OAuth2.0 概述

大部分 API 的访问如发表微博、获取私信，关注都需要用户身份，目前新浪微博开放平台用户身份鉴权有 OAuth2.0 和 Basic Auth（仅用于应用所属开发者调试接口），新版接口也仅支持这两种方式。

OAuth2.0 较 1.0 相比整个授权验证流程更简单更安全，也是未来最主要的用户身份验证和授权方式。

关于 OAuth2.0 协议授权流程查看 OAuth2.0 授权流程 ，其中 Client 指第三方应用，Resource Owner 指用户，Authorization Server 是我们的授权服务器，Resource Server 是 API 服务器。

开发者可以先浏览 OAuth2.0 的接口文档，熟悉 OAuth2 的接口及参数的含义，然后我们根据应用场景各自说明如何使用 OAuth2.0。

注意事项：

- 1、OAuth2.0 授权无需申请，任何应用都可以使用。如果开发者需要更长的授权有效期参考本文档授权有效期部分。
- 2、如果你是站外网页应用或客户端应用，出于安全性考虑，需要在平台网站填写 redirect_url（授权回调页），才能使用 OAuth2.0，填写地址：http://open.weibo.com/apps/应用 APPKEY/privilege/oauth 对于客户端，我们也提供了默认的回调页地址。详细请查看授权页功能部分。

接口文档

接口	说明
OAuth2/authorize	请求用户授权 Token
OAuth2/access_token	获取授权过的 Access Token
OAuth2/get_token_info	授权信息查询接口
OAuth2/get_oauth2_token	OAuth1.0 的 Access Token 更换至 OAuth2.0 的 Access Token

授权页

新版授权页改变了之前页面信息元素过多，对用户使用带来干扰的问题，登录和授权这两个行为已在新版中分离，用户能够更好地理解帐号登录和授权的过程，也为未来更多的功能带来承载空间。

当前一个最完整的授权分为三个步骤：登录-普通授权-高级授权（SCOPE）。但这三个步骤并不是必然出现，当用户的新浪微博处于登录状态时，页面会自动 跳转到普通授权页，“高级授权”同样也不是必须，如果开发者不申请 SCOPE 权限，系统会自动跳过此步骤，回调应用。我们在灰度测试中统计发现，只要合理 的使用高级授权，开发者完全不必担心增加操作所带来的页面流失率问题，相反，一个清晰的授权体验更能获取用户的信任。

与此同时，授权项将会变的更加有条理，之前的普通权限将作为基础服务，用户不再有感知，与用户隐私相关的会归到高级授权，用户在授权时有权利逐条取消，进一步增强了隐私控制。

应用场景

开发者需要根据各自的应用场景，选择适用的 **OAuth2.0** 授权流程：

- 1、网站或者站外 Web 应用，请参考：Web 应用的验证授权(Authorization Code)

- 2、桌面和无线客户端应用，请参考：Web 应用的验证授权(Authorization Code)，无线客户端可以直接使用官方 SDK，通过 WebView 方式使用授权页。
- 3、微博站内应用，请参考 站内应用开发指南。

Web 应用的验证授权

基本流程

1. 引导需要授权的用户到如下地址：

```
https://api.weibo.com/oauth2/authorize?
client_id=YOUR_CLIENT_ID&response_type=code&redirect_uri=YOUR_REGISTERED_REDIRECT_URI
```

2. 如果用户同意授权,页面跳转至 YOUR_REGISTERED_REDIRECT_URI/?code=CODE

3. 换取 Access Token

```
https://api.weibo.com/oauth2/access_token?
client_id=YOUR_CLIENT_ID&client_secret=YOUR_CLIENT_SECRET&grant_type=authorization_code&redirect_uri=YOUR_REGISTERED_REDIRECT_URI&code=CODE
```

（其中 client_id=YOUR_CLIENT_ID&client_secret=YOUR_CLIENT_SECRET 可以使用 basic 方式加入 header 中）

返回值

{ "access_token":"SlAV32hkKG", "remind_in ":3600, "expires_in":3600 }

4. 使用获得的 OAuth2.0 Access Token 调用 API

移动应用的验证授权

移动应用（主要指 Mobile Native App），建议使用官方提供的支持 SSO 授权的 SDK, 可以大大简化授权流程开发，降低开发成本。

参考：移动应用 SSO 授权

站内应用的验证授权

参考：站内应用开发指南

使用 OAuth2.0 调用 API

使用 OAuth2.0 调用 API 接口有两种方式：

1. 直接使用参数传递参数名为 access_token
https://api.weibo.com/2/statuses/public_timeline.json?access_token=abcd

2. 在 header 里传递 形式为在 header 里添加 Authorization:OAuth2 空格 abcd 这里的 abcd 假定为 Access Token 的值

其它接口参数正常传递即可。

授权有效期

程序一定要具备足够的健壮性，调用接口时判断接口的返回值，如果用户的 access_token 失效，需要引导用户重新授权。失效原因有以下几个：

1. 用户取消了对应用的授权
2. access_token 自然过期
3. 用户修改了密码，冻结了对应用的授权
4. 新浪发现用户帐号被盗，冻结了用户对应用的授权

授权级别和 OAuth2.0 access_token 有效期对应表：

授权级别	测试	普通	中级	高级	合作
授权有效期	1 天	7 天	15 天	30 天	90 天

注：

1. 只有未过文案审核的应用才处于测试级别。
2. 应用所属开发者授权应用时，有效期为 5 年。

access_token 自动延续方案

如果用户在授权有效期内重新打开授权页授权（如果此时用户有微博登录状态，这个页面将一闪而过），那么新浪会为开发者自动延长 access_token 的生命周期，请开发者维护新授权后得 access_token 值。

如何查询当前应用的授权级别

你可以在 http://open.weibo.com/apps/应用 APPKEY/privilege/oauth 上查询当前应用的授权级别。

如何计算某个用户的 **access_token** 过期时间？

开发者可以通过两种方式计算：

1. 用户授权时，oauth2/access_token 接口返回的 expires_in 值就是 access_token 的生命周期。
2. 从上述对应表中，找到应用所对应的授权有效期，过期时间 = 用户授权时间 + 授权有效期

如何申请授权有效期

可在应用控制台，接口管理标签下的授权机制选项中进行在线申请。

授权页功能

scope

scope 是 OAuth2.0 新版授权页提供的一个功能，通过 scope，平台将开放更多的微博核心功能给开发者，同时也加强用户隐私保护，提升了用户体验，用户在新 OAuth2.0 授权页中有权利选择赋予应用的功能。

scope 开放的接口文档：接口文档

客户端默认回调页

通常 Mobile Native App 没有服务器回调地址，您可以在应用控制台授权回调页处填写平台提供的默认回调页，该页面用户不可见，仅用于获取 access token。

OAuth2.0 客户端默认回调页：https://api.weibo.com/oauth2/default.html

强制登录

授权页会默认读取当前用户的新浪微博登录状态，如果你想让用户重新登录，请在调用 authorize 接口时传入参数：forcelogin=true，默认不填写此参数相当于 forcelogin=false。

取消授权回调页

开发者可以在应用控制台填写取消授权回调页，当用户取消你的应用授权时，开放平台会回调你填写的这个地址。并传递给你以下参数：

source：应用 appkey

uid ：取消授权的用户

auth_end ：取消授权的时间

OAuth2.0 相关资源

以下 **SDK** 包含了 **OAuth2.0** 及新版 **API** 接口

下载 Android SDK	下载 iOS SDK	下载 WP7 SDK
下载 PHP SDK(由 SAE 维护)	下载 Java SDK	下载 Python SDK
下载 Flash SDK	下载 Javascript SDK	下载 C# SDK

移动开发 **SDK** 说明文档

Android SDK 说明文档 iOS SDK 说明文档 WP7 SDK 说明文档

其他参考资料

OAuth 是一种国际通用的授权方式， OAuth2.0 的官方技术说明可参看 http://oauth.net/2/

如果你仍在使用 Oauth1.0，请进入浏览相关文档。

OAuth2.0 错误码

新浪微博 OAuth2.0 实现中，授权服务器在接收到验证授权请求时，会按照 OAuth2.0 协议对本请求的请求头部、请求参数进行检验，若请求不合法或验证未通过，授权服务器会返回相应的错误信息，包含以下几个参数：

- error: 错误码
- error_code: 错误的内部编号
- error_description: 错误的描述信息
- error_url: 可读的网页 URI，带有关于错误的信息，用于为终端用户提供与错误有关的额外信息。

错误信息的返回方式有两种：

1. 当请求授权 Endpoint：https://api.weibo.com/2/oauth2/authorize 时出现错误，返回方式是：跳转到 redirect_uri,并在 uri 的 query parameter 中附带错误的描述信息。

2. 当请求 access token endpoing:https://api.weibo.com/oauth2/access_token 时出现错误，返回方式：返回 JSON 文本。

例如：

{

- "error":"unsupported_response_type",
- "error_code":21329
- "error_description":"不支持的 ResponseType."

}

OAuth2.0 错误响应中的错误码定义如下表所示：

错误码**(error)**	错误编号**(error_code)**	错误描述**(error_description)**
redirect_uri_mismatch	21322	重定向地址不匹配
invalid_request	21323	请求不合法
invalid_client	21324	client_id 或 client_secret 参数无效
invalid_grant	21325	提供的 Access Grant 是无效的、过期的或已撤销的
unauthorized_client	21326	客户端没有权限
expired_token	21327	token 过期
unsupported_grant_type	21328	不支持的 GrantType
unsupported_response_type	21329	不支持的 ResponseType
access_denied	21330	用户或授权服务器拒绝授予数据访问权限
temporarily_unavailable	21331	服务暂时无法访问

OAuth2.0 相关问题

查看 OAuth2.0 相关问题