QQ截图20180104161235 **创意感动生活** **The Creative Life**

**TCL 客户API对接文档**

**TCL 版权所有**

**内部资料 注意保密**

QQ截图20180104161235 **创意感动生活** **The Creative Life**

**Life**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本号** | **更新内容** | **操作人** | **操作时间** |
| **V1.0** | **初稿** | **赖志远** | **2018-01-05** |

# 一、获取token

## 1、请求地址：

[https://xxxxxx/v1/b2bapi/oauth/token](https://xxxxxx/oauth/token)/access

## 2、请求方式：

POST

## 3、请求格式

JSON

## 4、请求参数说明：

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | **类型** | **是否必须** | **描述** |
| client\_id | String | 是 | 分配给客户应用的Id |
| client\_secret | String | 是 | Oauth2颁发的动态令牌 |
| grant\_type | String | 是 | 固定值client\_credentials |
| status | String | 可选 | OAuth会原值不动返回 |

## 5、请求参数示例：

{

"client\_id": "d843f6822b1b4fb5a3d244137",

"client\_secret": "4907e71a46aab501024cadbd8",

"grant\_type": "client\_credentials",

"status": "ok"

}

## 6、返回参数说明：

|  |  |  |
| --- | --- | --- |
| **名称** | **类型** | **描述** |
| code | String | 程序处理结果响应码 |
| msg | String | 程序处理结果描述 |
| data | Object | 参看data数据结构描述 |

**data数据结构描述：**

|  |  |  |
| --- | --- | --- |
| **名称** | **类型** | **描述** |
| access\_token | String | 令牌 |
| expires\_in | String | 令牌的倒计时有效期，单位秒 |
| refresh\_token | String | 下次刷新token令牌 |
| status | String | OAuth会原值不动返回 |

**在上面的返回参数中，程序处理结果响应码具体描述如下：**

|  |  |  |
| --- | --- | --- |
| **名称** | **类型** | **描述** |
| 8200 | String | 处理成功 |
| 8400 | String | 请求参数grant\_type为空 |
| 8401 | String | 请求参数client\_id为空 |
| 8402 | String | 请求参数client\_secret为空 |
| 8408 | String | 不支持的grant\_type类型 |
| 8409 | String | client\_id未注册 |
| 8410 | String | client\_secret动态安全码错误 |
| 8411 | String | 该客户端处于停用状态 |
| 8412 | String | 不合法IP |
| 8413 | String | 初始化token次数超出规定的规则范围 |
| 8500 | String | OAuth认证服务器系统错误 |

## 7、返回参数示例：

{

"code": "8200",

"msg": "请求处理成功",

"data": {

"access\_token": "d843f6822b1b4fb5a3d244137",

"expires\_in": "604800",

"refresh\_token": "4907e71a46aab501024cadbd8",

"status": "ok"

}

}

# 二、刷新token

**如果访问资源时返回的error为8415，则说明token已经过期。**

## 1、请求地址

[https://xxxxxx/v1/b2bapi/oauth/token](https://xxxxxx/oauth/token)/access

## 2、请求方式

POST

## 3、请求格式

JSON

## 4、请求参数说明

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | **类型** | **是否必须** | **描述** |
| grant\_type | String | 是 | 固定值refresh\_token |
| status | String | 可选 | OAuth会原值不动返回 |
| refresh\_token | String | 是 | 上次获取token返回的refresh\_token |

## 5、请求参数示例

{

"grant\_type": "refresh\_token",

"refresh\_token": "7e71a46aab501024ca",

"status": "ok"

}

## 6、返回参数说明

|  |  |  |
| --- | --- | --- |
| **名称** | **类型** | **描述** |
| code | String | 程序处理结果响应码 |
| msg | String | 程序处理结果描述 |
| data | Object | 参看data数据格式描述 |

**data数据格式描述：**

|  |  |  |
| --- | --- | --- |
| **名称** | **类型** | **描述** |
| access\_token | String | 令牌 |
| expires\_in | String | 令牌的倒计时有效期，单位秒 |
| refresh\_token | String | 下次刷新token令牌 |
| status | String | OAuth会原值不动返回 |

**在上面的返回参数中，程序处理结果响应码具体描述如下：**

|  |  |  |
| --- | --- | --- |
| **名称** | **类型** | **描述** |
| 8200 | String | 请求处理成功 |
| 8400 | String | 请求参数grant\_type为空 |
| 8401 | String | 请求参数client\_id为空 |
| 8402 | String | 请求参数client\_secret为空 |
| 8408 | String | 不支持的grant\_type类型 |
| 8409 | String | client\_id未注册 |
| 8410 | String | client\_secret动态安全码错误 |
| 8411 | String | 该客户端处于停用状态 |
| 8412 | String | 不合法IP |
| 8414 | String | 刷新token次数超出规定的规则范围 |
| 8416 | String | refresh\_token过期 |
| 8500 | String | OAuth认证服务器系统错误 |

## 7、返回参数示例

{

"code": "8200",

"msg": "请求处理成功",

"data": {

"access\_token": "d843f6822b1b4fb5a3d244137",

"expires\_in": "604800",

"refresh\_token": "4907e71a46aab501024cadbd8",

"status": "ok"

}

}

# 三、OAuth认证服务关键点描述

## 1、 token初始化

当每次客户端访问获取token请求时（grant\_type=”client\_credentials”），OAuth 认证服务器会重新生成新的token和refresh\_token;

## 2、token有效期

新生成的token有效期为604800 秒(7天)， refresh\_token有效期为15552000秒（半年）;

## 3、token安全限制

30天内同一个客户端获取token次数最大为202次；（理论上可以理解为从对接客户方第一次获取token后每隔30天内允许双方token缓存服务器重启公共次数为200次）;

30天内同一个客户端刷新token次数最大为35次;

## 4、token正确使用方式

当对接客户方准备访问某个第三方资源时，应该先判断服务器数据库或缓存是否存在OAuth认证服务器发放的token，这里有两种情况：

1. 如果不存在，则发起获取token请求（rant\_type=”client\_credentials”）到认证服务器，这时认证服务器会首次或重新生成该客户端（client\_id）的token和refresh\_token，并将token和refresh\_token返回给客户端；届时客户端应该将接受到的token和refresh\_token保存或覆盖数据库或缓存中旧的token和refresh\_token；然后携带token及其它业务参数请求第三方资源服务器;
2. 如果存在则直接携带该token及其它业务参数请求第三方资源服务器。如果第三方返回token过期的告知信息，则携带refresh\_token发起刷新token请求（grant\_type=”refresh\_type”）到OAuth认证服务器。如果认证服务器返回refresh\_token过期告知信息，则沿用上面第一点的逻辑，如果认证服务器正常返回新的token，同样参考第一点的处理新token的逻辑

## 5、其他

关于第3点提到的客户端不必做任何额外的逻辑判断，这个主要防止外部恶意攻击，正常使用（严格按照第4点的要求来使用）不应该超过这个数的；

# 四、验证token有效期和资源权限

## 1、请求地址

[https://xxxxxx/v1/b2bapi/oauth/token](https://xxxxxx/oauth/token)/verify

## 2、请求方式

POST

## 3、请求格式

JSON

## 4、请求参数说明

|  |  |  |  |
| --- | --- | --- | --- |
| **名称** | **类型** | **是否必须** | **描述** |
| grant\_type | String | 是 | 固定值client\_credentials |
| access\_token | String | 是 | 需要验证的access\_token |
| resource\_code | String | 是 | OAuthon认证服务注册的资源编码 |
| resource\_owner | String | 是 | 资源所属类型编码 |
| client\_ip | String | 是 | 发送access\_token源客户端ip |

## 请求参数示例

{

"grant\_type": "client\_credentials",

"access\_token": "d519d7f0f7044258aa912c204511a203",

"resource\_code": "query.stock.by.customer.no",

"resource\_owner": "SGAPI20180115",

"client\_ip": "47.156.12.09"

}

## 6、返回参数说明

|  |  |  |
| --- | --- | --- |
| **名称** | **类型** | **描述** |
| code | String | 程序处理结果响应码 |
| msg | String | 程序处理结果描述 |

**在上面的返回参数中，程序处理结果响应码具体描述如下：**

|  |  |  |
| --- | --- | --- |
| **名称** | **类型** | **描述** |
| 8201 | String | token和对应资源权限有效 |
| 8400 | String | 请求参数grant\_type为空 |
| 8404 | String | 请求参数access\_token为空 |
| 8405 | String | 请求参数resource\_owner为空 |
| 8406 | String | 请求参数resource\_code为空 |
| 8407 | String | 资源未注册 |
| 8408 | String | 不支持的grant\_type类型 |
| 8412 | String | 客户端IP不合法 |
| 8415 | String | token过期 |
| 8500 | String | OAuth认证服务器系统错误 |
| 8419 | String | 请求参数client\_ip为空 |
| 8420 | String | 不合法应用IP |
| 8421 | String | 资源权限不足 |
| 8422 | String | 资源所属类型编码未注册 |

## 7、返回参数示例

{

"code": "8201",

"msg": "token和对应资源权限有效"

}

**完毕**