**广东省生态环境厅智慧云平台**

**统一身份认证接入指南**

**二〇二〇年9月**

目录

[第一章 接入指南 1](#_Toc50539471)

[1.1 系统介绍 1](#_Toc50539472)

[1.2 接入流程 1](#_Toc50539473)

[1.3 业务场景 2](#_Toc50539474)

[1.4 业务流程 3](#_Toc50539475)

[1.5 接入指南 3](#_Toc50539476)

[1.5.1 系统配置指南 3](#_Toc50539477)

[1.5.2 认证服务开发接入 6](#_Toc50539478)

[1.6 统一身份认证接口 8](#_Toc50539479)

[1.6.1 获取授权码 8](#_Toc50539480)

[1.6.2 以授权码模式获取access\_token 9](#_Toc50539481)

[1.6.3 以密码模式获取access\_token 10](#_Toc50539482)

[1.6.4 校验token有效性 11](#_Toc50539483)

[1.6.5 获取当前登录用户基本信息 12](#_Toc50539484)

[1.6.6 获取当前登录用户详细信息 14](#_Toc50539485)

[1.6.7 用户退出 21](#_Toc50539486)

# 接入指南

## 系统介绍

统一配置系统：该系统用于为应用系统提供参数配置管理功能，核心功能包括：菜单配置、组织管理、部门管理、系统用户、角色授权、系统基础配置。

开放平台系统：该系统为应用支撑平台的外部网站系统，核心模块由数据开放、API开放、应用开放、个人用户中心四部分组成。提供用户注册、企业绑定、个人开发、应用系统接入申请、数据申请等功能。

平台基础系统：负责管理应用，维护应用和企业、组织架构等数据。

统一身份认证：提供统一身份认证、单点登录等认证服务。

应用支撑平台：包含上述系统组成应用支撑平台。

## 接入流程

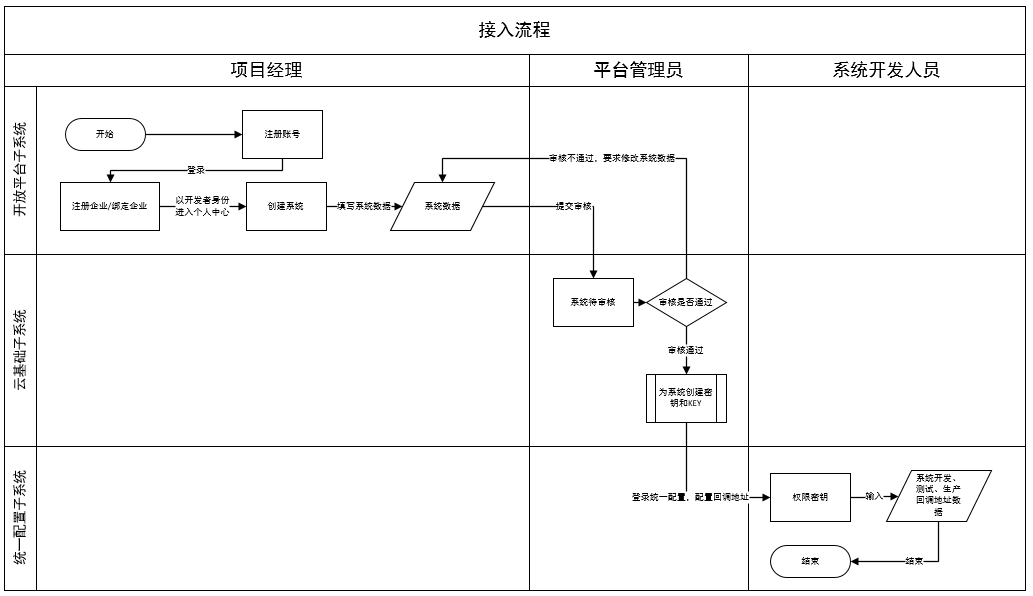


图 5 接入流程图

1. 项目经理通过开放平台注册开发者账号，注册成功后登录开放平台，完成承建商企业账号注册。新企业用户第一次登录系统，需要注册企业信息。已注册企业用户登录系统后，通过企业管理员提供邀请码完成企业信息的绑定。
2. 开发者账号登录开放平台，注册应用系统，勾选平台组件服务，等待后台管理员审核，审核通过后完成系统接入开发；审核不通过，则需重新修改申请信息再次提交审核。
3. 开发者账号登录开放平台，访问统一配置服务组件，查看平台为应用系统分配的密钥和KEY。根据应用系统需求配置测试回调、开发回调、生成回调地址。至此完成统一身份认证接入所需要的信息配置。

## 业务场景

普通用户访问应用系统，第一次未登录情况下，跳转到统一身份认证平台，选择手机号码、本地账号、企业微信、粤政易、微信账号、企业微信中的一种方式进行登录。

应用系统的系统权限分成两种类型，一种是针对指定的平台认证用户开放。一种是面向所有的平台用户开放。

针对第一种情况的应用系统，应用系统获取了认证中心返回的token数据，通过token向统一身份认证中心发起请求获取用户信息。此时认证中心会判断该用户是否有访问该应用的权限。如有则返回用户信息。如无，则返回用户无权限信息，该信息还包括统一身份服务提供的该认证用户无权限页面地址信息。应用系统获取到该信息后，需跳转到该页面。该页面包括提示无权限信息、重新登录按钮、申请权限按钮。重新登录按钮会跳转至新登录页面。申请权限按钮会通知平台该认证用户申请访问该应用系统。业务系统管理员通过开放平台进入统一配置组件，可以对该申请用户进行审核。

针对第二种情况的应用系统，用户通过统一身份认证服务认证后。应用系统可以根据token信息直接获取到用户信息。

至此完成统一用户认证、用户至应用系统之间权限管理的业务场景接入。业务系统可以通过获取到的用户信息完成后续的自身系统初始化工作。

综合所述应用系统统一身份接入包含如下两种业务场景：

1. 应用系统面向所有认证用户开放，应用系统需要接入统一身份认证、单点登录
2. 应用系统面向指定认证用户开放，应用系统需接入统一认证、单点登录服务、用户权限。

上述接入流程差异不大，整体接入流程可以参照附件outh2接入流程完成，在标准统一身份认证基础上，应用系统只需要在获取用户信息时，根据用户信息接口选择、对返回结果处理等操作就能完成权限模块接入。应用系统需要在自身业务系统中集成统一身份认证中心提供的用户中心页面供用户使用。

## 业务流程

普通用户访问业务系统，通过统一认证服务流程如下图所示：

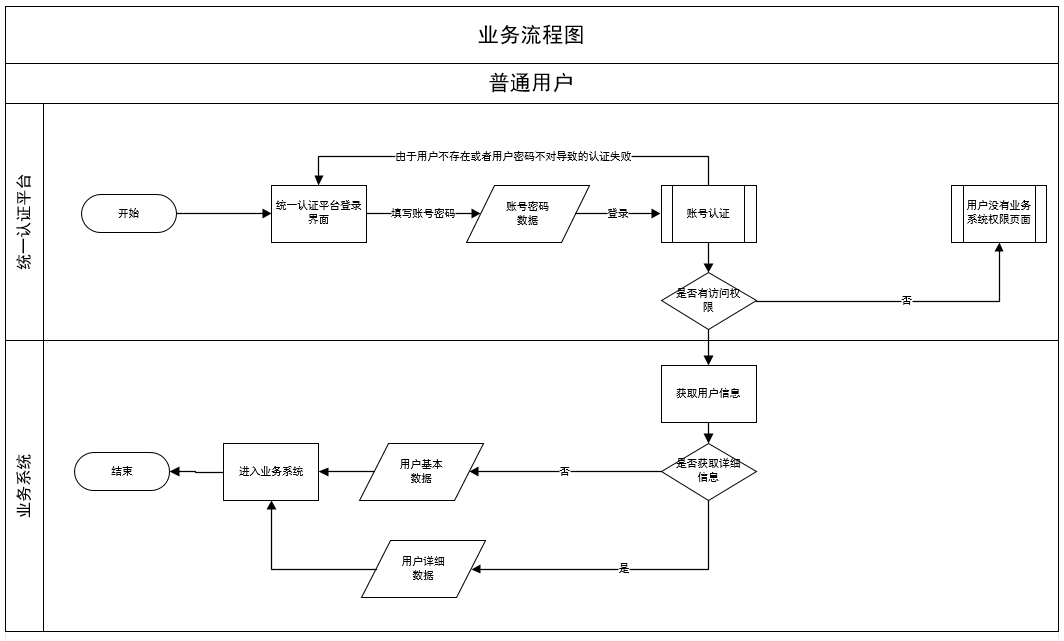


图 6 业务流程图

## 接入指南

### 系统配置指南

登录开放平台地址 https://it.gdeei.cn/OpenPlatform

第一步：访问开放平台注册开发账号



图 7 注册开发账号图

第二步：访问开放平台完成开发商信息绑定或注册



图 8 企业管理员页面图

第三步：访问开放平台创建应用系统，选择需要的服务。



图 9 创建系统图

第四步：访问开放平台统一配置组件，配置应用系统。

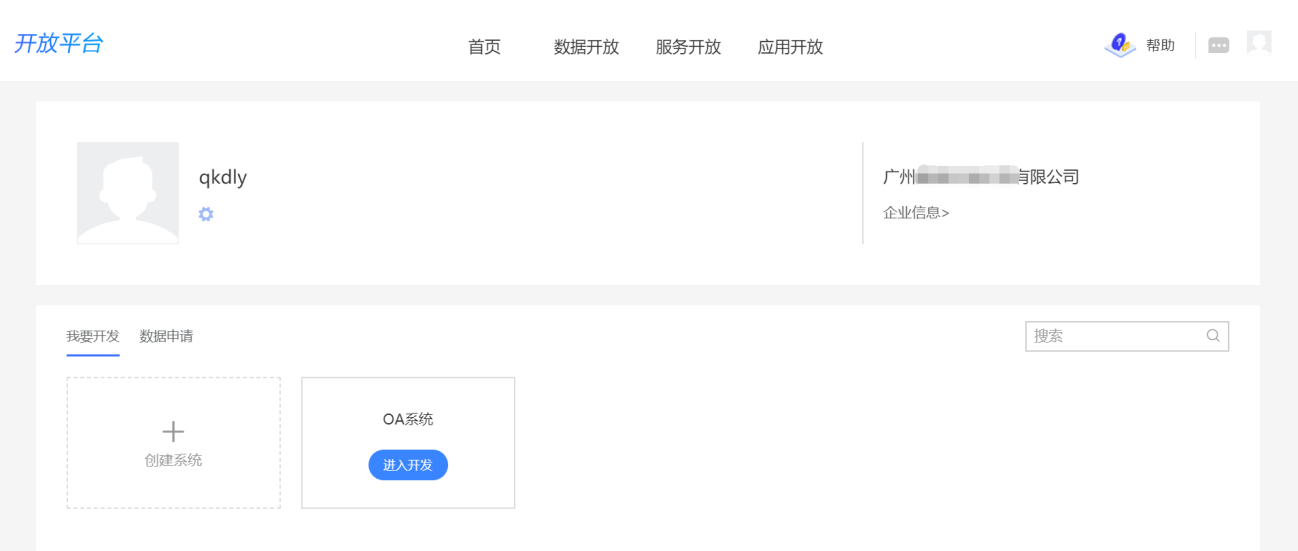


图 10 开发工作台图



图 11 系统组件图



图 12 系统用户访问权限策略配置图

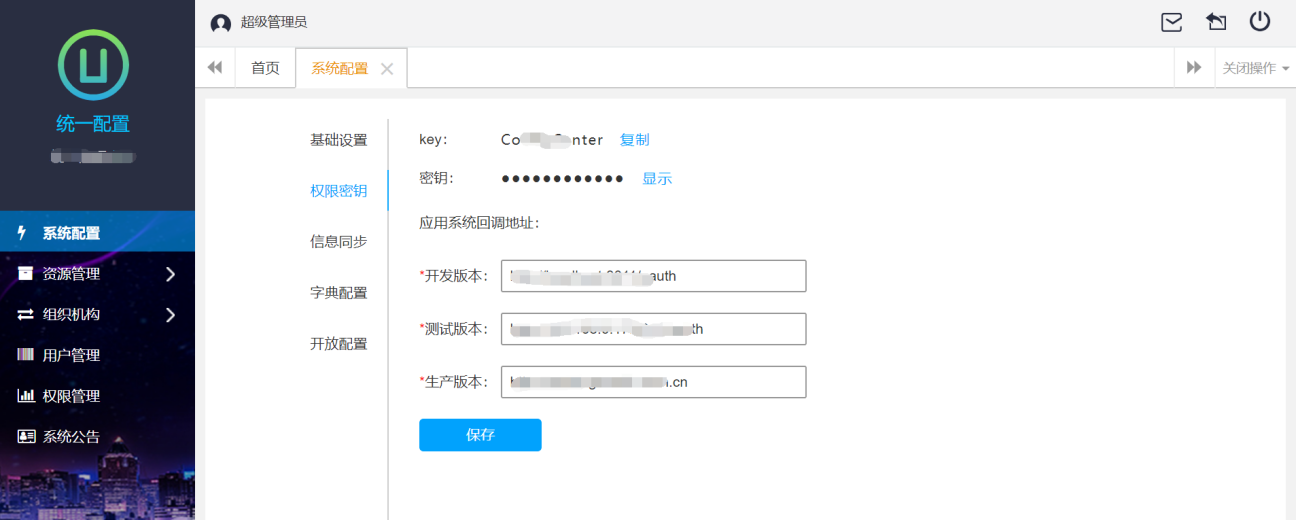


图 13系统的统一配置组件多租户界面图

第五步：应用系统嵌入用户中心页面



图 14 用户中心风格一

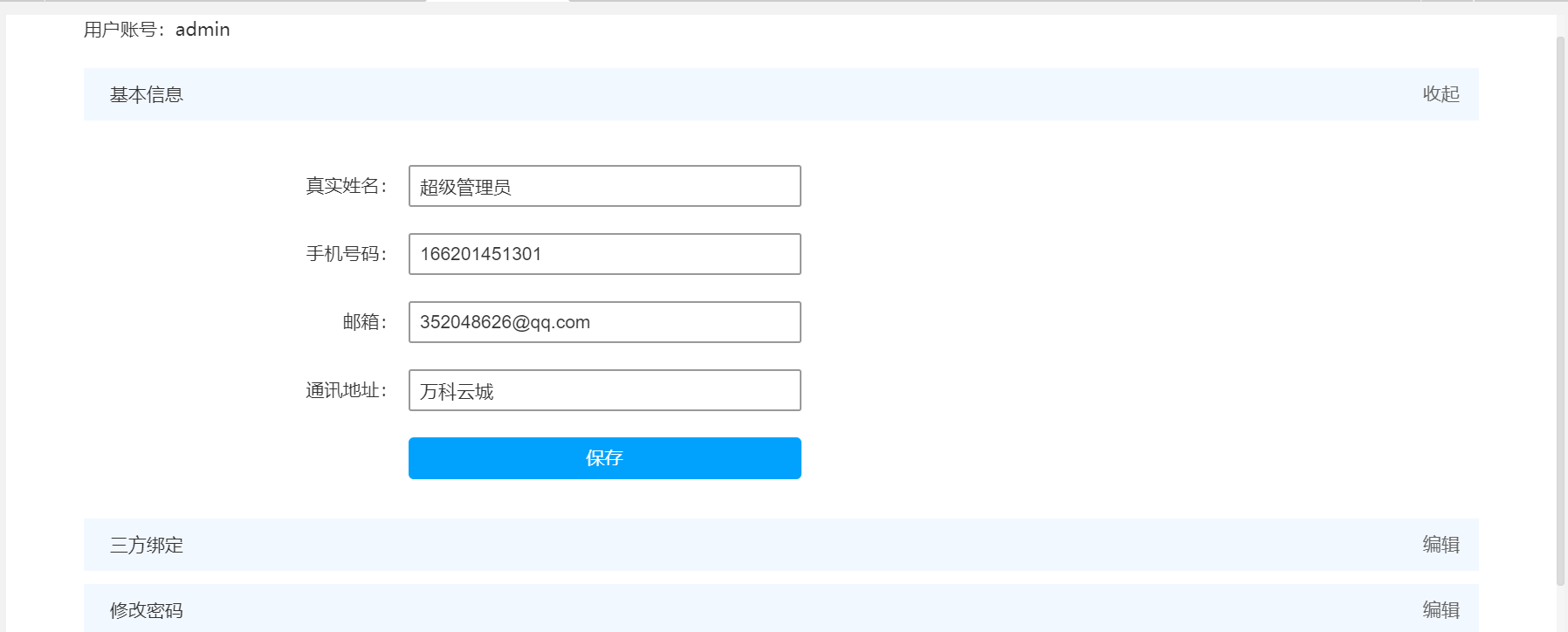


图 15用户中心风格二

### 认证服务开发接入

首先获取五个数据：统一身份认证服务器URL、系统A的KEY、系统A的密钥、系统A（在统一配置平台）配置的回调地址。

若：

系统A的KEY（clientId）：1234

系统A的密钥（clientSecret）：1a2b3c4d5e6f

系统A访问地址（callBackServer）：https://localhost:8060

统一身份认证服务器URL（oauthServer）：[https://oauth.server](http://oauth.server)

5.5.2.1单点登录接入

第一步：获取code：

oauthServer+"/oauth/authorize?client\_id="+clientId+"&response\_type=code&redirect\_uri="+redirectUrl+"&scope=all"

如果没有登录，则会跳转到统一身份认证登录页面。如果用户登录了，会从定向到redirect\_uri，授权码会作为它的参数

第二步：获取access\_token

oauthServer+"/oauth/token?code="+code+"&grant\_type=authorization\_code&client\_secret="+clientSecret+"&redirect\_uri="+redirectUri+"&client\_id="+clientId

第三步：获取用户信息，此时统一认证服务会根据该认证用户权限信息判断，决定是否返回用户信息。如果该用户不属于该应用系统，会跳转到无权限页面。否则返回用户数据以及进入系统。

获取当前登录用户基本信息：

oauthServer+"/user/simple?access\_token="+access\_token

获取当前登录用户详细信息包含配置的菜单权限数据：

oauthServer+"/user/detail?access\_token="+access\_token

5.5.2.3用户退出接入

原则上统一身份认证不提供单点退出功能，但为了保证用户体验，用户在一个系统退出登录后访问其他已登录过的系统也是退出状态。在用户退出登录时会调用统一身份认证用户退出接口，此时会清除登录用户的token信息，用户再次访问业务系统时需要业务系统校验用户在登录时所有获取的token的有效性，当token无效时，业务系统应该先清除现有登录用户的session，然后跳转到统一身份认证的登录界面。

## 统一身份认证接口

### 获取授权码

**表 4：获取授权码接口表**

|  |  |
| --- | --- |
| **接口功能** | 获得授权码 |
| **url** | https://it.gdeei.cn/oauth/oauth/authorize |
| **参数** | scope ：默认为all。 |
| client\_id ：表示系统的KEY，必选项 |
| redirect\_uri ：表示重定向URI,其值为系统在统一配置平台里面配置的回调地址。code授权码会当成redirect\_uri的参数返回。 |
| response\_type表示授权类型，必选项，此处的值固定为code |
| state:自定义字符串参数，非必填项。重定向时也会返回该参数 |
| **https请求方式** | GET |
| **说明** |  |

说明：打开连接

1》没登录。跳转到统一身份认证登录界面，输入账号密码认证通过后，会回调你传递的回调地址redirect\_uri，并将code放在其后。注意code只能用一次！

2》已登录。会回调你传递的回调地址redirect\_uri，刷新code并将code放在URL后。

如：[https://manhuaceshi.dev.cn/?code=MwvK33](http://manhuaceshi.dev.cn/?code=MwvK33)（格式redirect\_uri?code=授权码）

如：[https://manhuaceshi.dev.cn/?code=MwvK33](http://manhuaceshi.dev.cn/?code=MwvK33)&state=XXXXX（如果有state参数会原样返回）

### 以授权码模式获取access\_token

**表 5：获取access\_token接口表**

|  |  |
| --- | --- |
| 接口功能 | 通过授权码获得访问令牌access\_token |
| url | https://it.gdeei.cn/oauth/oauth/token |
| 参数 | client\_id ：表示客户端的ID，必选项 |
| client\_secret ：表示客户端的密钥，必选项 |
| code ：授权码 |
| grant\_type固定为authorization\_code |
| redirect\_uri ：认证完成并且用户对应用授权后返回的地址。 |
| 返回值 | access\_token ：访问令牌。  token\_type：获得的Token类型，Bearer  例如：  {  "access\_token":"114a00ef-47ba-432e-be67-4ff76375aaf5",  "token\_type": "bearer",  "expires\_in": 17822,  "scope": "all"  } |
| https请求方式 | POST |

### 以密码模式获取access\_token

|  |  |
| --- | --- |
| **接口功能** | 返回access\_token（以密码模式认证的） |
| **url** | https://it.gdeei.cn/oauth/oauth/token |
| **参数** | grant\_type：固定为password，必选项。 |
| scope：固定为all，必选项 |
| client\_id:系统key，必选项 |
| client\_secret:系统密钥，必选项 |
| username:账号，必选项 |
| password:账号密码，必选项 |
| **https请求方式** | POST |
| **说明** | 返回实例：  {  "access\_token":"b4d28373-3890-4302-831c-ffdf98736f06",  "token\_type": "bearer",  "expires\_in": 37512,  "scope": "all"  } |

### 校验token有效性

|  |  |
| --- | --- |
| 接口功能 | 校验token有效性接口 |
| url | https://it.gdeei.cn/oauth/oauth/check\_toke |
| 参数 | token ：token的值，必选项 |
| 返回值 | scope ：访问权限。  active：token有效性。  exp：失效时间  client\_id：客户端id  返回正常，状态码200  例如：  {  "scope": ["all"],  "active": true,  "exp": 1579006198,  "client\_id": "xxxxx"  }  返回异常，非200状态码  例如：  {  "error": "invalid\_token",  "error\_description": "Token was not recognised"  } |
| https请求方式 | GET |

### 获取当前登录用户基本信息

**表 6：获取用户基本信息表**

|  |  |
| --- | --- |
| **接口功能** | 通过访问令牌access\_token获得用户基本信息 |
| url | https://it.gdeei.cn/oauth/user/simple |
| 参数 | access\_token ：访问令牌 |
| 返回值 | 1、用户具有系统访问权限，返回数据示例：  {  "message": "操作成功",  "data": {  "user\_code": "zhouzg",#用户账号  "user\_name": "周展贵",#用户名称  #当前登录系统信息  "app": {  "code": "ConfigCenter",#系统编码  "name": "统一配置",#系统名称  "app\_type": "platform",#系统类型  "url": "https://172.20.105.204:8083",#系统地址  "icon": "2c94e94c6b45dcab016b4614fcf5000a",#系统图标ID  "version": "V1.0",#系统版本  "app\_desc": "采用云服务形可以避免同时开发这些模块。",#系统描述  "is\_admin": 1,#当前用户是否是系统的管理员  "state": 1#系统状态  },  #用户的企业信息，没有则为null  "ent": {  "id": "2c94e94c6bbac066016bc0c6d30e0030", #企业ID  "ent\_name": "周之家",#企业名称  "legal": "周代表",#企业法人代表  "capital": "999",#企业注册资金  "setup": "2019-07-04",#企业成立日期  "register": "ASDFGHJKL",#统一社会信用代码  "busi\_state": null,#企业经验状态  "ent\_type": null,#企业类型  "ein": null,#企业税号  "busi\_scope": null,#企业经营范围  "province": "广东省",#企业所在身份  "city": "广州市",#企业所在城市  "address": "小新塘",#企业地址  "contact": "周展贵",#企业联系人  "contact\_tel": "13660111727",#企业联系电话  "state": 1,#企业状态  "is\_admin": 1 #当前登录用户是否是企业管理员  },  #用户信息  "user": {  "code": "zhouzg",#用户账号  "name": "周展贵",#用户名称  "email": "13@qq.com",#用户邮件  "mobi\_tel": "",#电话  "user\_sex": null,#性别  "user\_tel": "",#手机  "user\_addr": "北京市,北京市市辖区,小新塘123",#联系地址  "idCard": null#身份证  }  },  "status": 200,  "time": "2019-09-29 03:06:09"  }  2、用户不具有系统访问权限，跳转到用户没有访问权限页面 |
| 格式 | JSON |
| https请求方式 | GET |

### 获取当前登录用户详细信息

**表 7：获取用户详细信息表**

|  |  |
| --- | --- |
| 接口功能 | 通过访问令牌access\_token获得用户详细信息，包括菜单权限数据。 |
| url | [https://it.gdeei.cn/oauth](http://172.20.105.204:8080/)/user/detail |
| 参数 | access\_token ：访问令牌 |
| 返回值 | {  "message": "操作成功",  "data": {  "user\_code": "XXX", #账号  "user\_name": "XXXX", #账号名称  "is\_admin": false, #是否是app的管理员  #app信息  "app": {  "code": "XX",  "name": "XX资源目录",  "app\_type": "project",  "url": "https://172.20.105.204:8085",  "icon": "2c94e94c6b45dcab016b49c6e33a0013",  "version": "V1.0",  "app\_desc": "资源目录",  "is\_admin": 0,  "state": 1  },  #用户信息  "user": {  "code": "XXX",  "name": "XXXX",  "email": "13@qq.com",  "mobi\_tel": "",  "user\_tel": "",  "user\_addr": "北京市,北京市市辖区,小新塘123"  },  #企业信息  "ent": {  "id": "2c94e94c6bbac066016bc0c6d30e0030",  "ent\_name": "X之家",  "legal": "周XX",  "capital": "999",  "setup": "2019-07-04",  "register": "ASDFGHJKL",  "province": "广东省",  "city": "广州市",  "address": "小新塘",  "contact": "XXX",  "contact\_tel": "13660111727",  "state": 1,  "is\_admin": 1  },  #机构信息  "org": {},  #部门信息  "dept": {  "org\_id": "2c94e94c6c09493f016c29db8b730058",  "direct\_id": "",  "pid": "root",  "area\_id": "abcde38bd6904ce9a27983834c5ddd12",  "code": "ZXLD",  "name": "中心领导",  "tel\_phone": "",  "leader": "",  "dept\_desc": "",  "state": 1  },  #默认角色信息  "role": {  "name": "角色B",  "code": "JRB",  "org\_id": "2c94e94c6c09493f016c29db8b730058",  "dept\_id": "",  "is\_admin\_role": 0,  "state": 1  },  #角色json数据  "roleJson": {  "JRA": [  {  "code": "Catalog-check",  "menu\_type": 1,  "children": [],  "name": "我的审核",  "icon": "fa fa-arrows",  "pid": "root",  "id": "ff808081683d3cc301683d68003a0001",  "url": "apply/apply"  },  {  "code": "zyml",  "menu\_type": 1,  "children": [  {  "code": "ztgl",  "menu\_type": 1,  "children": [],  "name": "主题管理",  "icon": "fa fa-area-chart",  "pid": "ff808081683d3cc301683d6843330002",  "id": "ff808081683d3cc301683d6895070003",  "url": "theme\\themeList"  },  {  "code": "zygl",  "menu\_type": 1,  "children": [],  "name": "资源管理",  "icon": "fa fa-at",  "pid": "ff808081683d3cc301683d6843330002",  "id": "ff808081683d3cc301683d6902ea0004",  "url": "info/infoManger"  }  ],  "name": "资源目录",  "icon": "fa fa-archive",  "pid": "root",  "id": "ff808081683d3cc301683d6843330002",  "url": ""  }  ],  "JRB": []  },    #用户在平台具有的全部角色信息  "roles": [  {  "name": "角色B",  "code": "JRB",  "org\_id": "2c94e94c6c09493f016c29db8b730058",  "dept\_id": "",  "is\_admin\_role": 0,  "state": 1  },  {  "name": "角色A",  "code": "JRA",  "org\_id": "2c94e94c6c09493f016c29db8b730058",  "dept\_id": "",  "is\_admin\_role": 0,  "state": 1  }  ],  "roleMenus": [  {  "code": "Catalog-check",  "menu\_type": 1,  "children": [],  "name": "我的审核",  "icon": "fa fa-arrows",  "pid": "root",  "id": "ff808081683d3cc301683d68003a0001",  "url": "apply/apply"  },  {  "code": "zyml",  "menu\_type": 1,  "children": [  {  "code": "ztgl",  "menu\_type": 1,  "children": [],  "name": "主题管理",  "icon": "fa fa-area-chart",  "pid": "ff808081683d3cc301683d6843330002",  "id": "ff808081683d3cc301683d6895070003",  "url": "theme\\themeList"  },  {  "code": "zygl",  "menu\_type": 1,  "children": [],  "name": "资源管理",  "icon": "fa fa-at",  "pid": "ff808081683d3cc301683d6843330002",  "id": "ff808081683d3cc301683d6902ea0004",  "url": "info/infoManger"  }  ],  "name": "资源目录",  "icon": "fa fa-archive",  "pid": "root",  "id": "ff808081683d3cc301683d6843330002",  "url": ""  }  ]  },  "status": 200,  "time": "2019-09-29 05:01:20"  } |
| **格式** | JSON |
| **https请求方式** | GET |

### 用户退出

|  |  |
| --- | --- |
| 接口功能 | 用户退出。**只能通过页面请求重定向才能有效** |
| url | https://it.gdeei.cn/oauth/oauth/logout |
| 参数 | callback ：登出后需要跳转的地址 |
| 返回值 | 无 |
| **格式** | 无 |
| **https请求方式** |  |

## 默认权限集成

业务系统在业务系统侧实现一个默认角色，并给该角色配置好可访问的页面，这样用户账号一旦被创建后无需授权也有权限访问该业务系统。

默认角色配置操作如下：

（1）检查统一配置中心中该应用的基础配置中，访问授权的选项是否为“自动”。只有选中“自动”，智慧云平台才能默认支持所有用户访问该业务系统。



图 13系统用户访问权限策略配置图

1. 业务系统开发商在业务系统侧配置或调整程序实现默认角色访问功能。

当用户详细信息接口返回一个默认角色（default）时，default不区分大小写，业务系统需要定义与实现该角色的功能。