。

错误码

请参见错误码。

3.2 用户类接口

3.2.1 如何调用 API

3.2.1.1 构造请求

本节介绍API请求的组成，并以调用OneAccess登录登出接口中的“用户名密码登录”为例说明如何调用API，用户名密码登录，正常调用成功会返回用户的session_token，可用来获取用户信息等。

前提条件

调用API前，需要获取管理员在OneAccess管理门户中已添加应用的通用信息中的ClientId，用以调用API实现相关接口功能。

请求 URI

OneAccess请求URI由如下部分组成。

{URI-scheme} :// {domain_name} / {resource-path}

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。

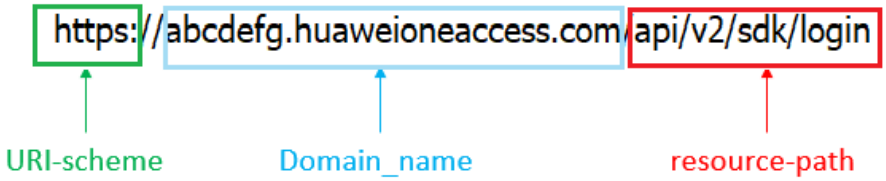
表 3-185 URI 中的参数说明

参数	描述
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OneAccess服务API需要使用用户访问域名，获取方法请参见获取用户访问域名。
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“用户名密码登录”API的resource-path为“/api/v2/sdk/login”。

例如您需要获取用户访问域名为“abcdefg.huaweioneaccess.com”的实例的session_token，则需使用用户访问域名“abcdefg.huaweioneaccess.com”，并在用户名密码登录的URI部分找到resource-path（ /api/v2/sdk/login ），拼接起来如下所示。

```
https://abcdefg.huaweioneaccess.com/api/v2/sdk/login
```

图 3-2 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在同一个实例也相同，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 3-186 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。

在用户名密码登录的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://abcdefg.huaweioneaccess.com/api/v2/sdk/login
```

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。例如用户Agent信息，应用标识等。

详细的通用请求消息头字段请参见**表3-187**。

表 3-187 通用请求消息头

名称	描述	是否必选	示例
X-operating-sys-version	调用方操作系统版本。	是	Android 10
X-device-fingerprint	调用方设备指纹。	是	156aysdna213sc50
X-device-ip	调用方IP。	否	10.10.10.1

名称	描述	是否必选	示例
X-agent	用户Agent信息。	是	Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L	国际化语言设置。	否	zh
X-client-id	应用标识，注册应用后分配的ClientId。	是	DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id	租户id，ISV应用调用则为必填。	否	08f770f51f80d2f40f38c00cb199fd20
X-signature	签名信息，用于判断用户登录状态，非所有接口需要，可参考具体接口说明，构造方式可参考**session token签名**。	否	D0JeOUuVqU8Ixvl0xrmewQRk4AuGZrtk1RfBxueNKUrNPpgSbXrYnzw...

对于获取用户名密码登录接口，添加消息头后的请求如下所示。

```
POST https://abcdefg.huaweioneaccess.com/api/v2/sdk/login
X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21
```

请求消息体（可选）

请求消息体通常以结构化格式（如JSON或XML）发出，传递除请求消息头之外的内容。若请求消息体中的参数支持中文，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，并不是每个接口都需要有请求消息体（或者消息体为空），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。

对于用户名密码登录接口，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，其中***UserName***为用户名，***PassWord***为密码。

```
POST https://abcdefg.huaweioneaccess.com/api/v2/sdk/login
X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36
```

```
(KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "user_name": "UserName",
  "password": "PassWord"
}
```

到此，这个请求需要的内容就具备了，您可以使用**curl**、**Postman**或直接编写代码等方式发送请求调用API。对于用户名密码登录接口，返回的响应消息体中“session_token”就是登录成功的凭证。有了session_token之后，您就可以用来获取用户信息等。

3.2.1.2 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

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。

对于用户名密码登录接口，如果调用后返回状态码为“200”，则表示请求成功。

响应消息头（可选）

对应请求消息头，响应同样也有消息头，如“Content-type”。

响应消息体（可选）

响应消息体通常以结构化格式（如JSON或XML）返回，传递除响应消息头之外的内容。

对于用户名密码登录接口，返回如下消息体。

```
{
  "session_token" : "bts**********************************2VO",
  "expire" : 604800,
  "status" : "SUCCESS"
}
```

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": "LOGIN.0002",
    "error_msg": "Invalid account name or password. Remaining attempts: 8."
}
```

其中，error_code表示错误类型，error_msg表示错误描述信息。

3.2.2 系统接口

3.2.2.1 获取服务器时间

功能介绍

获取服务器时间。

URI

GET /api/v2/sdk/server-date

请求参数

表 3-188 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 200

表 3-189 响应 Body 参数

参数	参数类型	描述
timestamp	String	服务端时间戳。

状态码： 400

表 3-190 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

获取服务器时间。请求头配置调用方系统为Android 10，调用方设备指纹为156aysdna213sac，调用方ip为10.10.10.1，应用标识为注册应用时分配的ClientId。

```
GET https://{domain_name}/api/v2/sdk/server-date

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21
```

响应示例

状态码： 200

请求成功。

```
{
  "timestamp" : "1628496895102"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.2.2 获取公钥

功能介绍

获取公钥，用于调用服务端接口时，对敏感信息进行加密操作（每个应用拥有不同的公钥，有且只有一个）。

URI

GET /api/v2/sdk/public-key

请求参数

表 3-191 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 200

表 3-192 响应 Body 参数

参数	参数类型	描述
public_key	String	应用的公钥

状态码： 400

表 3-193 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

获取加密公钥。请求头配置调用方系统为Android 10，调用方设备指纹为156aysdna213sac，调用方ip为10.10.10.1，应用标识为注册应用时分配的ClientId。

```
GET https://{domain_name}/api/v2/sdk/public-key

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21
```

响应示例

状态码： 200

请求成功。


```
{
  "public_key" : "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAibkfo0k5yU8ZEt6D5Rl6\nmNGGlGKyl1dO237iEUtl
ttf48YUBMrruAvINc68cT5hwHoQdZDAXq6YaK6j+QkmD\nOr/
wl5qUllrqrS5jMsyx80bWMkkJDmnV8WJWVlqmaEu1XJUTOinOlXHDwQtougP+
\nq6Ai0gQC395QESR5t9WKCGIFMoWuEesCj1K8YUW3lSBojiz+vCYQSdy0xTOC3uWz\nxds4mDe4qeX+9wSH
+XgFPCu/YpufNz+1iSBtALvpOGORT+zkPpt+0c7zvEpy+pgi\nsx0/
aV5vA6S481ZCYZR3gzG4xthVuS0o022UGdr5RNy6SxvoIrx09JG2RvhdWsxW\n7wIDAQAB\n-----END PUBLIC
KEY-----"
}
```


状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.3 注册

3.2.3.1 使用手机号和短信验证码注册

功能介绍

使用手机号和短信验证码注册。

URI

POST /api/v2/sdk/register/mobile-verify-code

请求参数

表 3-194 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-195 请求 Body 参数

参数	是否必选	参数类型	描述
user_name	否	String	用户名。
name	否	String	姓名。
mobile	是	String	手机号。
verify_code	是	String	短信验证码。
email	否	String	邮箱。
pwd	否	String	密码。
head_img	否	String	头像，填写url地址。
attr_gender	否	String	性别。 枚举值： ● **unknown：保密** ● **male：男性** ● **female：女性**
attr_birthday	否	String	生日，格式为yyyy-MM-dd。
attr_nick_name	否	String	昵称。
first_name	否	String	名字。
middle_name	否	String	中间名。
last_name	否	String	姓氏。
extension	否	Object	自定义扩展属性。

响应参数

状态码： 200

表 3-196 响应 Body 参数

参数	参数类型	描述
status	String	返回结果。 枚举值： ● **SUCCESS：登录成功** ● **ACCESS_DENIED：拒绝访问**
expire	Integer	session_token有效期，单位为秒，有效期内可使用session_token获取ticket。

参数	参数类型	描述
session_token	String	用户session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。

状态码： 400

表 3-197 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

使用手机号和短信验证码注册用户。用户名为zhangsan，姓名为张三，手机号为12345678901，短信验证码为1234，邮箱为12345678901@example.com，密码为Q******3。自定义扩展字段年龄值为18。

```
POST https://{domain_name}/api/v2/sdk/register/mobile-verify-code

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "user_name": "zhangsan",
  "name": "张三",
  "mobile": "12345678901",
  "verify_code": "1234",
  "email": "12345678901@example.com",
  "pwd": "Q******3",
  "head_img": "
  https://thirdwx.qlogo.cn/mmopen/vi_32/
Q0j4TwGTfTIQ8QOTSn3y4cYHLlMC3sv6RCBmeMkxtOog47Zr3v2Afbqc2bmP0WibUIUskX39eJlJ",
  "attr_gender": "male",
  "attr_birthday": "2022-02-17",
  "attr_nick_name": "张三",
  "first_name": "zhangsan",
  "middle_name": "zhangsan",
  "last_name": "zhangsan",
  "extension": {
    "age": "18"
  }
}
```

响应示例

状态码： 200

请求成功。

```
{
  "status" : "SUCCESS",
  "expire" : 43200,
  "session_token" : "LGT******sqa"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.4 验证码

3.2.4.1 获取图形验证码

功能介绍

获取图形验证码。

URI

GET /api/v2/sdk/captcha

请求参数

表 3-198 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。

参数	是否必选	参数类型	描述
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 200

表 3-199 响应 Body 参数

参数	参数类型	描述
captchaId	String	验证码ID。
projectCode	String	项目编码，当前不支持，固定返回null。
captchaOriginalPath	String	验证码原始路径，当前不支持，固定返回null。
captchaFontType	String	验证码字体类型，当前不支持，固定返回null。
captchaFontSize	String	验证码字体大小，当前不支持，固定返回null。
secretKey	String	秘钥，当前不支持，固定返回null。
originalImageBase64	String	原生图片base64。
point	String	滑块点选坐标。

参数	参数类型	描述
jigsawImageBase64	String	滑块图片base64。
wordList	String	点选文字。
pointList	String	点选坐标。
pointJson	String	点坐标（base64编码传输）。
token	String	每次请求验证码的唯一标识。
result	String	校验结果。
captchaVerification	String	后台二次校验参数。

状态码： 400

表 3-200 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

获取图形验证码。

```
GET https://{domain_name}/api/v2/sdk/captcha

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21
```

响应示例

状态码： 200

请求成功。


```
{
  "captchaId" : null,
  "projectCode" : null,
  "captchaOriginalPath" : null,
  "captchaFontType" : null,
  "captchaFontSize" : null,
  "secretKey" : "yMX******hmq",
  "originalImageBase64" : "iVBORw0KGgoAAAANSUhEUgAAATYABj/WRVk78AAAAASUVORK5CYII=",
```

```
  "point" : null,
  "jigsawImageBase64" : "iVBORw0KGgoAAAANSUhEUgADcAAAAASUVORK5CYII=",
  "wordList" : null,
  "pointList" : null,
  "pointJson" : null,
  "token" : "389******fd1",
  "result" : false,
  "captchaVerification" : null
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.4.2 校验图形验证码

功能介绍

校验图形验证码。

URI

POST /api/v2/sdk/captcha/verify

请求参数

表 3-201 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。

参数	是否必选	参数类型	描述
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-202 请求 Body 参数

参数	是否必选	参数类型	描述
point_json	是	String	坐标信息，y轴固定值5.0。
token	是	String	获取图形验证码返回的token。
sender	是	String	发送方（手机号、邮箱）。

响应参数

状态码： 200

表 3-203 响应 Body 参数

参数	参数类型	描述
captcha_token	String	图形验证码校验通过的凭证。

状态码： 400

表 3-204 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

校验图形验证码。坐标信息为{"x":237.0,"y":5.0}，token为71d******635，发送方手机号为12345678901。

```
POST https://{domain_name}/api/v2/sdk/captcha/verify

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "point_json": "{\"x\":237.0,\"y\":5.0}",
  "token": "71d******635",
  "sender": "12345678901"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "captcha_token" : "71d******635---{\"x\":237.0,\"y\":5.0}"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.4.3 获取国际区号

功能介绍

获取支持的国际区号。

URI

GET /api/v2/sdk/country-codes

请求参数

表 3-205 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 200

表 3-206 响应 Body 参数

参数	参数类型	描述
phoneAreaCodeDefinitions	Array of **PhoneAreaCodeDefinitionsResult** objects	支持的区号详情。
preferredAreaCode	String	当前管理门户配置的首选国际区号。

表 3-207 PhoneAreaCodeDefinitionsResult

参数	参数类型	描述
areaCode	String	国际电话区号。
displayMapping	**DisplayMapping** object	多语言显示名映射。
countryCode	String	国家地区代码。
mobileRegex	String	手机号格式正则。
areaCodeSuffixes	String	国际电话区号后缀。

表 3-208 DisplayMapping

参数	参数类型	描述
zh-TW	String	中文繁体描述。
en	String	英文描述。
zh-CN	String	中文简体描述。

状态码： 400

表 3-209 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

获取支持的国际区号。

```
GET https://{domain_name}/api/v2/sdk/country-codes

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21
```

响应示例

状态码： 200

请求成功。


```
{
  "phoneAreaCodeDefinitions" : [ {
    "areaCode" : "86",
    "displayMapping" : {
      "zh-TW" : "中國大陸",
      "en" : "China",
      "zh-CN" : "中国大陆"
    },
    "countryCode" : "CN",
    "mobileRegex" : "^(\\+86){0,1}\\-?1\\d{10}$",
    "areaCodeSuffixes" : [ ]
  }, {
    "areaCode" : "852",
    "displayMapping" : {
      "zh-TW" : "中國香港",
      "en" : "Hong Kong",
      "zh-CN" : "中国香港"
    },
    "countryCode" : "HK",
    "mobileRegex" : "^(\\+852){1}\\-?0{0,1}[1,4,5,6,7,8,9](?:\\d{7}|\\d{8}|\\d{12})$",
    "areaCodeSuffixes" : [ ]
  }, {
    "areaCode" : "886",
    "displayMapping" : {
      "zh-TW" : "中國臺灣",
      "en" : "Taiwan",
      "zh-CN" : "中国台湾"
    },
    "countryCode" : "TW",
    "mobileRegex" : "^(\\+886){1}\\-?[6,7,9](?:\\d{7}|\\d{8})$",
    "areaCodeSuffixes" : [ ]
  }, {
    "areaCode" : "853",
    "displayMapping" : {
      "zh-TW" : "中國澳門",
      "en" : "Macau",
      "zh-CN" : "中国澳门"
    },
    "countryCode" : "MO",
    "mobileRegex" : "^(\\+853){1}\\-?0{0,1}[1,4,5,6,7,8,9](?:\\d{7}|\\d{8}|\\d{12})$",
    "areaCodeSuffixes" : [ ]
  }, {
    "areaCode" : "93",
    "displayMapping" : {
      "zh-TW" : "阿富汗",
      "en" : "Afghanistan",
      "zh-CN" : "阿富汗"
```

```
    },
    "countryCode" : "AF",
    "mobileRegex" : "^(\\+93){1}\\-\\d{6,11}",
    "areaCodeSuffixes" : [ ]
  } ],
  "preferredAreaCode" : "CN"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.4.4 发送短信验证码

功能介绍

发送短信验证码。

URI

POST /api/v2/sdk/sms/send

请求参数

表 3-210 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。

参数	是否必选	参数类型	描述
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-211 请求 Body 参数

参数	是否必选	参数类型	描述
mobile	是	String	手机号。
type	是	String	发送场景。 枚举值： ● **REGISTER_SMS：注册短信** ● **LOGIN_SMS：登录短信** ● **FORGET_PWD_SMS：找回密码短信** ● **BIND_MOBILE_SMS：绑定短信** ● **UPDATE_MOBILE_SMS：修改手机号短信** ● **OTP_REST_SMS：二次认证短信**
captcha_token	是	String	图形验证码校验通过的凭证。

响应参数

状态码： 400

表 3-212 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

发送短信验证码，给指定手机号12345678901用于绑定手机号，图形验证码校验通过凭证为71d******635---{"x":237.0,"y":5.0}。

```
POST https://{domain_name}/api/v2/sdk/sms/send

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "mobile": "12345678901",
  "type": "BIND_MOBILE_SMS",
  "captcha_token": "71d******635---{\"x\":237.0,\"y\":5.0}"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.5 登录登出

3.2.5.1 用户名密码登录

功能介绍

用户名密码登录，正常调用成功会返回用户的session_token，开启密码过期检查或二次认证会返回state_token，失败返回失败信息。

URI

POST /api/v2/sdk/login

请求参数

表 3-213 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-214 请求 Body 参数

参数	是否必选	参数类型	描述
user_name	是	String	用户名。
password	是	String	密码。

响应参数

状态码： 200

表 3-215 响应 Body 参数

参数	参数类型	描述
status	String	登录流程状态标识。 枚举值： ● **SUCCESS：登录成功** ● **PASSWORD_WARN：密码快过期，需要调用密码过期强制修改密码接口设置密码** ● **PASSWORD_EXPIRED：密码已过期，需要调用密码过期强制修改密码接口设置密码** ● **ACCESS_DENIED：拒绝访问** ● **MFA_AUTH：登录成功但需要进行二次认证，需要调用根据state_Token获取手机号接口、手机和短信验证码二次认证接口进行二次认证**
session_token	String	用户session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。
expire	Integer	session_token有效期，单位为秒，有效期内可以使用session_token获取sso_ticket。
state_token	String	用户带有状态的令牌。
data	String	返回说明。

状态码： 400

表 3-216 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

用户名密码登录。用户名为test01，用户密码为1******6。

```
POST https://{domain_name}/api/v2/sdk/login

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "user_name": "test01",
  "password": "1******6"
}
```

响应示例

状态码： 200

成功匹配用户返回session_token。

```
{
  "session_token" : "bts******2VO",
  "expire" : 604800,
  "status" : "SUCCESS"
}
```

状态码

状态码	描述
200	成功匹配用户返回session_token。
400	参数无效。

错误码

请参见错误码。

3.2.5.2 手机短信验证码登录

功能介绍

手机短信验证码登录。

URI

POST /api/v2/sdk/login/mobile-verify-code

请求参数

表 3-217 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-218 请求 Body 参数

参数	是否必选	参数类型	描述
mobile	是	String	接收验证码的手机号。
verify_code	是	String	接收到的验证码。

响应参数

状态码： 200

表 3-219 响应 Body 参数

参数	参数类型	描述
status	String	登录流程状态标识。 枚举值： ● **SUCCESS：登录成功** ● **PASSWORD_WARN：密码快过期，需要调用密码过期强制修改密码接口设置密码** ● **PASSWORD_EXPIRED：密码已过期，需要调用密码过期强制修改密码接口设置密码** ● **ACCESS_DENIED：拒绝访问** ● **MFA_AUTH：登录成功但需要进行二次认证，需要调用根据state_Token获取手机号接口、手机和短信验证码二次认证接口进行二次认证**
session_token	String	用户session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。
expire	Integer	session_token有效期，单位为秒，有效期内可以使用session_token获取sso_ticket。
state_token	String	用户带有状态的令牌。
data	String	返回说明。

状态码： 400

表 3-220 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

手机短信验证码登录。接收验证码的手机号为12345678901，验证码为232326。

```
POST https://{domain_name}/api/v2/sdk/login/mobile-verify-code

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36
(KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "mobile": "12345678901",
  "verify_code": "232326"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "status" : "SUCCESS",
  "session_token" : "bts******2VO",
  "expire" : 604800
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.5.3 微信登录

功能介绍

微信登录。

URI

POST /api/v2/sdk/login/wechat

请求参数

表 3-221 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-222 请求 Body 参数

参数	是否必选	参数类型	描述
code	是	String	授权码（app拉起微信应用的时候微信应用提供的授权码）。

响应参数

状态码： 200

表 3-223 响应 Body 参数

参数	参数类型	描述
status	String	登录流程状态标识。 枚举值： ● **SUCCESS：登录成功** ● **SOCIAL_BIND：绑定流程，需要调用验证码和社交帐号登录绑定手机号相关接口完成绑定流程** ● **USER_REGISTER：自动注册绑定流程，需要调用验证码和社交帐号注册并绑定手机号相关接口完成注册绑定流程** ● **ACCESS_DENIED：拒绝访问** ● **MFA_AUTH：登录成功但需要进行二次认证，需要调用验证码和二次认证相关接口进行二次认证**
session_token	String	用户session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。
expire	Integer	session_token有效期，单位为秒，有效期内可以使用session_token获取sso_ticket。
state_token	String	用户带有状态的令牌。
data	String	返回说明。

状态码： 400

表 3-224 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

微信登录。微信应用提供的授权码为ad12sasdsfe3dfdg3sc。

```
POST https://{domain_name}/api/v2/sdk/login/wechat

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "code": "ad12sasdsfe3dfdg3sc"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "status" : "SUCCESS",
  "session_token" : "bts******2VO",
  "expire" : 604800
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.5.4 支付宝登录

功能介绍

支付宝登录。

URI

POST /api/v3/sdk/login/alipay

请求参数

表 3-225 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-226 请求 Body 参数

参数	是否必选	参数类型	描述
code	是	String	授权码（app拉起支付宝应用的时候支付宝应用提供的授权码）。

响应参数

状态码： 200

表 3-227 响应 Body 参数

参数	参数类型	描述
status	String	登录流程状态标识。 枚举值： ● **SUCCESS：登录成功** ● **SOCIAL_BIND：绑定流程，需要调用验证码和社交帐号登录绑定手机号相关接口完成绑定流程** ● **USER_REGISTER：自动注册绑定流程，需要调用验证码和社交帐号注册并绑定手机号相关接口完成注册绑定流程** ● **ACCESS_DENIED：拒绝访问** ● **MFA_AUTH：登录成功但需要进行二次认证，需要调用验证码和二次认证相关接口进行二次认证**
session_token	String	用户session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。
expire	Integer	session_token有效期，单位为秒，有效期内可以使用session_token获取sso_ticket。
state_token	String	用户带有状态的令牌。
data	String	返回说明。

状态码： 400

表 3-228 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

支付宝登录。支付宝提供的授权码为ad12sasdsfe3dfdg3sc。

```
POST https://{domain_name}/api/v2/sdk/login/alipay

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36
(KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "code": "ad12sasdsfe3dfdg3sc"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "status" : "SUCCESS",
  "session_token" : "bts******2VO",
  "expire" : 604800
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.5.5 退出登录

功能介绍

退出登录。

URI

GET /api/v2/sdk/logout

请求参数

表 3-229 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-signature	是	String	加密数据为session_token=xxx&timestamp=xxx&nonce=xxx，其中：session_token为会话凭证，timestamp表示当前时间戳，nonce表示当前时间戳的16进制，加密方式为RSA公钥加密。当前时间戳可调用获取服务器时间接口获取，加密公钥可调用获取公钥接口获取。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 400

表 3-230 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

退出登录。

```
GET https://{domain_name}/api/v2/sdk/logout

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-signature:D0JeOUuVqU8Ixvl0xrmewQRk4AuGZrtk1RfBxueNKUrNPpgSbXrYnzw...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21
```

响应示例

无

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.6 社交帐号

3.2.6.1 社交帐号登录绑定手机号

功能介绍

在管理门户配置的认证源选择未关联用户为绑定时，用于社交帐号绑定手机号操作。

URI

POST /api/v2/sdk/social/bind

请求参数

表 3-231 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-state-token	是	String	临时令牌。当认证源配置为绑定时，用于社交帐号绑定手机号操作，需要传入对应的state_token，绑定成功返回用户session_token，绑定失败返回失败信息。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-232 请求 Body 参数

参数	是否必选	参数类型	描述
mobile	是	String	接收验证码的手机号。
verify_code	是	String	接收到的验证码。

响应参数

状态码： 200

表 3-233 响应 Body 参数

参数	参数类型	描述
status	String	登录流程状态标识，返回SUCCESS表示登录成功。
session_token	String	用户session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。
expire	Integer	session_token有效期，单位为秒，有效期内可以使用session_token获取ticket。

状态码： 400

表 3-234 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

社交帐号登录绑定手机号。绑定手机号为12345678901，接收到的验证码为123456。

```
POST https://{domain_name}/api/v2/sdk/social/bind

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-state-token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "mobile": "12345678901",
  "verify_code": "123456"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "session_token" : "bts******2VO",
  "expire" : 604800,
  "status" : "SUCCESS"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.6.2 社交帐号注册并绑定手机号

功能介绍

在管理门户配置的认证源选择未关联用户为绑定时或注册时，用于社交帐号注册并绑定手机号操作。

URI

POST /api/v2/sdk/social/register-bind

请求参数

表 3-235 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。

参数	是否必选	参数类型	描述
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-state-token	是	String	临时令牌。当认证源配置为绑定时，用于社交帐号绑定手机号操作，需要传入对应的state_token，绑定成功返回用户session_token，绑定失败返回失败信息。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-236 请求 Body 参数

参数	是否必选	参数类型	描述
mobile	是	String	接收验证码的手机号。
verify_code	是	String	接收到的验证码。

响应参数

状态码： 200

表 3-237 响应 Body 参数

参数	参数类型	描述
status	String	登录流程状态标识，返回SUCCESS表示登录成功。

参数	参数类型	描述
session_token	String	用户session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。
expire	Integer	session_token有效期，单位为秒，有效期内可以使用session_token获取ticket。

状态码： 400

表 3-238 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

社交账号注册并绑定手机号。手机号为12345678901，收到的验证码为123456。

```
POST https://{domain_name}/api/v2/sdk/social/register-bind

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-state-token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "mobile": "12345678901",
  "verify_code": "123456"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "session_token" : "bts******2VO",
  "expire" : 604800,
  "status" : "SUCCESS"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.6.3 获取用户已绑定的社交帐号列表

功能介绍

获取用户已绑定的社交帐号列表。

URI

GET /api/v2/sdk/social

请求参数

表 3-239 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。

参数	是否必选	参数类型	描述
X-signature	是	String	加密数据为session_token=xxx&timestamp=xxx&nonce=xxx，其中：session_token为会话凭证，timestamp表示当前时间戳，nonce表示当前时间戳的16进制，加密方式为RSA公钥加密。当前时间戳可调用获取服务器时间接口获取，加密公钥可调用获取公钥接口获取。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 200

表 3-240 响应 Body 参数

参数	参数类型	描述
social	Array of **SocialResult** objects	社交帐号信息集合。

表 3-241 SocialResult

参数	参数类型	描述
id	String	系统自动生成的id。
userId	String	用户id。
socialType	String	社交类型。
social_uid	String	社交id。
socialNickname	String	昵称。
socialHeadImage	String	头像。

参数	参数类型	描述
socialAccountDetails	String	描述。
createdAt	String	创建时间。
updatedAt	String	修改时间。

状态码： 400

表 3-242 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

获取用户已绑定的社交帐号列表。

```
GET https://{domain_name}/api/v2/sdk/social

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-signature:D0JeOUuVqU8Ixvl0xrmewQRk4AuGZrtk1RfBxueNKUrNPpgSbXrYnzw...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21
```

响应示例

状态码： 200

请求成功。

```
{
  "social" : [ {
    "id" : "20210516130247432-C84E-E5EA8CFE7",
    "userId" : "20210515202200788-094F-074FB1341",
    "socialType" : "weixin",
    "social_uid" : "001GKgGa15HGZA0aOxIa1bFktp1GKgG4_social_uid",
    "socialNickname" : "zhangsan",
    "socialHeadImage" : "https://thirdwx.qlogo.cn/mmopen/vi_32/
Q0j4TwGTfTIQ8QOTSn3y4cYHLlMC3sv6RCBmeMkxtOog47Zr3v2Afbqc2bmP0WibUIUskX39eJlJAEbAibXs",
    "socialAccountDetails" : "zhangsan",
    "createdAt" : "2021-05-16 13:02:48.513",
    "updatedAt" : "2021-05-16 13:02:48.513"
  } ]
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.6.4 社交帐号解绑

功能介绍

社交帐号解绑。

URI

POST /api/v2/sdk/social/unbind-account

请求参数

表 3-243 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。

参数	是否必选	参数类型	描述
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-signature	是	String	加密数据为session_token=xxx&timestamp=xxx&nonce=xxx，其中：session_token为会话凭证，timestamp表示当前时间戳，nonce表示当前时间戳的16进制，加密方式为RSA公钥加密。当前时间戳可调用获取服务器时间接口获取，加密公钥可调用获取公钥接口获取。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-244 请求 Body 参数

参数	是否必选	参数类型	描述
id	是	String	系统自动生成的id，可通过查询用户绑定的社交帐号列表接口获取。

响应参数

状态码： 400

表 3-245 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

通过绑定社交账号时自动生成的id解绑社交帐号。

```
POST https://{domain_name}/api/v2/sdk/social/unbind-account
```

```
X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36
(KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-signature:D0JeOUuVqU8Ixvl0xrmewQRk4AuGZrtk1RfBxueNKUrNPpgSbXrYnzw...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "id": "001GKgGa15HGZA0aOxIa1bFktp1GKgG4"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.7 密码管理

3.2.7.1 跳过强制修改密码

功能介绍

调用密码登录相关接口时，如果密码快过期，并且用户选择跳过修改密码时调用本接口，需要传入对应的state_token。

URI

GET /api/v2/sdk/pwd/skip-update

请求参数

表 3-246 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。

参数	是否必选	参数类型	描述
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-state-token	是	String	临时令牌，调用密码登录相关接口，密码快过期时返回的state_token。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 200

表 3-247 响应 Body 参数

参数	参数类型	描述
status	String	登录流程状态标识。 枚举值： ● **SUCCESS：登录成功** ● **ACCESS_DENIED：拒绝访问**
session_token	String	用户session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。

参数	参数类型	描述
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。
expire	Integer	session_token有效期，单位为秒，有效期内可以使用session_token获取ticket。

状态码： 400

表 3-248 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

跳过强制修改密码。

```
GET https://{domain_name}/api/v2/sdk/pwd/skip-update

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-state-token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21
```

响应示例

状态码： 200

请求成功。

```
{
  "status" : "SUCCESS",
  "expire" : 43200,
  "session_token" : "LGT******sqa"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.7.2 密码过期强制修改密码

功能介绍

调用密码登录相关接口时，如果密码已过期或者密码快过期，并且用户选择修改密码时调用本接口，需要传入对应的state_token。

URI

POST /api/v2/sdk/pwd/update

请求参数

表 3-249 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-state-token	是	String	临时令牌，调用密码登录相关接口，密码快过期或已过期时返回的state_token。

参数	是否必选	参数类型	描述
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-250 请求 Body 参数

参数	是否必选	参数类型	描述
old_password	是	String	用户的原密码。
new_password	是	String	设置的新密码。

响应参数

状态码： 200

表 3-251 响应 Body 参数

参数	参数类型	描述
status	String	登录流程状态标识。 枚举值： ● **SUCCESS：登录成功** ● **ACCESS_DENIED：拒绝访问**
session_token	String	用户session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。
expire	Integer	session_token有效期，单位为秒，有效期内可以使用session_token获取ticket。

状态码： 400

表 3-252 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

密码过期强制修改密码。

```
POST https://{domain_name}/api/v2/sdk/pwd/update

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36
(KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-state-token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "old_password": "P******d",
  "new_password": "P******3"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "status" : "SUCCESS",
  "expire" : 43200,
  "session_token" : "LGT******sqa"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.7.3 通过手机号找回密码

功能介绍

用户在登录页面单击忘记密码，并选择通过手机号找回密码时，需要输入手机号、验证码、新的密码并通过图形验证码校验后调用本接口。

URI

POST /api/v2/sdk/pwd/update-by-mobile

请求参数

表 3-253 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-254 请求 Body 参数

参数	是否必选	参数类型	描述
mobile	是	String	接收验证码的手机号。
verify_code	是	String	接收到的验证码。
password	是	String	新密码。

响应参数

状态码： 400

表 3-255 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

通过手机号找回密码。手机号为12345678901，验证码为123456，新密码为P******d。

```
POST https://{domain_name}/api/v2/sdk/pwd/update-by-mobile

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "mobile": "12345678901",
  "verify_code": "123456",
  "password": "P******d"
}
```

响应示例

无

状态码

状态码	描述
200	请求成功
400	参数无效。

错误码

请参见错误码。

3.2.8 二次认证

3.2.8.1 通过 state_Token 获取手机号

功能介绍

用于手机号短信二次认证时，通过state_token获取手机号。

URI

GET /api/v2/sdk/mobile-by-token

请求参数

表 3-256 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-state-token	是	String	用户带有状态的令牌。登录相关接口返回为二次认证场景时，会返回该state_token。

参数	是否必选	参数类型	描述
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 200

表 3-257 响应 Body 参数

参数	参数类型	描述
mobile	String	手机号。

状态码： 400

表 3-258 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

通过state_Token获取手机号。请求头X-state-token为eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...。

```
GET https://{domain_name}/api/v2/sdk/mobile-by-token

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-state-token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21
```

响应示例

状态码： 200

请求成功。

```
{
  "mobile" : "12345678901"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.8.2 手机号短信验证码二次认证

功能介绍

登录过程中如果需要二次认证，则调用本接口根据手机号、短信验证码认证。

URI

POST /api/v2/sdk/mfa/sms

请求参数

表 3-259 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。

参数	是否必选	参数类型	描述
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-state-token	是	String	用户带有状态的令牌。登录相关接口返回为二次认证场景时，会返回该state_token。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-260 请求 Body 参数

参数	是否必选	参数类型	描述
mobile	是	String	接收验证码的手机号。
verify_code	是	String	接收到的验证码。

响应参数

状态码： 200

表 3-261 响应 Body 参数

参数	参数类型	描述
status	String	登录流程状态标识。 枚举值： ● **SUCCESS：登录成功** ● **ACCESS_DENIED：拒绝访问**
session_token	String	用户session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。
expire	Integer	session_token有效期，单位为秒，有效期内可以使用session_token获取ticket。

状态码： 400

表 3-262 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

手机号短信验证码二次认证。手机号为12345678901，验证码为123456。

```
POST https://{domain_name}/api/v2/sdk/mfa/sms

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-state-token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "mobile": "12345678901",
  "verify_code": "123456"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "status" : "SUCCESS",
  "expire" : 43200,
  "session_token" : "LGT******sqa"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.9 个人信息管理

3.2.9.1 查询个人信息

功能介绍

用户登录成功后查询个人信息时调用本接口。

URI

GET /api/v2/sdk/profile

请求参数

表 3-263 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-signature	是	String	加密数据为session_token=xxx&timestamp=xxx&nonce=xxx，其中：session_token为会话凭证，timestamp表示当前时间戳，nonce表示当前时间戳的16进制，加密方式为RSA公钥加密。当前时间戳可调用获取服务器时间接口获取，加密公钥可调用获取公钥接口获取。

参数	是否必选	参数类型	描述
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 200

表 3-264 响应 Body 参数

参数	参数类型	描述
user_name	String	用户名。
name	String	姓名。
mobile	String	手机号。
verify_code	String	短信验证码。
email	String	邮箱。
pwd	String	密码。
head_img	String	头像，填写url地址。
attr_gender	String	性别。 枚举值： ● **unknown：保密** ● **male：男性** ● **female：女性**
attr_birthday	String	生日，格式为yyyy-MM-dd。
attr_nick_name	String	昵称。
first_name	String	名字。
middle_name	String	中间名。
last_name	String	姓氏。
extension	Object	自定义扩展属性。

状态码： 400

表 3-265 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

无

响应示例

状态码： 200

请求成功。

```
{
  "user_name": "zhangsan",
  "name": "张三",
  "head_img": "https://thirdwx.qlogo.cn/mmopen/vi_32/
Q0j4TwGTfTIQ8QOTSn3y4cYHLlMC3sv6RCBmeMkxtOog47Zr3v2Afbqc2bmP0WibUIUskX39eJlJAEbAibXs",
  "email": "12345678901@example.com”,
  "mobile": "12345678901"
  "attr_gender":"male",
  "attr_birthday": "2022-02-17",
  "attr_nick_name": "张三",
  "first_name": "zhangsan",
  "middle_name": "zhangsan",
  "last_name": "zhangsan",
  "extension": {
    "age":"18"
  }
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.9.2 修改个人信息

功能介绍

用户登录成功后修改个人信息时调用本接口，本接口不支持修改个人密码、手机号、邮箱。

URI

POST /api/v2/sdk/profile/update

请求参数

表 3-266 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-signature	是	String	加密数据为session_token=xxx&timestamp=xxx&nonce=xxx，其中：session_token为会话凭证，timestamp表示当前时间戳，nonce表示当前时间戳的16进制，加密方式为RSA公钥加密。当前时间戳可调用获取服务器时间接口获取，加密公钥可调用获取公钥接口获取。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

表 3-267 请求 Body 参数

参数	是否必选	参数类型	描述
user_name	否	String	用户名。
name	否	String	姓名。
mobile	是	String	手机号。
verify_code	是	String	短信验证码。
email	否	String	邮箱。
pwd	否	String	密码。
head_img	否	String	头像，填写url地址。
attr_gender	否	String	性别。 枚举值： ● **unknown：保密** ● **male：男性** ● **female：女性**
attr_birthday	否	String	生日，格式为yyyy-MM-dd。
attr_nick_name	否	String	昵称。
first_name	否	String	名字。
middle_name	否	String	中间名。
last_name	否	String	姓氏。
extension	否	Object	自定义扩展属性。

响应参数

状态码： 400

表 3-268 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

修改个人信息。

```
POST https://{domain_name}/api/v2/sdk/profile/update
```

```
X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36
(KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-signature:D0JeOUuVqU8Ixvl0xrmewQRk4AuGZrtk1RfBxueNKUrNPpgSbXrYnzw...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "user_name": "zhangsan",
  "name": "张三",
  "head_img": "https://thirdwx.qlogo.cn/mmopen/vi_32/
Q0j4TwGTfTIQ8QOTSn3y4cYHLlMC3sv6RCBmeMkxtOog47Zr3v2Afbqc2bmP0WibUIUskX39eJlJAEbAibXs",
  "attr_gender": "male",
  "attr_birthday": "2022-02-17",
  "attr_nick_name": "张三",
  "first_name": "zhangsan",
  "middle_name": "zhangsan",
  "last_name": "zhangsan",
  "extension": {
    "age": "18"
  }
}
```

响应示例

无

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.10 SSO

3.2.10.1 通过 session_token 获取 sso_ticket

功能介绍

获取用户信息时，先调用本接口获取sso_ticket。

URI

POST /api/v2/tenant/sso/session-token/sso-ticket

请求参数

表 3-269 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。
X-tenant-id	否	String	租户外部ID，如果为ISV方调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id。

表 3-270 请求 Body 参数

参数	是否必选	参数类型	描述
session_token	是	String	登录成功返回的会话token。
operating_sys_version	是	String	调用方操作系统版本，例如：Android 10。
device_ip	是	String	调用方设备ip，例如：10.10.10.1。
device_fingerprint	是	String	调用方设备指纹，同一个用户调用接口时该参数的值需和登录接口中的值保持统一，例如：156aysdna213sc50。
agent	否	String	调用方User-Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
client_id	否	String	应用授权ID，获取用户信息时如果想获取的是单点应用的用户信息，则需要传入单点应用的client_id。

响应参数

状态码： 200

表 3-271 响应 Body 参数

参数	参数类型	描述
expire	Integer	过期时间，单位秒。
sso_ticket	String	一次性票据，通过用户登录后的session_token获取一次性访问票据sso_ticket，通过sso_ticket可以获取用户信息。

状态码： 400

表 3-272 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

通登录成功后响应得到值为iJK******ITu的session_token获取sso_ticket。

```
POST https://{domain_name}/api/v2/tenant/sso/session-token/sso-ticket

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "session_token": "iJK******ITu",
  "operating_sys_version": "Android 10",
  "device_ip": "10.10.10.1",
  "device_fingerprint": "156aysdna213sac",
  "agent": "Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36",
  "client_id": "9fIHl3Dc9ivToWLVtblrF6Sjv9Fx47JJ"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "expire" : 9600,
  "sso_ticket" : "cd7******yjn"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.10.2 通过 sso_ticket 获取用户信息

功能介绍

通过sso_ticket获取用户信息。

URI

POST /api/v2/tenant/sso/sso-ticket/verify

请求参数

表 3-273 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。
X-tenant-id	否	String	租户外部ID，如果为ISV方调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id。

表 3-274 请求 Body 参数

参数	是否必选	参数类型	描述
sso_ticket	是	String	一次性访问票据，通过用户登录后的session_token获取一次性访问票据sso_ticket，通过sso_ticket可以获取用户信息。
operating_sys_version	是	String	调用方操作系统版本，例如：Android 10。
device_ip	是	String	调用方设备ip，例如：10.10.10.1。
device_fingerprint	是	String	调用方设备指纹，同一个用户调用接口时该参数的值需保持统一，例如：156aysdna213sc50。
agent	否	String	调用方User-Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。

响应参数

状态码： 200

表 3-275 响应 Body 参数

参数	参数类型	描述
code	String	错误码。
message	String	错误描述。
data	**data** object	用户信息。

表 3-276 data

参数	参数类型	描述
user	**UserInfoDataResult** object	用户信息。

表 3-277 UserInfoDataResult

参数	参数类型	描述
userName	String	用户名。
id	String	用户id。
name	String	姓名。
mobile	String	手机号。
email	String	邮箱。

状态码： 400

表 3-278 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

通过session_token换取的sso_ticket查询用户信息，sso_ticket值为ssoTicket-r5TCBLU14oSGxCMVdxeB5HA1uJiV。

```
POST https://{domain_name}/api/v2/tenant/sso/sso-ticket/verify

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "sso_ticket": "ssoTicket-r5TCBLU14oSGxCMVdxeB5HA1uJiV",
  "operating_sys_version": "Android 10",
  "device_ip": "10.10.10.1",
  "device_fingerprint": "156aysdna213sac",
  "agent": "Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "code" : "0",
  "message" : "success",
  "data" : {
    "user" : {
      "name" : "20220330162435",
      "mobile" : "12345678901",
      "id" : "20220330162436475-7570-D943B4FF3",
      "userName" : "20220330162435",
```

```
    "email" : "20220330162435@example.com"
  }
 }
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.10.3 刷新 session_token

功能介绍

刷新session_token。

URI

POST /api/v2/tenant/sso/session-token/refresh

请求参数

表 3-279 请求 Header 参数

参数	是否必选	参数类型	描述
Content-Type	是	String	该字段内容填为“application/json;charset=utf8”。
Authorization	是	String	认证凭据，值：Bearer {access_token}，access_token通过“获取访问凭据”接口获取。
X-tenant-id	否	String	租户外部ID，如果为ISV方调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id。

表 3-280 请求 Body 参数

参数	是否必选	参数类型	描述
session_token	是	String	用户登录后的session_token。
operating_sys_version	是	String	调用方操作系统版本，例如：Android 10。
device_ip	是	String	调用方设备ip，例如：10.10.10.1。
device_fingerprint	是	String	调用方设备指纹，同一个用户调用接口时该参数的值需保持统一，例如：156aysdna213sc50。
agent	否	String	调用方User-Agent信息。例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。

响应参数

状态码： 200

表 3-281 响应 Body 参数

参数	参数类型	描述
session_token	String	用户新的session_token，可使用该token调用单点登录接口获取sso_ticket，通过sso_ticket可以获取用户信息。
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。
expire	Integer	过期时间，单位为秒。

状态码： 400

表 3-282 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

根据用户登录成功后获取值为r5y******LU1的session_token再刷新session_token。

```
POST https://{domain_name}/api/v2/tenant/sso/session-token/refresh

Authorization: Bearer 334963fc-1e4a-473b-9096-52a929140...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21

{
  "session_token": "r5y******LU1",
  "operating_sys_version": "Android 10",
  "device_ip": "10.10.10.1",
  "device_fingerprint": "156aysdna213sac",
  "agent": "Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36"
}
```

响应示例

状态码： 200

请求成功。

```
{
  "session_token" : "lqI******JFH"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.2.11 id_token 管理

3.2.11.1 通过 session_token 生成 id_token

功能介绍

通过session_token生成id_token，一般刷新id_token时使用。

URI

POST /api/v2/sdk/session-token/refresh-id-token

请求参数

表 3-283 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-signature	是	String	加密数据为session_token=xxx&timestamp=xxx&nonce=xxx，其中：session_token为会话凭证，timestamp表示当前时间戳，nonce表示当前时间戳的16进制，加密方式为RSA公钥加密。当前时间戳可调用获取服务器时间接口获取，加密公钥可调用获取公钥接口获取。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 200

表 3-284 响应 Body 参数

参数	参数类型	描述
id_token	String	本质上是一个JWT Token，包含了用户身份信息，默认2小时有效，支持可配置。

状态码： 400

表 3-285 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

无

响应示例

状态码： 200

请求成功。

```
{
  "id_token" : "eyJ******dhg"
}
```

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.3 应用集成接口

3.3.1 如何调用 API

3.3.1.1 构造请求

本节介绍API请求的组成，并以调用OneAccess基于OAuth2.0的应用认证集成所需接口“获取Access Token”为例接口说明如何调用API，获取Access Token，Access Token可用于调用获取用户信息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** 。

前提条件

调用API前，需要获取管理员在OneAccess管理门户中已添加应用的**通用信息**中的ClientId以及ClientSecret，可以调用API实现相关接口功能。

请求 URI

OneAccess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 3-286 URI 中的参数说明

参数	描述
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OneAccess服务API需要使用用户访问域名，获取方法请参见**获取用户访问域名**。
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“获取用户Token”API的resource-path为“api/v1/oauth2/token”。
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。

例如您需要获取用户访问域名为“abcdefg.huaweioneaccess.com”的实例Access Token，则需使用用户访问域名“abcdefg.huaweioneaccess.com”，并在获取Access Token的URI部分找到resource-path（ /api/v1/oauth2/token ），拼接起来如下所示。

```
https://abcdefg.huaweioneaccess.com/api/v1/oauth2/token
```

图 3-3 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在同一个实例也相同，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 3-287 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的URI部分，您可以看到其请求方法为“POST”，则其请求为：

```
POST https://abcdefg.huaweioneaccess.com/api/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。

详细的公共请求消息头字段请参见**表3-288**。

表 3-288 公共请求消息头

名称	描述	是否必选	示例
Content-Type	消息体的类型（格式）。默认取值为“application/json”，有其他取值时会在具体接口中专门说明。	是	application/json

名称	描述	是否必选	示例
Accept	接受响应类型。推荐用户使用默认值application/json，有其他取值时会在具体接口中专门说明。	否	application/json
Content-Length	请求body长度，单位为Byte。	否	3495

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://abcdefg.huaweioneaccess.com/api/v1/oauth2/token
Content-Type: application/json
```

请求消息体（可选）

该部分可选。请求消息体通常以结构化格式（如JSON或XML）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。若请求消息体中的参数支持中文，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，其中***domain_name***为用户访问域名，*************为认证登录后回调获取的授权码，***ClientId***为注册应用后分配的接口认证凭证ID，***ClientSecret***为注册应用后分配的接口认证凭证密钥，***https://example.com***为注册应用时填写的回调地址。

```
POST https://abcdefg.huaweioneaccess.com/api/v1/oauth2/token
Content-Type: application/json

code=******&
client_id=ClientId&
client_secret=ClientSecret&
redirect_uri=https://example.com&
grant_type=authorization_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。对于获取用户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。

3.3.1.2 返回结果

状态码

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。

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。

对于获取访问凭据接口，如果调用后返回状态码为“200”，则表示请求成功。

响应消息头（可选）

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（可选）

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" : "334**********************************140...",
  "expires_in" : 1719,
  "refresh_token":"42e******************w24...",
  "token_type" : "Bearer",
  "scope" : "get_user_info",
}
```

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": "invalid_client",
  "error_description": "Invalid authorization code"
}
```

其中，error表示错误类型，error_description表示错误描述信息。

3.3.2 基于 CAS 的应用认证集成

3.3.2.1 认证登录

功能介绍

用户访问集成应用时，应用向OneAccess发起基于CAS的认证登录（重定向方式），用户添加该应用授权帐号，用户使用应用认证登录接口POST/api/v1/login/form 传递参数：username、password；用户输入用户密码认证成功后，在调用下面的接口，OneAccess将重定向回应用，携带ticket参数传递Service Ticket票据。

URI

GET /api/v1/cas/login

表 3-289 Query 参数

参数	是否必选	参数类型	描述
service	是	String	应用接受票据的地址，URL编码，必须与应用CAS配置中的应用回调URL一致。

请求参数

无

响应参数

状态码： 302

表 3-290 响应 Header 参数

参数	参数类型	描述
Location	String	认证登录成功，重定向地址。例：https://example.com?ticket=ST-eYlKs8FrLCltwRwfm8AiwCxmQ8gAL...

请求示例

调用CAS单点登录接口进行认证，配置携带票据信息的重定向地址为https://example.com。

```
GET https://{domain_name}/api/v1/cas/login?service=https://example.com
```

响应示例

无

状态码

状态码	描述
302	认证登录成功或已登录，携带Service Ticket重定向到service地址。例：https://example.com?ticket=ST-eYlKs8FrLCltwRwfm8AiwCxmQ8gALNSK

错误码

请参见错误码。

3.3.2.2 验证票据(CAS3.0)

功能介绍

应用验证票据，并获取用户属性信息。

URI

GET /api/v1/cas/p3/serviceValidate

表 3-291 Query 参数

参数	是否必选	参数类型	描述
service	是	String	应用接受票据的地址，必须与应用CAS配置中的应用回调URL一致。
ticket	是	String	票据，认证登录获取的Service Ticket。
format	否	String	响应用户信息的格式，可选择XML和JSON。 缺省值：**XML**

请求参数

无

响应参数

无

请求示例

查询CAS3.0接口验证票据，参数分别配置应用回调地址https://example.com及认证登录接口获取的认证票据ST-eYlKs8FrLCltwRwfm8AiwCxmQ8gAL...，使用JSON响应格式获取用户属性信息。

```
GET https://{domain_name}/api/v1/cas/p3/serviceValidate?service=https://example.com&ticket=ST-eYlKs8FrLCltwRwfm8AiwCxmQ8gAL...&format=JSON
```

响应示例

状态码： 200

请求成功。

- 示例 1

```
<cas:serviceResponse xmlns:cas="http://www.yale.edu/tp/cas">
    <cas:authenticationSuccess>
        <cas:user>minghui</cas:user>
        <cas:attributes>
            <cas:authenticationDate>2020-02-11T09:28:14.987Z</cas:authenticationDate>
            <cas:longTermAuthenticationRequestTokenUsed>false</
cas:longTermAuthenticationRequestTokenUsed>
            <cas:isFromNewLogin>true</cas:isFromNewLogin>
            <cas:date>2020-02-03T16:00:00.000Z</cas:date>
            <cas:birthday>2020-02-04T16:00:00.000Z</cas:birthday>
            <cas:createAt>2020-01-10T09:01:04.000Z</cas:createAt>
            <cas:disabledAt>null</cas:disabledAt>
            <cas:disabed>false</cas:disabed>
        </cas:attributes>
    </cas:authenticationSuccess>
</cas:serviceResponse>
```

- 示例 2

```
{
  "serviceResponse" : {
    "authenticationSuccess" : {
      "attributes" : {
        "date" : "2020-02-03T16:00:00.000Z",
        "birthday" : "2020-02-04T16:00:00.000Z",
        "createAt" : "2020-01-10T09:01:04.000Z",
        "disabed" : false,
        "authenticationDate" : "2020-02-11T06:43:30.588Z",
        "longTermAuthenticationRequestTokenUsed" : false,
        "isFromNewLogin" : true
      },
      "user" : "minghui"
    }
  }
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见错误码。

3.3.2.3 注销登录

功能介绍

注销登录会话。

URI

GET /api/v1/cas/logout

表 3-292 Query 参数

参数	是否必选	参数类型	描述
service	否	String	注销退出后的重定向地址，不设置则跳转登录页，若设置必须与应用CAS配置中的应用回调URL一致。

请求参数

无

响应参数

无

请求示例

注销CAS登录会话，重定向到应用回调地址https://example.com。

```
GET https://{domain_name}/api/v1/cas/logout?service= https://example.com
```

响应示例

无

状态码

状态码	描述
302	如果传递service，重定向到servie地址，否则重定向到登录页。

错误码

请参见错误码。

3.3.2.4 验证票据(CAS1.0)

功能介绍

应用验证票据。

URI

GET /api/v1/cas/validate

表 3-293 Query 参数

参数	是否必选	参数类型	描述
service	是	String	应用接受票据的地址，必须与应用CAS配置中的应用回调URL一致。
ticket	是	String	票据，认证登录获取的Service Ticket。

请求参数

无

响应参数

无

请求示例

查询CAS1.0接口验证票据，参数分别配置应用回调地址https://example.com及认证登录接口获取的认证票据ST-eYlKs8FrLCltwRwfm8AiwCxmQ8gAL...，获取用户属性信息。

```
GET https://{domain_name}/api/v1/cas/validate?service=https://example.com&ticket=ST-eYlKs8FrLCltwRwfm8AiwCxmQ8gAL...
```

响应示例

状态码： 200

请求成功。

```
{
  "application/text" : "yes用户名"
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见错误码。

3.3.2.5 验证票据(CAS2.0)

功能介绍

应用验证票据，并获取用户信息。

URI

GET /api/v1/cas/serviceValidate

表 3-294 Query 参数

参数	是否必选	参数类型	描述
service	是	String	应用接受票据的地址，必须与应用CAS配置中的应用回调URL一致。
ticket	是	String	票据，认证登录获取的Service Ticket。

参数	是否必选	参数类型	描述
format	否	String	响应用户信息的格式，可选择XML和JSON。 缺省值：**XML**

请求参数

无

响应参数

无

请求示例

查询CAS2.0接口验证票据，参数分别配置应用回调地址https://example.com及认证登录接口获取的认证票据ST-eYlKs8FrLCltwRwfm8AiwCxmQ8gAL...，使用JSON响应格式获取用户属性信息。

```
GET https://{domain_name}/api/v1/cas/serviceValidate?service=https://example.com&ticket=ST-eYlKs8FrLCltwRwfm8AiwCxmQ8gAL...&format=JSON
```

响应示例

状态码： 200

请求成功。

- 示例 1

```
<cas:serviceResponse xmlns:cas="http://www.yale.edu/tp/cas">
    <cas:authenticationFailure code="INVALID_TICKET">Ticket ST-l1HnvKIWa0hhKTapEMdR7CU31iSG2... not recognized</cas:authenticationFailure>
</cas:serviceResponse>
```

- 示例 2

```
{
  "serviceResponse" : {
    "authenticationFailure" : {
      "code" : "INVALID_TICKET",
      "description" : "the ticket provided was not valid, ticket is ST-l1HnvKIWa0hhKTapEMdR7CU31iSG2..."
    }
  }
}
```

状态码

状态码	描述
200	请求成功。

错误码

请参见错误码。

3.3.3 基于 SAML2.0 的应用认证集成

3.3.3.1 IdP-initiated 单点登录

功能介绍

发起基于IdP-initiated的单点登录。

URI

GET /api/v1/saml2/idp/sso

表 3-295 Query 参数

参数	是否必选	参数类型	描述
sp	是	String	应用Entity ID。

请求参数

无

响应参数

无

请求示例

发起基于IdP-initiated的单点登录，entity ID为https://example.com/sp/

```
https://{domain_name}/api/v1/saml2/idp/sso?sp=https://example.com/sp/
```

响应示例

无

状态码

状态码	描述
200	用户已登录，向SP断言消费地址发送断言。
302	用户未登录，跳转用户登录地址。

错误码

请参见错误码。

3.3.3.2 获取 IdP 元数据 metadata

功能介绍

获取基于SAML2.0的身份提供商IdP的Metadata文件。（不支持postman接口请求下载）

URI

GET /api/v1/saml2/idp/metadata

请求参数

无

响应参数

无

请求示例

获取基于SAML2.0的身份提供商IdP的Metadata文件。

```
GET https://{domain_name}/api/v1/saml2/idp/metadata
```

响应示例

无

状态码

状态码	描述
200	请求成功。

错误码

请参见错误码。

3.3.4 基于 OAuth2.0 的应用认证集成

3.3.4.1 认证登录获取授权码

功能介绍

用户访问集成应用时，应用向OneAccess发起授权登录请求（重定向方式），用户输入用户密码认证成功后，OneAccess将重定向回应用回调地址，并携带授权码code参数。

URI

GET /api/v1/oauth2/authorize

表 3-296 Query 参数

参数	是否必选	参数类型	描述
response_type	是	String	授权类型，固定值：code。
client_id	是	String	应用标识，注册应用后，分配的ClientId。
scope	否	String	授权范围 ，固定值：get_user_info。
redirect_uri	否	String	成功授权后的回调地址，地址可以是注册应用时填写的回调地址，也可以是注册应用时填写的回调地址的域名，建议配置为应用的首页或者应用的用户中心。注意需要对uri进行URLEncode处理。
state	否	String	应用的状态值。可用于防止CSRF攻击，成功授权后回调应用时会原样带回，应用用它校验认证请求与回调请求的对应关系。可以包含字母和数字。

请求参数

无

响应参数

状态码： 302

表 3-297 响应 Header 参数

参数	参数类型	描述
Location	String	认证登录成功，重定向地址。例：https://example.com?code=z2D...&state=test

请求示例

获取OAuth2.0授权码。授权类型为固定值code，配置应用注册时生成的clientId，成功授权后的回调地址为https://example.com，授权范围为固定值get_user_info。

```
GET https://{domain_name}/api/v1/oauth2/authorize?response_type=code&client_id=NzZeWuiJa91dPSRdZQChMazIh13AW...&redirect_uri=https://example.com&scope=get_user_info&state=test
```

响应示例

无

状态码

状态码	描述
302	用户未登录，跳转用户登录页面；用户已登录，携带授权码重定向到redirect_uri地址。例：https://example.com?code=z2D...&state=test。

错误码

请参见错误码。

3.3.4.2 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 /api/v1/oauth2/token

请求参数

表 3-298 FormData 参数

参数	是否必选	参数类型	描述
code	是	String	授权码，认证登录获取授权码接口返回的授权码。
client_id	是	String	应用标识，注册应用后，分配的ClientId。
client_secret	是	String	应用密钥，注册应用后，分配的ClientSecret。
grant_type	是	String	授权类型，固定值：authorization_code。
redirect_uri	否	String	回调地址，地址可以是注册应用时填写的回调地址，也可以是注册应用时填写的回调地址的域名。若传入，则需要与调用认证登录获取授权码接口的入参redirect_url保持一致。

响应参数

状态码： 200

表 3-299 响应 Body 参数

参数	参数类型	描述
access_token	String	授权服务器返回给第三方应用的访问令牌。
token_type	String	访问令牌类型。固定值：Bearer。
expires_in	Long	访问令牌的有效期，以秒为单位。
scope	String	授权范围。
refresh_token	String	刷新令牌。默认不生成refresh_token，如果需要，在应用的“认证配置”中设置“Refresh Token有效期”后生成返回。

状态码： 400

表 3-300 响应 Body 参数

参数	参数类型	描述
error	String	错误类型。
error_description	String	错误描述。

请求示例

获取AccessToken，后续使用该token获取用户信息。code使用认证登录获取授权码接口返回的授权码z2D...，client_id和client_secert使用注册应用时分配的ClientId和ClientSecret，redirect_uri配置为应用的回调地址https://example.com，grant_type为固定值authorization_code。

```
POST https://{domain_name}/api/v1/oauth2/token

Content-Type: application/x-www-form-urlencoded

code=z2D...&
client_id=NzZeWuiJa91dPSRdZQChMazIh13AW...&
client_secret=NzZeWuiJa91dPSRdZQChMazIh13AW...&
redirect_uri=https://example.com&
grant_type=authorization_code
```

响应示例

状态码： 200

请求成功。

```
{
  "access_token" : "NqM******d3k",
  "token_type" : "Bearer",
  "expires_in" : "7200",
  "scope" : "get_user_info",
  "refresh_token" : "42e******w24"
}
```

状态码： 400

请求错误。

```
{
  "error" : "invalid_grant",
  "error_description" : "Invalid authorization code"
}
```

状态码

状态码	描述
200	请求成功。
400	请求错误。

错误码

请参见错误码。

3.3.4.3 获取用户信息

功能介绍

获取用户信息。

URI

GET /api/v1/oauth2/userinfo

请求参数

表 3-301 请求 Header 参数

参数	是否必选	参数类型	描述
Authorization	是	String	认证凭据，值：Bearer {access_token}。
Accept	是	String	接收响应类型，值：application/json。

响应参数

状态码： 200

表 3-302 响应 Body 参数

参数	参数类型	描述
id	String	用户ID
userName	String	用户名
name	String	姓名
email	String	邮箱地址
mobile	String	手机号

状态码： 401

表 3-303 响应 Body 参数

参数	参数类型	描述
error	String	错误类型。
error_description	String	错误描述。

请求示例

基于access_token 查询用户信息。

```
GET https://{domain_name}/api/v1/oauth2/userinfo

Authorization: Bearer b7e1fda8-33ce-432c-9b97-7ff035fac...
Accept: application/json
```

响应示例

状态码： 200

请求成功。

```
{
  "id" : "20201029190841785-CB37-8BD36B...",
  "name" : "test",
  "userName" : "test",
  "mobile" : "12345678901",
  "email" : "123@example.com"
}
```

状态码： 401

认证失败。

```
{
  "error" : "unauthorized",
  "error_description" : "Full authentication is required to access this resource"
}
```

状态码

状态码	描述
200	请求成功。
401	认证失败。

错误码

请参见错误码。

3.3.4.4 刷新 Access Token

功能介绍

刷新AccessToken。

URI

POST /api/v1/oauth2/token

请求参数

表 3-304 FormData 参数

参数	是否必选	参数类型	描述
client_id	是	String	应用标识，注册应用后，分配的ClientId。
client_secret	是	String	应用密钥，注册应用后，分配的ClientSecret。
refresh_token	是	String	刷新令牌，获取Access Token接口中返回。
grant_type	是	String	授权类型，固定值：refresh_token。

响应参数

状态码： 200

表 3-305 响应 Body 参数

参数	参数类型	描述
access_token	String	授权服务器返回给第三方应用的访问令牌。
token_type	String	访问令牌类型。固定值：Bearer。
expires_in	Long	访问令牌的有效期，以秒为单位。
scope	String	授权范围。
refresh_token	String	刷新令牌。

状态码： 400

表 3-306 响应 Body 参数

参数	参数类型	描述
error	String	错误类型。
error_description	String	错误描述。

请求示例

基于refresh_token刷新access_token，refresh_token通过调用获取AccessToken接口的响应值获取，client_id和client_secret使用注册应用时分配的ClientId和ClientSecret，grant_type为固定值refresh_token。

```
POST https://{domain_name}/api/v1/oauth2/token

Content-Type: application/x-www-form-urlencoded

client_id=NzZeWuiJa91dPSRdZQChMazIh13AW...&
client_secret=NzZ******3AW&
refresh_token=e8e******7e3&
grant_type=refresh_token
```

响应示例

状态码： 200

请求成功。

```
{
  "access_token" : "9b0******df2",
  "token_type" : "Bearer",
  "expires_in" : 7200,
  "scope" : "get_user_info",
  "refresh_token" : "dec******7f1"
}
```

状态码： 400

请求错误。

```
{
  "error" : "invalid_grant",
  "error_description" : "Invalid refresh token"
}
```

状态码

状态码	描述
200	请求成功。
400	请求错误。

错误码

请参见错误码。

3.3.5 基于 OIDC 的应用认证集成

3.3.5.1 认证登录获取授权码

功能介绍

用户访问集成应用时，应用向OneAccess发起授权登录请求（重定向方式），用户输入用户密码认证成功后，OneAccess将重定向回应用，并携带授权码code参数。

URI

GET /api/v1/oauth2/authorize

表 3-307 Query 参数

参数	是否必选	参数类型	描述
client_id	是	String	应用标识，注册应用后，分配的ClientId。
redirect_uri	否	String	回调地址，表示应用接收OneAccess授权码的地址。地址可以是注册应用时填写的回调地址，也可以是注册应用时填写的回调地址的域名。
response_type	是	String	授权类型，固定值：code。
scope	否	String	授权范围，固定值：openid。
state	否	String	应用的状态值。可用于防止CSRF攻击，成功授权后回调应用时会原样带回，应用用它校验认证请求与回调请求的对应关系。可以包含字母和数字。

请求参数

无

响应参数

状态码： 302

表 3-308 响应 Header 参数

参数	参数类型	描述
Location	String	认证登录成功，重定向地址。例：https://example.com?code=z2D...&state=test

请求示例

获取OIDC授权码。授权类型为固定值code，配置应用注册时生成的clientId，成功授权后的回调地址为https://example.com，授权范围为固定值openid。

```
GET https://{domain_name}/api/v1/oauth2/authorize?
response_type=code&client_id=cU0L3GsEq1vuOJ5iQrRSu5AyPnKL8...&redirect_uri=https://
example.com&scope=openid&state=test
```

响应示例

无

状态码

状态码	描述
302	用户未登录，跳转用户登录页面。用户已登录，携带授权码重定向到redirect_uri地址。例：https://example.com?code=z2D...&state=test。

错误码

请参见错误码。

3.3.5.2 获取 ID Token

功能介绍

获取ID Token。

URI

POST /api/v1/oauth2/token

请求参数

表 3-309 FormData 参数

参数	是否必选	参数类型	描述
grant_type	是	String	授权类型，固定值：authorization_code。
code	是	String	授权码，认证登录后回调获取的授权码。
client_id	是	String	应用标识，注册应用后，分配的ClientId。

参数	是否必选	参数类型	描述
client_secret	是	String	应用密钥，注册应用后，分配的ClientSecret。
redirect_uri	是	String	回调地址，地址可以是注册应用时填写的回调地址，也可以是注册应用时填写的回调地址的域名。

响应参数

状态码： 200

表 3-310 响应 Body 参数

参数	参数类型	描述
access_token	String	授权服务器返回给第三方应用的访问令牌。
token_type	String	访问令牌类型。固定值：Bearer。
expires_in	String	访问令牌的有效期，以秒为单位。
scope	String	授权范围。
refresh_token	String	刷新令牌。默认不生成refresh_token，如果需要，在应用的“认证配置”中设置“Refresh Token有效期”后生成返回。
id_token	String	ID Token。

状态码： 400

表 3-311 响应 Body 参数

参数	参数类型	描述
error	String	错误类型。
error_description	String	错误描述。

请求示例

基于授权码获取ID Token。授权类型为固定值authorization_code，使用注册应用时分配的ClientId和ClientSecret，重定向地址配置为注册应用时的回调地址https://example.com。

```
POST https://{domain_name}/api/v1/oauth2/token
```

```
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&
code=0yV...&
client_id=cU0L3GsEq1vuOJ5iQrRSu5AyPnKL8...&
client_secret=EFj******TcE&
redirect_uri=https://example.com
```

响应示例

状态码： 200

请求成功。

- 示例 1

```
{
  "access_token" : "ObU******NpD",
  "token_type" : "Bearer",
  "expires_in" : 7200,
  "scope" : "openid",
  "id_token" : "eyJ******Njg"
}
```

- 示例 2

```
{
  "access_token" : "NqMh******d3k",
  "token_type" : "Bearer",
  "expires_in" : 7200,
  "scope" : "openid",
  "refresh_token" : "5wI******anH",
  "id_token" : "eyJ******Njg"
}
```

状态码： 400

请求错误。

```
{
  "error" : "invalid_grant",
  "error_description" : "Invalid authorization code"
}
```

状态码

状态码	描述
200	请求成功。
400	请求错误。

错误码

请参见错误码。

3.3.5.3 刷新 Access Token

功能介绍

刷新AccessToken。

URI

POST /api/v1/oauth2/token

请求参数

表 3-312 FormData 参数

参数	是否必选	参数类型	描述
client_id	是	String	应用标识，注册应用后，分配的ClientId。
client_secret	是	String	应用密钥，注册应用后，分配的ClientSecret。
refresh_token	是	String	刷新令牌，获取ID Token接口中返回。
grant_type	是	String	授权类型，固定值：refresh_token。

响应参数

状态码： 200

表 3-313 响应 Body 参数

参数	参数类型	描述
access_token	String	授权服务器返回给第三方应用的访问令牌。
token_type	String	访问令牌类型。固定值：Bearer。
expires_in	String	访问令牌的有效期，以秒为单位。
scope	String	授权范围。
refresh_token	String	刷新令牌。
id_token	String	ID Token。

状态码： 400

表 3-314 响应 Body 参数

参数	参数类型	描述
error	String	错误类型。
error_description	String	错误描述。

请求示例

基于refresh_token刷新access_token，refresh_token通过调用获取IDToken接口的响应值获取，client_id和client_secret使用注册应用时分配的ClientId和ClientSecret，grant_type为固定值refresh_token。

```
POST https://{domain_name}/api/v1/oauth2/token

Content-Type: application/x-www-form-urlencoded

client_id=cU0L3GsEq1vuOJ5iQrRSu5AyPnKL8...&
client_secret=EFj******TcE&
refresh_token=b462******7ef&
grant_type=refresh_token
```

响应示例

状态码： 200

请求成功。

```
{
  "access_token" : "270******6d5",
  "token_type" : "Bearer",
  "expires_in" : 7200,
  "scope" : "openid",
  "refresh_token" : "162******412",
  "id_token" : "eyJ******YTk"
}
```

状态码： 400

请求错误。

```
{
  "error" : "invalid_grant",
  "error_description" : "Invalid authorization code"
}
```

状态码

状态码	描述
200	请求成功。
400	请求错误。

错误码

请参见错误码。

3.3.5.4 隐式授权

功能介绍

用户访问集成应用时，应用通过隐式授权方式获取Access Token和ID Token，向OneAccess发起授权登录请求（重定向方式），用户输入用户密码认证成功后，OneAccess将重定向回应用，并携带Access Token和ID Token参数。

URI

GET /api/v1/oauth2/authorize

表 3-315 Query 参数

参数	是否必选	参数类型	描述
client_id	是	String	应用标识，注册应用后，分配的ClientId。
redirect_uri	是	String	回调地址，表示应用接收OneAccess Token（ID Token或Access Token）的地址。地址可以是注册应用时填写的回调地址，也可以是注册应用时填写的回调地址的域名。
response_type	是	String	授权类型。可选值：id_token或id_token token。 ● 取id_token值时，返回id_token。 ● 取id_token token值时，返回access_token和id_token。
scope	是	String	授权范围，固定值：openid。
state	否	String	应用的状态值。可用于防止CSRF攻击，成功授权后回调应用时会原样带回，应用用它校验认证请求与回调请求的对应关系。可以包含字母和数字。

请求参数

无

响应参数

状态码： 302

表 3-316 响应 Header 参数

参数	参数类型	描述
location	String	认证登录成功，重定向地址。- list text here授权类型为id_token时，返回https://example.com#id_token=eyJraWQiOi.JlNWFlNTg1Mzky.NjA0Njg...- list text here授权类型为id_token token时，返回https://example.com#access_token=f9dd6b8a-4b4f-4380-bf3a-39f8bfbef...&token_type=Bearer&expires_in=7199&id_token=eyJraWQiOi.JlNWFlNTg1Mzky.NjA0Njg...

请求示例

- 基于授权类型值为id_token token进行隐式授权，此时响应会携带access_token和id_token。

```
GET https://{domain_name}/api/v1/oauth2/authorize?response_type=id_token token&client_id=cU0L3GsEq1vuOJ5iQrRSu5AyPnKL8...&redirect_uri=https://example.com&scope=openid&state=test
```

- 基于授权类型值为id_token进行隐式授权，此时响应会携带id_token。

```
GET https://{domain_name}/api/v1/oauth2/authorize?response_type=id_token&client_id=cU0L3GsEq1vuOJ5iQrRSu5AyPnKL8...&redirect_uri=https://example.com&scope=openid&state=test
```

响应示例

无

状态码

状态码	描述
302	用户未登录，跳转用户登录页面。 用户已登录，携带Access Token和ID Token重定向到redirect_uri地址。

错误码

请参见错误码。

3.3.5.5 获取 OIDC metadata

功能介绍

获取基于OpenID Connect的身份提供商IdP的Metadata文件。

URI

GET /api/v1/oauth2/.well-known/openid-configuration

请求参数

无

响应参数

无

请求示例

获取基于OpenID Connect的身份提供商IdP的Metadata文件。

```
GET https://{domain_name}/api/v1/oauth2/.well-known/openid-configuration
```

响应示例

无

状态码

状态码	描述
200	请求成功。

错误码

请参见错误码。

3.3.6 退出登录

功能介绍

退出登录。

URI

GET /api/v2/sdk/logout

请求参数

表 3-317 请求 Header 参数

参数	是否必选	参数类型	描述
X-operating-sys-version	是	String	调用方操作系统版本，例如：Android 10。

参数	是否必选	参数类型	描述
X-device-fingerprint	是	String	调用方设备指纹，例如：156aysdna213sc50。
X-device-ip	否	String	调用方IP，例如：10.10.10.1。
X-agent	是	String	用户Agent信息，例如：Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36。
X-L	否	String	用于国际化语言设置，例如：zh。
X-client-id	是	String	应用标识，注册应用后分配的ClientId。
X-signature	是	String	加密数据为session_token=xxx&timestamp=xxx&nonce=xxx，其中：session_token为会话凭证，timestamp表示当前时间戳，nonce表示当前时间戳的16进制，加密方式为RSA公钥加密。当前时间戳可调用获取服务器时间接口获取，加密公钥可调用获取公钥接口获取。
X-tenant-id	否	String	租户id，ISV应用调用则为必填，需要将{domain_name}换成ISV通用域名{common_domain}，请求Header参数中需要指定对应租户的tenant_id，并将X-client-id换成ISV应用模板的client_id。

响应参数

状态码： 400

表 3-318 响应 Body 参数

参数	参数类型	描述
error_code	String	错误码。
error_msg	String	错误详情。

请求示例

退出登录。

```
GET https://{domain_name}/api/v2/sdk/logout

X-operating-sys-version: Android 10
X-device-fingerprint: 156aysdna213sac
X-device-ip: 10.10.10.1
X-agent: Mozilla/5.0 (Linux; Android 10; Redmi K30 Build/QKQ1.190825.002; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/80.0.3987.99 Mobile Safari/537.36
X-L: zh
X-client-id: DRrYIqauawN0I8myTMoDTPys6ezGZxnm
X-signature:D0JeOUuVqU8lxvl0xrmewQRk4AuGZrtk1RfBxueNKUrNPpgSbXrYnzw...
X-tenant-id: 08f770f51f80d2f40f38c00cb199fd21
```

响应示例

无

状态码

状态码	描述
200	请求成功。
400	参数无效。

错误码

请参见错误码。

3.3.6.1 全局退出

功能介绍

注销会话退出登录，当用户退出第三方应用系统时，除退出应用系统本身的会话外，同时将销毁OneAccess生成的SSO票据，OneAccess销毁SSO票据后，浏览器将重定向到应用端指定的回调地址URL。

URI

GET /api/v1/logout

表 3-319 Query 参数

参数	是否必选	参数类型	描述
redirect_url	否	String	注销退出后的重定向地址，不设置则跳转登录页，注意需要进行URL Encode。

请求参数

无

响应参数

无

请求示例

OneAccess全局退出登录并重定向到应用回调地址https://example.com。

```
GET https://{domain_name}/api/v1/logout?redirect_url= https://example.com
```

响应示例

无

状态码

状态码	描述
302	默认重定向到用户登录页面，如果指定redirect_url，则跳转redirect_url地址。

错误码

请参见错误码。

4 附录

4.1 session token 签名

签名流程

1. 构造待签名数据："session_token="+sessionToken+"&timestamp="+timestamp+"&nonce="+nonce。

   其中，timestamp为当前服务器时间戳，可调用获取服务器时间戳接口获取，nonce为随机字符串，每次签名请重新生成，可为当前时间戳的16进制。

2. 获取公钥publicKey，通过调用获取公钥接口获取。

   签名算法为RSA公钥加密，填充模式为RSA/ECB/OAEPWithSHA-256AndMGF1Padding，待签名数据加密后需要进行Base64编码。

Java 签名代码实例

```
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.apache.commons.codec.binary.Base64;
import javax.crypto.Cipher;
import java.nio.charset.Charset;
import java.security.*;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.PKCS8EncodedKeySpec;
import java.security.spec.X509EncodedKeySpec;
import java.util.Date;

public class RSAUtils {
    public static final Provider provider = new BouncyCastleProvider();
    public static final String KEY_ALGORITHM = "RSA";
    public static final String BEGIN_PRI_KEY = "-----BEGIN RSA PRIVATE KEY-----";
    public static final String END_PRI_KEY = "-----END RSA PRIVATE KEY-----";
    public static final String BEGIN_PUB_KEY = "-----BEGIN PUBLIC KEY-----";
    public static final String END_PUB_KEY = "-----END PUBLIC KEY-----";

    //加密
    public static String encrypt(String input, String publicKey) {
        // 去除公钥开头、结束标识和换行符
        publicKey = publicKey.replaceAll(BEGIN_PUB_KEY, "").replaceAll(END_PUB_KEY, "").replace("\\n", "");
        try {
            byte[] enStrByte =  encrypt(input, getPublicRSAKey(publicKey));
            return Base64Utils.encodeToString(enStrByte);
        }catch (Exception e){
```

```
            throw new RuntimeException("Could not encrypt data ",e);
        }
    }

    private static PublicKey getPublicRSAKey(String key) throws NoSuchAlgorithmException,
InvalidKeySpecException {
        X509EncodedKeySpec x509 = new X509EncodedKeySpec(Base64Utils.decodeFromString(key));
        KeyFactory kf = KeyFactory.getInstance(KEY_ALGORITHM, provider);
        return kf.generatePublic(x509);
    }

    private static byte[] encrypt(String input, PublicKey publicKey)
            throws Exception {
        Cipher cipher = Cipher.getInstance("RSA/ECB/OAEPWithSHA-256AndMGF1Padding", provider);
        cipher.init(Cipher.ENCRYPT_MODE, publicKey);
        byte[] re = cipher.doFinal(input.getBytes("UTF-8"));
        return re;
    }

    //解密
    public String decrypt(String input, String privateKey) {
        privateKey = privateKey.replaceAll(BEGIN_PRI_KEY, "").replaceAll(END_PRI_KEY, "").replace("\\n", "");
        try {
            byte[] bt = Base64.decodeBase64(input);
            byte[] decryptedData = RSAUtils.decrypt(bt, RSAUtils.getPrivateRSAKey(privateKey));
            return validateData(decryptedData);
        }catch (Exception e){
            return e.getMessage();
        }
    }

    private static byte[] decrypt(byte[] encrypted, PrivateKey privateKey)
            throws Exception {
        Cipher cipher = Cipher.getInstance("RSA/ECB/OAEPWithSHA-256AndMGF1Padding", provider);
        cipher.init(Cipher.DECRYPT_MODE, privateKey);
        return cipher.doFinal(encrypted);
    }

    public static PrivateKey getPrivateRSAKey(String key) throws InvalidKeySpecException,
NoSuchAlgorithmException {
        PKCS8EncodedKeySpec pkcs8 = new PKCS8EncodedKeySpec(Base64Utils.decodeFromString(key));
        KeyFactory kf = KeyFactory.getInstance(KEY_ALGORITHM, provider);
        return kf.generatePrivate(pkcs8);
    }

    private static String validateData(byte[] decryptedData) {
        String dataStr = new String(decryptedData, Charset.defaultCharset());
        if (dataStr!=null && dataStr.length() > 0){
            String[] split = dataStr.split("#");
            if (split.length > 1 && split[split.length-1].length() == String.valueOf(new
Date().getTime()).length()) {
                try {
                    if (new Date().getTime() - Long.parseLong(split[split.length-1]) < 5*60*1000L){
                        return dataStr.substring(0,dataStr.length()-1-split[split.length-1].length());
                    }else {
                        throw new RuntimeException("operate time out");
                    }
                } catch (Exception e) {
                    throw new  RuntimeException("wrong timestamp ", e);
                }
            }else {
                return dataStr;
            }
        }
        return null;
    }
}
```

4.2 对 OIDC 协议中的 id_token 进行验证

步骤1 登录OneAccess管理门户，选择“设置 > 服务配置”。

步骤2 在服务配置页面，单击“OIDC”。

步骤3 在OIDC页面，单击“OIDC设置”。

步骤4 获取jwks_uri地址。

"authorization_endpoint": "https://t[redacted]cudoneaccess.com/api/v1/oauth2/authorize", "token_endpoint": "https://t[redacted]cess.com/api/v1/oauth2/token", "issuer": "https://test-[redacted]access.com/api/v1/oauth2", "jwks_uri": "https://t[redacted]cess.com/api/ecb/oauth2/keys", "scopes_supported": ["openid"], "grant_types_supported": ["authorization_code", "refresh_token", "implicit"], "request_uri_parameter_supported": true, "subject_types_supported": ["public"], "userinfo_endpoint": "https://t[redacted]cess.com/api/v1/oauth2/userinfo", "id_token_signing_alg_values_supported": ["RS256", "RS384", "RS512"], "display_values_supported": ["page"], "claim_types_supported": ["normal"], "claims_supported": ["mfa", "amd", "nbf", "sub", "exp", "iat", "jti"]}

步骤5 在浏览器中输入jwks_uri地址，根据创建的OIDC应用中的签名加密方式获取密钥，如RS512取下图中红框内容。

{"keys": [{"kty": "RSA", "kid": "54ee4e[redacted]", "use": "sig", "alg": "RS384", "n": "lbPd30wAJ8BKfqrs12t[redacted]", "e": "AQAB"},
{"kty": "RSA", "kid": "a9b2c31d8b814[redacted]", "use": "sig", "alg": "RS512", "n": "ewBC9C9CTTnZ4bP_5Fcmgdd6yZaIlq[redacted]", "e": "AQAB"},
{"kty": "RSA", "kid": "e8b2d7f67e3446[redacted]", "use": "sig", "alg": "RS256", "n": "1MMO9LHBlaMD2MbfKqwMMbZWcv7v3[redacted]", "e": "AQAB"}]}

步骤6 使用该密钥对id_token进行验证。

----结束

4.3 错误码

状态码	错误码	错误信息	描述	处理措施
400	APP.0001	Application does not exist.	应用不存在	请检查对应应用是否存在
400	APP.0002	Application ID required.	应用ID不能为空	请检查入参中的应用ID字段是否为空
400	APP.0003	Application disabled.	应用已禁用	请联系管理员或换一个未禁用的应用再试
400	APP_ACCOUNT.0001	Application account does not exist.	应用账号不存在	请检查对应应用账号是否存在
400	APP_ACCOUNT.0002	Application account already exists.	应用账号已存在	更换未添加过的应用账号
400	APP_ACCOUNT.0003	Unsupported application account.	不支持此应用账号类型	请检查应用账号类型是否正确
400	APP_ACCOUNT.0004	Unsupported application account permission.	不支持此应用账号权限类型	请检查应用账号权限类型是否正确

状态码	错误码	错误信息	描述	处理措施
400	APP_ACCOUNT.0006	Public account does not exist.	应用公共账号不存在	请检查对应应用公共账号是否存在
400	APP_ACCOUNT.0007	Extended attribute does not exist.	应用账号扩展属性不存在	请检查对应应用账号扩展属性是否存在
400	APP_ACCOUNT.0008	The name of the application account required.	应用账号名称不能为空	请检查入参中的应用账号名称字段是否为空
400	APP_ACCOUNT.0035	Application account name required.	应用账号名不能为空	请检查入参中的应用账号名字段是否为空
400	APP_ACCOUNT.0036	Application account name invalid.	应用账号名不符合校验规则	请检查入参中的应用账号名字段是否符合校验规则
400	APP_ORG.0001	Application organization does not exist.	应用机构不存在	请检查对应应用机构是否存在
400	APP_ORG.0002	Application organization is not enabled.	应用机构未开启	请检查对应应用是否开启应用机构
400	APP_ORG.0003	Application organization code already exists.	应用机构编码已存在	更换未添加过的应用机构编码
400	APP_ORG.0004	Parent application organization does not exist.	父级应用机构不存在	请检查对应应用机构是否存在
400	APP_ORG.0005	Application organization cannot be modified.	应用机构不能被修改	请检查对应应用是否是租户名下的应用
400	APP_ORG.0006	Application organization and its parent must be different.	父级应用机构和应用机构不能是同一个	请检查父级应用机构是否和应用机构是同一个机构

状态码	错误码	错误信息	描述	处理措施
400	APP_ORG.0007	Application organizations cannot be deleted.	应用机构不能被删除	请检查对应应用机构下是否存在子机构或用户
400	APP_ORG.0008	Application organization code required.	应用机构编码不能为空	请检查入参中的应用机构编码字段是否为空
400	APP_ORG.0009	Application organization name required.	应用机构名称不能为空	请检查入参中的应用机构名称字段是否为空
400	APP_ORG.0010	Application organization name already exists.	应用机构名称已存在	更换同层级下未添加过的应用机构名称
400	APP_ORG.0011	Invalid application organization code.	应用机构编码不符合校验规则	请检查入参中的应用机构编码字段是否符合校验规则
400	APP_ORG.0012	Invalid application organization name.	应用机构名称不符合校验规则	请检查入参中的应用机构名称字段是否符合校验规则
400	APP_ROLE.0001	Application role does not exist.	应用角色不存在	请检查对应应用角色是否存在
400	APP_ROLE.0002	Application role is not enabled.	应用角色未开启	请检查对应应用是否开启应用角色
400	APP_ROLE.0003	Application role already exists.	应用角色已存在	更换未添加过的应用角色
400	APP_ROLE.0004	Application role is bound to accounts.	应用角色存在账号绑定	请先解绑应用账号
400	APP_ROLE.0005	Application role code required.	应用角色代码不能为空	请检查入参中应用角色代码是否为空
400	APP_ROLE.0006	Application role code invalid.	应用角色代码不符合校验规则	请检查入参中的应用角色代码字段是否符合校验规则

状态码	错误码	错误信息	描述	处理措施
400	APP_ROLE.0007	Application role name required.	应用角色名称不能为空	请检查入参中应用角色名称是否为空
400	APP_ROLE.0008	Application role name invalid.	应用角色名称不符合校验规则	请检查入参中的应用角色名称字段是否符合校验规则
400	CAPTCHA.0002	Invalid CAPTCHA code.	图形验证码校验失败	请检查输入项是否正确并重新调用
400	CAPTCHA.0003	CAPTCHA token expired.	图形验证码校验通过令牌已失效	请重新获取和校验图形验证码后再调用
400	CAPTCHA.0004	Invalid CAPTCHA token.	图形验证码校验通过令牌校验失败	输入的令牌和校验图形验证码中返回的令牌不一致
400	CAPTCHA.0005	Unsupported scenario.	不支持此发送场景	请检查发送方式是否正确
400	CAPTCHA.0006	Failed to send the verification code.	验证码发送失败	请检查输入项是否正确并重新调用
400	CAPTCHA.0007	Incorrect verification code.	验证码不正确	请检查输入的验证码是否正确
400	COM.0002	System busy. Please try again later.	系统繁忙，请稍后重试	请联系管理员
400	LOGIN.0001	User has been locked due to multiple login failures. It will be unlocked in {0} minutes and {1} seconds.	由于多次登录失败，用户已被锁定。 它将在 {0} 分钟和 {1} 秒内解锁	请解锁后重试
400	LOGIN.0002	Invalid account name or password. Remaining attempts: {0}	无效的账号或密码。 剩余次数:{0}	请检查输入的用户名或密码是否正确
400	LOGIN.0003	id_token generate error.	id_token 生成失败	请检查输入的用户名或密码是否正确

状态码	错误码	错误信息	描述	处理措施
400	MOBILE.0002	Unauthenticated mobile number.	未经认证的手机号	请检查输入的手机号是否正确
400	ORG.0001	Organization does not exist.	组织不存在	请检查对应组织是否存在
400	ORG.0002	Parent organization does not exist.	父级组织不存在	请检查对应父组织是否存在
400	ORG.0010	Organization code required.	组织编码不能为空	请检查组织编码
400	ORG.0011	Organization name required.	组织名称不能为空	请检查入参中的组织名称字段是否为空
400	ORG.0012	Organization code already exists.	组织编码已存在	更换未添加过的组织编码
400	ORG.0014	Invalid organization code.	组织编码不符合校验规则	请检查入参中的组织代码字段是否符合校验规则
400	ORG.0015	Invalid organization name.	组织名称不符合校验规则	请检查入参中的组织名称字段是否符合校验规则
400	ORG.0016	Organizations cannot be deleted.	组织不能被删除	请检查对应组织下是否存在子组织或用户
400	ORG.0017	Organization and its parent must be different.	父组织与当前组织不允许重复	请检查父组织与当前组织不允许重复
400	PAGE.0001	Number of records per page is invalid.	每页数量不符合校验规则	请检查输入每页数量
400	PARAM.0001	Incomplete device information.	设备信息不完整	请检查输入的设备信息是否完整
400	PARAM.0002	clientId required.	clientId不能为空	请检查输入的clientId是否为空

状态码	错误码	错误信息	描述	处理措施
400	PARAM.0004	Coordinates required.	坐标信息不能为空	请检查输入的坐标信息是否为空
400	PARAM.0005	Token required.	图形验证码身份令牌不能为空	请检查输入的图形验证码身份令牌是否为空
400	PARAM.0006	Sender required.	发送方不能为空	请检查输入的发送方是否为空
400	PARAM.0007	Scenario required.	发送场景不能为空	请检查输入的发送场景是否为空
400	PARAM.0008	CAPTCHA token required.	图形验证码校验通过令牌不能为空	请检查输入的图形验证码校验通过令牌是否为空
400	PARAM.0009	Verification code required.	验证码不能为空	请检查输入的验证码是否为空
400	PARAM.0010	Account required.	账号不能为空	请检查输入的账号是否为空
400	PARAM.0011	WeChat authorization code required.	微信授权码不能为空	请检查输入的微信授权码是否为空
400	PARAM.0012	Alipay authorization code required.	支付宝授权码不能为空	请检查输入的支付宝授权码是否为空
400	PARAM.0013	State token required.	临时令牌不能为空	请检查输入的临时令牌是否为空
400	PARAM.0014	Invalid state token.	临时令牌无效	请检查输入的临时令牌是否正确
400	PARAM.0017	PARAM.0017	社交ID不能为空	请检查输入的社交ID是否为空
400	PARAM.0018	Old password required.	原密码不能为空	请检查入参中的原密码字段是否为空
400	PARAM.0019	New password required.	新密码不能为空	请检查入参中的新密码字段是否为空
400	PARAM.0020	Old and new passwords must be different.	原密码和新密码不能一致	请检查输入的原密码和新密码是否一致
400	PARAM.0028	Old password is incorrect.	原密码校验失败	请重新输入密码

状态码	错误码	错误信息	描述	处理措施
400	PARAM.0029	Invalid list.	集合大小不符合校验规则	请检查入参中的集合大小是否符合校验规则
400	PARAM.0030	Signature invalid or expired.	签名无效或已过期	请重新生成签名后再试
400	PARAM.0031	SSO ticket required.	一次性令牌不能为空	请检查输入的一次性令牌是否为空
400	PARAM.0032	SSO ticket invalid or expired.	一次性令牌无效或已过期	请重新获取一次性令牌后再试
400	PWD.0001	Historical passwords cannot be used.	不允许使用历史密码	不允许使用历史密码，请重新输入密码
400	PWD.0002	Password cannot be the username spelled backwards.	密码不允许使用用户名的倒写	密码不允许使用用户名的倒写，请重新输入密码
400	PWD.0003	Password cannot include username, mobile number, or email prefix.	密码中不允许包含：用户名、手机号、邮箱前缀、姓名拼音	密码中不允许包含：用户名、手机号、邮箱前缀、姓名拼音，请重新输入密码
400	PWD.0004	Weak password.	密码复杂度低	密码复杂度低，请重新输入密码
400	PWD.0005	Weak password.	该密码为弱密码	该密码为弱密码，请重新输入密码
400	PWD.0006	Max. {0} identical characters in password.	密码中最大字符重复数不能超过{0}	密码中最大字符重复数不能超过{0}，请重新输入密码
400	PWD.0007	Password must be {0} to {1} characters.	密码长度为{0}~{1}个字符	密码长度为{0}~{1}个字符，请重新输入密码
400	PWD.0008	Password required.	密码不能为空	请检查输入的密码是否为空

状态码	错误码	错误信息	描述	处理措施
400	SOCIAL.0001	Social media account already bound to another account. Unbind them first.	社交账号已绑定，请先解绑	请检查社交账号是否已绑定，或换个手机号进行绑定
400	USER.0001	User does not exist.	用户不存在	请检查对应用户是否存在
400	USER.0004	User disabled.	姓氏不能为空	请联系管理员
400	USER.0008	Username required.	用户名不能为空	请检查入参中的用户名字段是否为空
400	USER.0009	Name required.	姓名不能为空	请检查入参中的姓名字段是否为空
400	USER.0010	Mobile number required.	手机号不能为空	请检查入参中的手机号字段是否为空
400	USER.0011	Email address required.	邮箱不能为空	请检查入参中的邮箱字段是否为空
400	USER.0012	First name required.	名字不能为空	请检查入参中的名字字段是否为空
400	USER.0013	Middle name required.	中间名不能为空	请检查入参中的中间名字段是否为空
400	USER.0014	Last name required.	姓氏不能为空	请检查入参中的姓氏字段是否为空
400	USER.0015	Nickname required.	昵称不能为空	请检查入参中的昵称字段是否为空
400	USER.0016	Birth date required.	生日不能为空	请检查入参中的生日字段是否为空
400	USER.0017	Gender required.	性别不能为空	请检查入参中的性别字段是否为空
400	USER.0018	ID type required.	证件类型不能为空	请检查入参中的证件类型字段是否为空
400	USER.0019	ID number required.	证件号码不能为空	请检查入参中的证件号码字段是否为空

状态码	错误码	错误信息	描述	处理措施
400	USER.0020	Country/ region required.	国家或地区不能为空	请检查入参中的国家或地区字段是否为空
400	USER.0021	City required.	城市不能为空	请检查入参中的城市字段是否为空
400	USER.0022	Employee ID required.	工号不能为空	请检查入参中的工号字段是否为空
400	USER.0024	Immediate supervisor required.	直属上级不能为空	请检查入参中的直属上级字段是否为空
400	USER.0026	On-boarding date required.	入职时间不能为空	请检查入参中的入职时间字段是否为空
400	USER.0027	Office location required.	工作所在地不能为空	请检查入参中的工作所在地字段是否为空
400	USER.0028	Extended attribute {0} required.	扩展属性{0}不能为空	请检查入参中的扩展属性{0}字段是否为空
400	USER.0029	Username already exists.	用户名已存在	更换未添加过的用户名
400	USER.0030	Mobile number already exists.	手机号已存在	更换未添加过的手机号
400	USER.0031	Email address already exists.	邮箱已存在	更换未添加过的邮箱
400	USER.0032	ID number already exists.	证件号码已存在	更换未添加过的证件号码
400	USER.0033	Employee ID already exists.	工号已存在	更换未添加过的工号
400	USER.0035	Extended attribute {0} already exists.	扩展属性{0}已存在	更换未添加过的扩展属性{0}
400	USER.0036	Invalid username.	用户名不符合校验规则	请检查入参中的用户名字段是否符合【管理门户-用户-用户属性定义】中的校验规则

状态码	错误码	错误信息	描述	处理措施
400	USER.0037	Invalid name.	姓名不符合校验规则	请检查入参中的姓名字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0038	Invalid mobile number.	手机号不符合校验规则	请检查入参中的手机号字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0039	Invalid email address.	邮箱不符合校验规则	请检查入参中的邮箱字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0040	Invalid first name.	名字不符合校验规则	请检查入参中的名字字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0041	Invalid middle name.	中间名不符合校验规则	请检查入参中的中间名字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0042	Invalid last name.	姓氏不符合校验规则	请检查入参中的姓氏字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0043	Invalid nickname.	昵称不符合校验规则	请检查入参中的昵称字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0044	Invalid birth date.	生日不符合校验规则	请检查入参中的生日字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0045	Invalid gender.	性别不符合校验规则	请检查入参中的性别字段是否符合【管理门户-用户-用户属性定义】中的校验规则

状态码	错误码	错误信息	描述	处理措施
400	USER.0046	Invalid ID type.	证件类型不符合校验规则	请检查入参中的证件类型字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0047	Invalid ID number.	证件号码不符合校验规则	请检查入参中的证件号码字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0048	Invalid country or region.	国家或地区不符合校验规则	请检查入参中的国家或地区字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0049	Invalid city.	城市不符合校验规则	请检查入参中的城市字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0050	Invalid employee ID.	工号不符合校验规则	请检查入参中的工号字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0052	Invalid immediate supervisor.	直属上级不符合校验规则	请检查入参中的直属上级字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0053	Invalid user type.	人员类型不符合校验规则	请检查入参中的人员类型字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0054	Invalid on-boarding date.	入职时间不符合校验规则	请检查入参中的入职时间字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0055	Invalid office location.	工作所在地不符合校验规则	请检查入参中的工作所在地字段是否符合【管理门户-用户-用户属性定义】中的校验规则

状态码	错误码	错误信息	描述	处理措施
400	USER.0056	Extended attribute {0} is invalid.	扩展属性{0}不符合校验规则	请检查入参中的扩展属性{0}字段是否符合【管理门户-用户-用户属性定义】中的校验规则
400	USER.0061	User ID required.	用户ID不能为空	请检查入参中的用户ID字段是否为空