OAuth 2.0 使用说明

目录

[1 关于OAuth 2.0 2](#_Toc392144361)

[1.1 角色 3](#_Toc392144362)

[1.2 名词解释 3](#_Toc392144363)

[2 Authorization Code Grant的使用 3](#_Toc392144364)

[2.1 授权过程 4](#_Toc392144365)

[2.2 授权接口地址、参数和返回值 5](#_Toc392144366)

[2.3 令牌接口地址、参数和返回值 6](#_Toc392144367)

[3 Implicit Grant 的使用 7](#_Toc392144368)

[3.1 授权过程 8](#_Toc392144369)

[3.2 授权接口地址、参数和返回 8](#_Toc392144370)

[4 Client Credentials Grant的使用 9](#_Toc392144371)

[4.1 授权过程 10](#_Toc392144372)

[4.2 令牌接口地址、参数和返回 10](#_Toc392144373)

[5 Refresh Token的使用 11](#_Toc392144374)

[5.1 令牌接口地址、参数和返回值 11](#_Toc392144375)

[6 OAUTH2.0客户端发起的取消授权 12](#_Toc392144376)

[6.1 令牌接口地址、参数和返回值 12](#_Toc392144377)

[7 错误列表 13](#_Toc392144378)

[7.1 错误返回参数 13](#_Toc392144379)

[7.2 错误码列表 13](#_Toc392144380)

[8 授权信息维护 14](#_Toc392144381)

[9 应用举例 14](#_Toc392144382)

[9.1 第三方系统使用UIS作为用户登录认证 14](#_Toc392144383)

## 关于OAuth 2.0

OAuth 2.0授权框架可以控制第三方应用对HTTPS服务的有限访问，它支持用户对第三方应用的授权也支持对第三方应用的授权。它目前是IETF的开放标准：RFC6749 <http://tools.ietf.org/html/rfc6749>。 OAuth2.0的定义中包含有Authorization Code Grant, Implicit Grant, Resource Owner Password Credentials Grant, Client Credentials Grant 四种主要的授权模式。

TAC为第三方应用复旦大学使用UIS（统一身份认证）的接口服务，之前的服务接口使用了私有协议，必须使用特定的API进行开发，对开发语言有一定的限制。OAuth 2.0由于是开放协议，网络上有适用于各种语言的开源API提供（参见 <http://oauth.net/2>）。另一个重要的改进是用户相关资源的访问可以由用户在授权页面上决定，只有用户授权的信息第三方应用才可以获取。

OAuth 2.0除了可以提供身份验证以外，主要设计为访问各种用户保护的资源，因此，我们将会陆续在TAC的资源服务中添加各种新的资源信息以供访问，这些信息的访问都必须经过用户授权。

## Authorization Code Grant的使用

Authorization Code Grant是最常用的授权方式，它可以应用到所有拥有单独的服务端的场景，即可以作为用户所有资源的授权访问，也可以作为UIS用户认证方式。

### 授权过程

图1 Authorization Code Grant 过程

1. 用户通过浏览器访问接口信息
2. 如果用户尚未登录或者第三方应用还没有用户授权的access\_token则将用户重定向到授权服务器的用户授权页面。
3. 用户浏览器访问TAC上的授权页面，TAC验证用户浏览器带来的第三方应用提供的标识符和redirect\_uri回调地址，验证通过后，如果用户尚未登录过UIS或者UIS登录已超时，TAC将用户重定向到UIS登录页面。如果用户已经进行过UIS登录则跳到5。
4. 用户浏览器访问UIS登录页面，用户完成UIS登录，UIS将用户重定向回授权服务器的授权页面。
5. 用户在授权页面对第三方应用请求访问的资源内容进行授权，完成授权后授权服务器将用户重定向到第三方指定的redirect\_uri，用户的授权码以code参数传回。
6. 用户浏览器访问第三方应用的redirect\_uri回调页面
7. 第三方应用使用code作为参数访问授权服务器的token接口，授权服务器验证第三方应用的标识符、口令和授权码，验证通过后以JSON格式返回访问令牌access\_token，有效期和刷新令牌refresh\_token
8. 第三方应用使用access\_token访问资源服务器上的资源，资源服务器验证access\_token后返回用户授权的信息。
9. 第三方应用完成用户登录或返回用户请求的信息。
10. 当access\_token过期后第三方应用可以向授权服务器发起refresh请求，刷新access\_token和refresh\_token。

### 授权接口地址、参数和返回值

接口地址： <https://tac.fudan.edu.cn/oauth2/authorize.act>

参数表：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数 | 选项 | 说明 | 示例 |
| client\_id | 必须 | 客户端（第三方应用）标识 | example |
| response\_type | 必须 | 返回类型 code | code |
| redirect\_uri | 建议 | 必须与登记的匹配，无此参数返回默认回调页面 | http://example.com  /auth\_callback |
| scope | 可选 | 请求授权的内容，默认为学/工号 | username mobile |
| state | 非常建议 | 客户端状态信息，可用于防止CSRF攻击 | 45fd4834fab |

返回值：

|  |  |  |
| --- | --- | --- |
| 参数 | 说明 | 示例 |
| code | 用户授权码 | 6b8c20d0-91c5-4d05-9dd1-e439f064aa0f |
| state | 客户端状态，与请求相同 | 45fd4834fab |
| scope | 用户实际授权内容 | username |

示例：

请求

https://tac.fudan.edu.cn/oauth2/authorize.act?client\_id=example&response\_type=code&scope=basic%20mobile&state=1234&redirect\_uri= http://example.com/auth\_callback

用户授权页面



图2 用户授权界面

授权回调地址

http://example.com/auth\_callback?client\_id=example&code=d0c08873-6328-43f4-a1a0-2ece098a4aec&scope=basic&state=1234

### 令牌接口地址、参数和返回值

接口地址：<https://tac.fudan.edu.cn/oauth2/token.act>

客户端认证：

request参数方式 client\_id和client\_secret参数

BASIC认证方式 在HTTP Header中加入

Authorization: Basic BASE64(<client\_id>:<client\_secret>)

例：Authorization: Basic ZXhhbXBsZToxMjM0NTY=

参数表：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数 | 选项 | 说明 | 示例 |
| client\_id | 必须 | 客户端（第三方应用）标识 | example |
| client\_secret | 可选 | 客户端口令，参数方式认证使用 | 123456 |
| grant\_type | 必须 | 授权类型 authorization\_code | authorization\_code |
| redirect\_uri | 必须 | 必须与访问授权接口的相同 | http://example.com  /auth\_callback |
| code | 必须 | 授权接口返回的授权码 | 6b8c20d0-91c5-4d05-9dd1-e439f064aa0f |

返回JSON对象属性：

|  |  |  |
| --- | --- | --- |
| 属性 | 说明 | 示例 |
| access\_token | 访问令牌 | 5445d2c4-b968-43cc-9306-ad1af6e54e23 |
| token\_type | 令牌类型 | Bearer |
| expires\_in | 过期时间（单位：秒） | 36000 |
| refresh\_token | 刷新令牌 | faadd371-4793-4987-a492-d02999b77eeb |

示例：

请求

https://tac.fudan.edu.cn/oauth2/token.act?client\_id=example&client\_secret=123456&grant\_type=authorization\_code&code=6b8c20d0-91c5-4d05-9dd1-e439f064aa0f

返回

{

"access\_token":"5445d2c4-b968-43cc-9306-ad1af6e54e23",

"token\_type":"Bearer",

"expires\_in":36000,

"refresh\_token":"faadd371-4793-4987-a492-d02999b77eeb"

}

## Implicit Grant 的使用

Implicit Grant授权方式用于那些没有服务器端的第三方应用，如Javascript。这种方式下访问令牌将通过fragment书签的方式返回到回调地址上。这种方式不能取得刷新令牌，而且使用这种方式授权的客户端建议令牌有效期应该比较短，以免因用户令牌泄露而造成资源数据泄露。

### 授权过程

图3 Implicit Grant授权过程

1. 用户通过浏览器向第三方应用发出访问保护资源请求
2. 如果第三方应用还没有用户授权的access\_token则将用户重定向到授权服务器的用户授权页面。
3. 用户浏览器访问TAC上的授权页面，TAC验证用户浏览器带来的第三方应用提供的标识符和redirect\_uri回调地址，验证通过后，如果用户尚未登录过UIS或者UIS登录已超时，TAC将用户重定向到UIS登录页面。如果用户已经进行过UIS登录则跳到5。
4. 用户浏览器访问UIS登录页面，用户完成UIS登录，UIS将用户重定向回授权服务器的授权页面。
5. 用户在授权页面对第三方应用请求访问的资源内容进行授权，完成授权后授权服务器将用户重定向到第三方指定的redirect\_uri，用户的访问令牌以access\_token参数传回。
6. 用户浏览器访问第三方应用的redirect\_uri回调页面，并通过access\_token访问资源服务器上的资源。

### 授权接口地址、参数和返回 post请求

接口地址： <https://localhost:61580/connection/gettoken>

参数表：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数 | 选项 | 说明 | 示例 |
| client\_id | 必须 | 客户端（第三方应用）标识 Ip 白名单 | example |
| Username | 必须 | 返回类型 token | token |
| password | 可选 | 请求授权的内容，默认为学/工号 | username mobile |

返回值：

|  |  |  |
| --- | --- | --- |
| 参数 | 说明 | 示例 |
| access\_token | 访问令牌 | 5445d2c4-b968-43cc-9306-ad1af6e54e23 |
| token\_type | 令牌类型 | Bearer |
| expires\_in | 过期时间（单位：秒） | 3600 |

示例：

请求

## Client Credentials Grant的使用

Client Credentials用于授权第三方应用访问用户不敏感的数据，第三方应用通过客户端认证后获取访问令牌，这种方式不会生成刷新令牌。

### 授权过程

图4 Client Credentials Grant授权过程

1. 用户通过浏览器向第三方应用发出访问保护资源请求
2. 第三方应用使用它的标识和口令作为参数访问授权服务器的token接口，授权服务器验证第三方应用的标识符、口令和授权码，验证通过后以JSON格式返回访问令牌access\_token，有效期
3. 第三方应用使用access\_token访问资源服务器上的资源，资源服务器验证access\_token后返回用户授权的信息。
4. 第三方应用返回用户请求的信息。

### 令牌接口地址、参数和返回

接口地址：<https://tac.fudan.edu.cn/oauth2/token.act>

客户端认证：

request参数方式 client\_id和client\_secret参数

BASIC认证方式 在HTTP Header中加入

Authorization: Basic BASE64(<client\_id>:<client\_secret>)

例：Authorization: Basic ZXhhbXBsZToxMjM0NTY=

参数表：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数 | 选项 | 说明 | 示例 |
| client\_id | 必须 | 客户端（第三方应用）标识 | example |
| client\_secret | 可选 | 客户端口令，参数方式认证使用 | 123456 |
| grant\_type | 必须 | 授权类型 client\_credentials | client\_credentials |
| scope | 可选 | 请求授权内容 | lesson |

返回JSON对象属性：

|  |  |  |
| --- | --- | --- |
| 属性 | 说明 | 示例 |
| access\_token | 访问令牌 | 5445d2c4-b968-43cc-9306-ad1af6e54e23 |
| token\_type | 令牌类型 | Bearer |
| expires\_in | 过期时间（单位：秒） | 3600 |

示例：

请求

https://tac.fudan.edu.cn/oauth2/token.act?client\_id=example&client\_secret=123456&grant\_type=client\_credentials

返回

{

"access\_token":"3b2ec8d9-7cc8-4382-9f3a-397538f0b400",

"token\_type":"Bearer",

"expires\_in":3600

}

## Refresh Token的使用

刷新令牌接口用于使用Authorization Code Grant方式获得的access\_token过期后，使用同时获得的refresh\_token生成新的access\_token。

### 令牌接口地址、参数和返回值

接口地址：<https://tac.fudan.edu.cn/oauth2/token.act>

客户端认证：

request参数方式 client\_id和client\_secret参数

BASIC认证方式 在HTTP Header中加入

Authorization: Basic BASE64(<client\_id>:<client\_secret>)

例：Authorization: Basic ZXhhbXBsZToxMjM0NTY=

参数表：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数 | 选项 | 说明 | 示例 |
| client\_id | 必须 | 客户端（第三方应用）标识 | example |
| client\_secret | 可选 | 客户端口令，参数方式认证使用 | 123456 |
| grant\_type | 必须 | 授权类型 refresh\_token | refresh\_token |
| refresh\_token | 必须 | 刷新令牌 | e8368dcd-7cb3-4515-b01f-545ad21ea46f |
| scope | 可选 | 请求授权的内容，默认为学/工号 | username mobile |

返回JSON对象属性：

|  |  |  |
| --- | --- | --- |
| 属性 | 说明 | 示例 |
| access\_token | 访问令牌 | dc38f04c-041d-4729-be29-7843cd572476 |
| token\_type | 令牌类型 | Bearer |
| expires\_in | 过期时间（单位：秒） | 36000 |
| refresh\_token | 刷新令牌 | 42848c29-596e-48e4-9e7a-c1da822e646d |

示例：

请求

https://tac.fudan.edu.cn/oauth2/token.act?client\_id=example&client\_secret=123456&grant\_type=refresh\_token&refresh\_token=e8368dcd-7cb3-4515-b01f-545ad21ea46f

返回

{

"access\_token":"dc38f04c-041d-4729-be29-7843cd572476",

"token\_type":"Bearer",

"expires\_in":36000,

"refresh\_token":"42848c29-596e-48e4-9e7a-c1da822e646d"

}

## OAUTH2.0客户端发起的取消授权

此功能属于扩展功能，用于客户端代用户向授权服务器发起取消授权的操作。

### 令牌接口地址、参数和返回值

接口地址：<https://tac.fudan.edu.cn/oauth2/token.act>

客户端认证：

request参数方式 client\_id和client\_secret参数

BASIC认证方式 在HTTP Header中加入

Authorization: Basic BASE64(<client\_id>:<client\_secret>)

例：Authorization: Basic ZXhhbXBsZToxMjM0NTY=

参数表：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数 | 选项 | 说明 | 示例 |
| client\_id | 必须 | 客户端（第三方应用）标识 | example |
| client\_secret | 可选 | 客户端口令，参数方式认证使用 | 123456 |
| grant\_type | 必须 | 授权类型 revoke\_token | revoke\_token |
| access\_token | 必须 | 刷新令牌 | e8368dcd-7cb3-4515-b01f-545ad21ea46f |
| state | 非常建议 | 客户端状态信息，可用于防止CSRF攻击 | 45fd4834fab |

返回JSON对象属性：

|  |  |  |
| --- | --- | --- |
| 属性 | 说明 | 示例 |
| error | 错误代码 | invalid\_request |
| error\_description | 错误描述 | response\_type is required |
| error\_uri | 错误说明网址 |  |
| state | 客户端状态，与请求相同 | 45fd4834fab |

示例：

请求

https://tac.fudan.edu.cn/oauth2/token.act?client\_id=example&client\_secret=123456&grant\_type=revoke\_token&access\_token=e8368dcd-7cb3-4515-b01f-545ad21ea46f

返回

{

"error":0,

"error\_description":"access\_token revoked",

" error\_uri ":””,

" state ":"45fd4834fab "

}

## 错误列表

### 错误返回参数

|  |  |  |
| --- | --- | --- |
| 属性 | 说明 | 示例 |
| error | 错误代码 | invalid\_request |
| error\_description | 错误描述 | response\_type is required |
| error\_uri | 错误说明网址 |  |
| state | 客户端状态，与请求相同 | 45fd4834fab |

### 错误码列表

|  |  |
| --- | --- |
| 错误代码 | 说明 |
| invalid\_request | 非法请求，包括必要参数缺失 |
| invalid\_client | 非法的客户端，客户端标识不存在或者客户端认证失败 |
| unauthorized\_client | 客户端不允许使用该授权方式 |
| access\_denied | 拒绝访问 |
| unsupported\_response\_type | 不支持的response\_type值 |
| unsupported\_grant\_type | 不支持的grant\_type值 |
| invalid\_scope | 请求的scope非法 |
| server\_error | 服务器内部错误 |
| temporarily\_unavailable | 服务暂时不可用 |
| invalid\_grant | code, refresh\_token, access\_token失效或过期 |
| user\_canceled | 用户点击了授权页面中的取消按钮 |

## 授权信息维护

客户端授权管理界面地址：<https://tac.fudan.edu.cn/oauth2/myclient.act>

使用管理员UIS账号登录后，点击列出的客户端名称，列出所有的授权信息，可以删除选中的授权。



图5 客户端授权管理界面

用户授权管理界面地址：<https://tac.fudan.edu.cn/oauth2/myauth.act>

用户UIS登录后，可列出所有的授权信息，可以修改授权或者删除授权



图6 用户授权信息管理界面

## 应用举例

### 第三方系统使用UIS作为用户登录认证

第三方系统信息：

标识：example

口令：123456

回调地址：http://example.com/auth\_callback

步骤：

1. 用户通过浏览器向第三方应用发出登录请求

http://example.com/login

1. 如果用户尚未登录将用户重定向到授权服务器的用户授权页面。将生成的state参数保存在用户的session中留作之后验证用

https://tac.fudan.edu.cn/oauth2/authorize.act?client\_id=example&response\_type=code&state=1234&redirect\_uri= http://example.com/auth\_callback

1. 用户浏览器访问TAC上的授权页面，TAC验证用户浏览器带来的第三方应用提供的标识符和redirect\_uri回调地址，验证通过后，如果用户尚未登录过UIS或者UIS登录已超时，TAC将用户重定向到UIS登录页面。如果用户已经进行过UIS登录则跳到5。
2. 用户浏览器访问UIS登录页面，用户完成UIS登录，UIS将用户重定向回授权服务器的授权页面。
3. 用户在授权页面对第三方应用请求访问的资源内容进行授权，完成授权后授权服务器将用户重定向到第三方指定的redirect\_uri，用户的授权码以code参数传回。

http://example.com/auth\_callback?client\_id=example&code=d0c08873-6328-43f4-a1a0-2ece098a4aec&scope=username&state=1234

1. 用户浏览器访问第三方应用的redirect\_uri回调页面，将用户session中的state信息与回调中的state参数进行比对，比对失败的为CSRF攻击，直接丢弃。
2. 第三方应用使用code作为参数访问授权服务器的token接口，授权服务器验证第三方应用的标识符、口令和授权码，验证通过后以JSON格式返回访问令牌access\_token，有效期和刷新令牌refresh\_token

请求：

https://tac.fudan.edu.cn/oauth2/token.act?client\_id=example&client\_secret=123456&grant\_type=authorization\_code&code= d0c08873-6328-43f4-a1a0-2ece098a4aec

返回JSON：

{

"access\_token":"dc38f04c-041d-4729-be29-7843cd572476",

"token\_type":"Bearer",

"expires\_in":36000,

"refresh\_token":"42848c29-596e-48e4-9e7a-c1da822e646d"

}

1. 第三方应用使用access\_token访问资源服务器上的userinfo接口，资源服务器验证access\_token后返回用户基本信息。

请求：https://tac.fudan.edu.cn/resource/userinfo.act?access\_token=dc38f04c-041d-4729-be29-7843cd572476

返回：

{"department":"100149","email":null,"mobile":null,"user\_id":"04538","user\_name":null,"user\_type":"教职工"}

1. 第三方应用认定UIS用户04538完成认证。

**安全说明：必须使用state参数来防止CSRF攻击，否则可能会被另一个用户冒用登录，尤其是在进行用户身份绑定类型的使用中更要非常小心。**