有生云

统一接口认证(sso_OAuth)文档

产品版本：V2.0

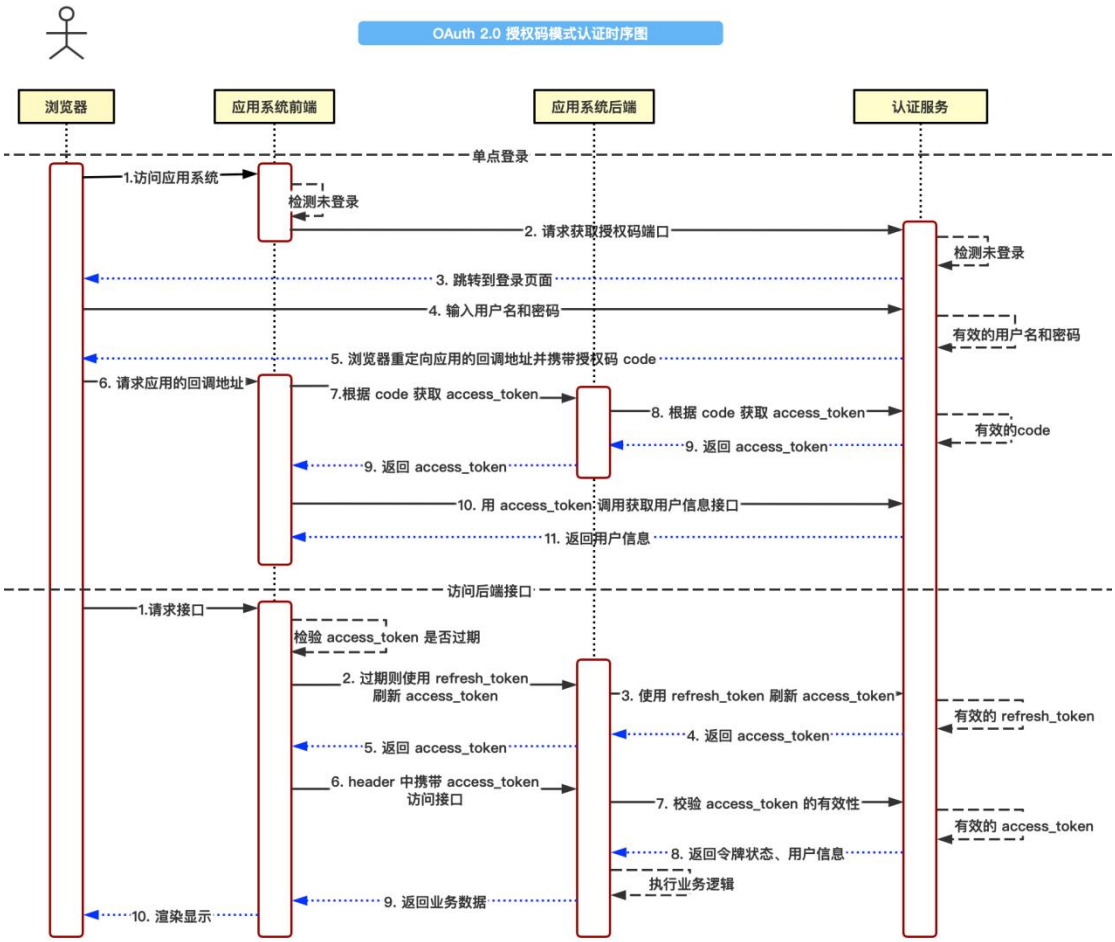
文档版本：202401

北京有生博大软件股份有限公司

目录

统一认证接口

统一身份认证平台将基于 Oauth2.0 协议授权码模式与应用系统实现技术对接。



上图为 OAuth 2.0 授权码模式认证时序图，描述了一个应用的授权认证及访问过程。

上图分两个阶段，阶段一为单点认证阶段：

1) 访问应用系统，应用系统检测未登录。
2) 请求获取授权码端口 /sso/oauth2.0/authorize。
3) 系统检测到用户未登录，重定向至登录页面。
4) 用户输入用户名密码登录。
5) 认证服务认证通过后携带授权码 code 重定向。
6) 浏览器跳转至应用。
7) 应用系统前端调用应用系统后端访问令牌接口
8) 后端资源服务服务器再去调用统一认证 /sso/oauth2.0/accessToken 接口获取访问令牌 access_token。因为 client_secret 存储在后端服务器中更为安全。
9) 认证服务返回访问令牌 access_token 给应用系统后端。
10) 应用系统前端拿到应用系统后端返回的访问令牌 access_token 后将其缓存在本地。

11) 应用通过获取用户信息接口 /sso/oauth2.0/profile 获取用户信息。
12) 认证服务返回用户信息。
阶段二为访问后端接口：

1） 检测应用系统中的，
2） 应用系统前端可先检查访问令牌 access_token 是否过期，过期的令牌可通过调用刷新访问令牌的接口，应用系统前端调用应用系统后端的刷新令牌接口。如果检查访问令牌没有过期可以直接到第六步执行访问接口
3） 应用系统后端再调用统一认证的刷新访问令牌接口/sso/oauth2.0/accessToken 刷新令牌。
4） 认证服务返回访问令牌 access_token 到应用系统后端。
5） 应用系统前端拿到应用系统后端返回的访问令牌 access_token 后将其缓存在本地。
6） 请求应用系统后端接口，并在请求头中带上访问令牌 access_token。
7） 应用系统后端接收到请求后调用统一认证的访问令牌校验接口 /sso/oauth2.0/introspect 进行令牌校验。
8） 校验通过应用系统后端会收到令牌状态、用户信息等返回，之后可继续进行业务的处理。
9） 应用系统前端收到后端返回的业务数据。
10） 浏览器渲染数据显示。
以下是上述过程中会用到的接口：

1. 获取授权码

请求地址：http://ip:port/sso/oauth2.0/authorize
请求方法：GET
描述：授权用户启动身份验证流程，浏览器访问该端口
请求参数：

参数名	描述
response_type	为固定值 code
client_id	申请的客户端 id。
redirect_uri	重定向 url，认证通过后会重定向回来并以授权码 code 作为请求参数。

2. 获取访问令牌

接口地址：http://ip:port/sso/oauth2.0/accessToken
请求方法：POST

描述：通过授权码 code 获取访问令牌

请求参数：

参数名	描述
grant_type	授权类型为固定值 authorization_code。
client_id	申请的客户端 id。
client_secret	申请的客户端密钥。
code	请求授权返回的授权码 code，一个授权码使用一次后便会失效。
redirect_uri	重定向 url。

响应字段：

字段	描述
access_token	访问令牌。
refresh_token	刷新令牌。
token_type	令牌类型。
expires_in	过期时间（秒）。
scope	权限范围。

响应示例：


```
{
  access_token: "AT-54-1EupnbVn1TkmLbALdI-WcvXaoKfzyzHM",
  refresh_token: "RT-54-KpmWKmYFR4Fcqxfn9P4psadOtfvNRo-C",
  token_type: "bearer",
  expires_in: 28800,
  scope: ""
}
```

3. 获取用户信息

接口地址：http://ip:port/sso/oauth2.0/profile

请求方法：GET

描述：获取认证过的用户信息

请求参数：

参数名	描述
access_token	访问令牌

响应字段：

字段	描述
avator	头像 url
CAID	CAID
dn	由 name 组成的父子关系列表(倒序)，之间用逗号分隔
email	邮箱
guidPath	由 ID 组成的父子关系列表(正序)，之间用逗号分隔
IDNum	身份证号
isValidateIE	是否为合法的 IE 版本（针对使用 IE 的情况）
loginName	登录名
loginType	登录类型
mobile	电话号码
name	姓名
oauthClientId	oauth 客户端 id
original	是否为原始账号（针对多岗）
originalID	原始账号 id
parentID	人员父节点 id
password	密码
personID	人员 id
personType	人员类型
roles	角色
sex	性别
tenantID	租户 id
tenantLoginName	租户登录名
tenantManager	是否为租户管理员
tenantName	租户名
service	授权认证的服务 url
id	登录名
client_id	oauth 客户端 id

响应示例：

{
avator: "",
CAID: "",
dn: "cn=系统管理员,ou=临时机构,o=XXX 集团",
email: "",
guidPath:
"4868e899c5034a87a49b5cd9d345de96,dea693bbd9434bc0afdc81701efbf545,4c106ab010ef47858e0acc84f98ea2a1",
IDNum: "",
isValidateIE: "true",
loginName: "admin",
loginType: "loginName",
mobile: "13557738412",
name: "有生系统管理员",
oauthClientId: "clientid",
original: 1,
originalID: "",
parentID: "dea693bbd9434bc0afdc81701efbf545",
password: "20:45:41:09:B4:4F:B4:1F:BD:C4:A9:C6:CC:79:4E:F9:01:06:5F:E6",
personID: "4c106ab010ef47858e0acc84f98ea2a1",
personType: "deptPerson",
roles:
"110414316670487a830302c6cb0b377a,bcf4575777b848a2ac2895d82114c0b8,4077f1d749ea422fafb3dd8edf62c520,4a9ab012256244359d3784ef39571421,33cf7e2e32fd4c1f880dd5c18062a6b4,efcb36000f58463995bf2b4ca3d668f8,81071e045d1844e783b07f6fa1f54fec,13fcfb1ef8d14d60922b894457fb2ac9,6c23871ef38842d4b88a10f3996462f5,b0f5787cd3834fa9b54f61420b7fe3e9,0ac46d6772734d33a8c0cf2791fb38df,9b104ecf820f453d8840a35b7253249e,636559a379a74dc09024065094b85c43,fc188d02dc30491b8902f839c7385a58,fe3a4bbbbc5d4c55890ed61e434235b6,fbc01a1a4f754331bbab077db661eb16,7c1a43e45c034752a9e2c781d0df7cbe,761132882ee949438dc975413490283c,32bdfd9969f343988e6516c6c4a42605,117c27048dfc4af98841b4771f4a64eb",
sex: 1,

tenantID: "f3a988b6825a4f8f90928c4bedaaea15",
tenantLoginName: "risesoft",
tenantManager: true,
tenantName: "北京有生博大软件股份有限公司",
service: "http://localhost:8080/platform",
id: "admin",
client_id: "clientid"
}

4. 刷新访问令牌

接口地址：http://ip:port/sso/oauth2.0/accessToken

请求方法：POST

描述：当访问令牌过期了可通过 refresh_token 去获取新的访问令牌

请求参数：

参数名	描述
grant_type	授权类型为固定值 refresh_token
client_id	申请的客户端 id
client_secret	申请的客户端密钥
refresh_token	刷新令牌

响应示例：


```
{
    access_token: "AT-80-YwO-UIy7ZkDaNHPQRZv5WE8nSFsBiOn7",
    refresh_token: "RT-80-3DQO8G4lkqa9fgMGhVVbrRZqGEPnhakP",
    token_type: "bearer",
    expires_in: 28800,
    scope: ""
}
```

5. 访问令牌校验

接口地址：http://ip:port/sso/oauth2.0/introspect

请求方法：POST

描述：查询访问令牌 access_token 的状态，其中应用的凭证 client_id 和 client_secret 需以 Basic Auth 的形式提供

请求参数：

参数名	描述
token	访问令牌 access_token

请求头：

参数名	描述
Authorization	应用的凭证，参数值为 Basic <Auth> 其中 <Auth> 为经过 base64 编码的 client_id 和 client_secret，即 base64_encode(client_id:client_secret)

响应示例：

{
  "active": true,
  "attr":
"{\"tenantLoginName\":\"risesoft\",\"oauthClientId\":\"clientid\",\"loginType\":\"login
Name\",\"roles\":\"035fc633bc624890bcefdceebf86e487,b3a518829f2443ee806f9d83
31017b48,093e6250f1fd44e0bc1312322e8271f6,5c460016c5c44412ac629a8ff2e7d5c
f\",\"dn\":\"cn=管理员,o=北京有生博大软件股份有限公司
\",\"parentID\":\"4a725fe6f01b41ee9d5670a8bb2702de\",\"IDNum\":\"\",\"password\":
\"3D:4F:2B:F0:7D:C1:BE:38:B2:0C:D6:E4:69:49:A1:07:1F:9D:0E:3D\",\"tenantNa
me\":\"北京有生博大软件股份有限公司
\",\"loginName\":\"swadmin\",\"tenantID\":\"8b60c9b967c947e6b6b5a5fe37525cdb\",
\"personID\":\"8ae05acc257b4a499b5d153db99a2e77\",\"originalID\":\"\",\"personTy
pe\":\"\",\"tenantManager\":true,\"email\":\"\",\"original\":1,\"CAID\":\"_0000000000
000000000000000\",\"sex\":0,\"guidPath\":\"4a725fe6f01b41ee9d5670a8bb2702de,8ae05
acc257b4a499b5d153db99a2e77\",\"mobile\":\"13049111111\",\"isValidateIE\":\"true
\",\"positionId\":\"07a05d2e9b194c378ec7f43b07609732\",\"name\":\"管理员
\",\"avator\":\"\"}",
  "sub": "swadmin",
  "scope": "CAS",
  "iat": 1680765407,
  "exp": 1680794207,
  "realmName": "primaryAuthenticationHandler",
  "uniqueSecurityName": "swadmin",
  "tokenType": "bearer",

"aud": "http://localhost:7070/demo/org?code=OC-9-xgen2Vk68bzklHo3RHzNQ7x7Y5lEDYlN",
"client_id": "clientid",
"grant_type": "authorization_code"
}

6. 退出地址

地址：http://ip:port/sso/logout

说明：只需要在浏览器访问该地址，认证服务端会使当前浏览器登录的用户所访问的所有系统的票据过期，并自动重定向到综合信息平台的登录页面。