**海尔集团统一身份认证中心**

**单点登录集成标准**

|  |  |  |  |
| --- | --- | --- | --- |
| 文件编号 | 单点登录集成标准 | | |
| 文件状态 | []草稿 [√] 正式发布 []正在修改 | | |
| 当前版本 | V1.0 | | |
| 拟 制 |  | 日期 |  |
| 审 核 |  | 日期 |  |
| 批 准 |  | 日期 |  |
| 发布日期 |  | | |
| 生效日期 |  | | |

海尔集团

**目 录**

[1 单点登录认证服务接口 3](#_Toc15743924)

[1.1 描述 3](#_Toc15743925)

[1.2 OAuth认证服务接口 3](#_Toc15743926)

[1.2.1 认证流程 3](#_Toc15743927)

[1.2.2 认证接口 4](#_Toc15743928)

[1.2.3 应用集成demo 8](#_Toc15743929)

[1.3 接口调用注意事项 8](#_Toc15743930)

[1.3.1 urlEncode编码 8](#_Toc15743931)

[1.3.2 HTTPS安全协议 8](#_Toc15743932)

# 单点登录认证服务接口

## 描述

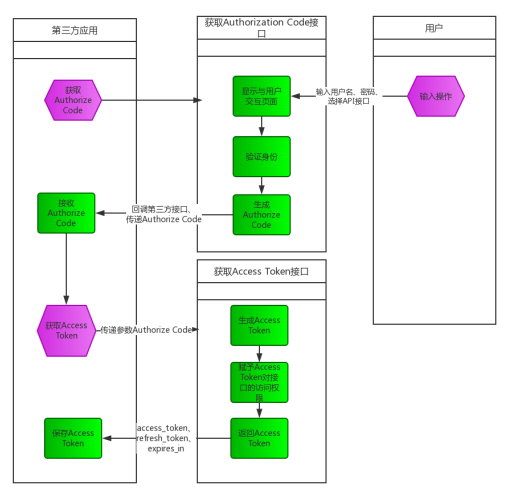
本文档的阅读对象为需要与IDM通过Oauth接口方式集成单点登录的应用开发人员。

## OAuth认证服务接口

### 认证流程

要求：需要用户介入，用户输入用户名与密码

流程图：



### 认证接口

#### 认证接口

接口说明：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 接口名 | authorize | | | | |
| URL Path | https://认证中心域名/idp/oauth2/authorize | | | | |
| 请求类型 | GET | | | | |
| 请求示例 | https://认证中心域名/idp/oauth2/authorize?client\_id=20170829065450049-938C-587B3F8FB&redirect\_uri=http://www.baidu.com&response\_type=code&state=123 | | | | |
| 请求参数 | 参数名 | 中文说明 | | 描述 | |
| client\_id | 应用标识 | | 客户端应用注册ID  测试环境统一用：oauthTest | |
| redirect\_uri | 跳转地址 | | 应用系统地址：处理认证中心返回的授权code值 | |
| response\_type | 响应类型 | | 固定值：code | |
| state | 任意值 | | 用于保持请求和回调的状态，在回调时，会在Query Parameter中回传该参数。开发者可以用这个参数验证请求有效性，也可以记录用户请求授权页当前的位置。这个参数可用于防止跨站请求伪造（CSRF）攻击 | |
| 处理逻辑 | 判断参数  验证client\_id是否有效  认证链校验用户名密码  根据以上判断、验证及认证结果返回JSON数据 | | | | |
| 返回值 | 类型：String，即：以JSON格式返回角色数据集  参数不完整及错误时：  client\_id缺失时  {  "errcode": "1001",  "msg": "缺少参数client\_id"  }  redirect\_uri缺失时：  {  "errcode": "1016",  "msg": "缺少参数redirect\_url"  }  client\_secret缺失时：  {  "errcode": "1008",  "msg": "缺少参数client\_secret"  }  client\_id无效时：  {  "errcode": "1005",  "msg": "参数client\_id非法"  }  正确返回时：  {  "code": "ese3edf4d5f4d24g55634dfe",  } | | | | |
| 返回参数 | 参数名 | | 中文说明 | | 描述 |
| errcode | | 错误代码 | |  |
| msg | | 提示信息 | |  |
| code | | 认证成功返回的code | |  |
| 描述 | 获取授权码的rest接口 | | | | |

#### 获取授权接口(authorization\_code模式)

接口说明：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 接口名 | getToken | | | |
| URL Path | https://认证中心域名/idp/oauth2/getToken | | | |
| 请求类型 | POST | | | |
| 支持格式 | JSON | | | |
| 请求参数示例 | "client\_id":"78a6d9e35ec647c185ea2bcb7a77e8f2",  "client\_secret":"efdb83bb33cc4ba08dd28f591ffaa476",  "code":"5ec647c183c8f591c4ba08dd ",  "grant\_type":"authorization\_code" | | | |
| 参数 | 参数名 | 中文说明 | 描述 | |
| client\_id | 应用标识 | 客户端应用注册ID  测试环境固定值：oauthTest | |
| client\_secret | 密钥 | 客户端应用注册密钥  测试环境固定值：  09bb3743b7474ba2ada887e65899cf2a | |
| code | 授权码 | 调用认证接口（authorize）获得code | |
| grant\_type | 认证方式 | 请求类型，默认authorization\_code | |
| 处理逻辑 | 判断参数  验证参数有效性  根据以上判断、验证及认证结果返回JSON数据 | | | |
| 返回值 | 类型：String，即：以JSON格式返回角色数据集  参数不完整及错误时：  client\_id缺失时  {  "errcode": "1001",  "msg": "缺少参数client\_id"  }  code缺失时：  {  "errcode": "1009",  "msg": "缺少参数code"  }  grant\_type缺失时：  {  "errcode": "1010",  "msg": "缺少参数grant\_type  }  client\_secret缺失时：  {  "errcode": "1008",  "msg": "缺少参数client\_secret"  }  client\_id无效时：  {  "errcode": "1005",  "msg": "参数client\_id非法"  }  code无效时：  {  "errcode": "1014  "msg": "参数code非法  }  正确返回时：  {  "access\_token":"skiew234i3i4o6uy77b4k3b3v2j1vv53j"  "expires\_in":"1500",  "refresh\_token":"iewoer233422i34o2i34uio55iojhg6g"  "uid":"admin"  } | | | |
| 返回参数 | 参数名 | 中文说明 | | 描述 |
| errcode | 错误代码 | |  |
| msg | 提示信息 | |  |
| access\_token | 获取的授权码token值 | |  |
| refresh\_token | 刷新授权码token | | 根据刷新token可以生成新的token |
| uid | 用户ID | | 唯一标识 |
| expires\_in | 授权码有效时间（秒） | |  |
| 描述 | 根据认证code获取应用的access\_token | | | |

#### 获取用户信息接口

接口说明：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 接口名 | getUserInfo | | | | |
| URL Path | https://认证中心域名/idp/oauth2/getUserInfo | | | | |
| 请求类型 | GET | | | | |
| 请求示例 | https://认证中心域名/idp/oauth2/getUserInfo?access\_token=uhd2k3k5j3&client\_id=sei62jhb21b1l56n | | | | |
| 参数 | 参数名 | 中文说明 | | 描述 | |
| access\_token |  | | token授权码 | |
| client\_id | 应用标识 | | 客户端应用注册ID | |
| 处理逻辑 | 判断参数  验证参数有效性  根据以上判断、验证及认证结果返回JSON数据 | | | | |
| 返回值 | 类型：String，即：以JSON格式返回角色数据集  参数不完整及错误时：  client\_id缺失时  {  "errcode": "1001",  "msg": "缺少参数client\_id"  }  access\_token缺失时：  {  "errcode": "2001"  "msg": "缺少参数access\_token "  }  uid缺失时：  {  "errcode": "2006"  "msg": "缺少参数uid "  }  client\_id无效时：  {  "errcode": "1005",  "msg": "参数client\_id非法"  }  access \_token无效时  {  "errcode": "2002"  "msg": "参数access \_token不正确或过期"  }  uid无效时  {  "errcode": "3001 "  "msg": "查询用户信息为空"  }  正确返回时：  {  用户信息  } | | | | |
| 返回参数 | 参数名 | | 中文说明 | | 描述 |
| errcode | | 错误代码 | |  |
| msg | | 提示信息 | |  |
| 用户信息 | | 用户信息为json格式 | |  |
| 描述 | 获取用户信息 | | | | |

### 应用集成demo



## 接口调用注意事项

### urlEncode编码

由于HTTP URL自身限制，无论REST接口还是认证辅助接口，传入的参数值如果包含例如”%”、”&”、” ”、”=”等特殊字符或中文时，需要先作urlEncode编码。推荐所有参数值先都作urlEncode编码再调用接口传入。

### HTTPS安全协议

REST接口以及认证辅助接口说明：

以上例子默认都采用HTTP协议，为增加安全性，实际部署时支持HTTPS协议。当采用HTTPS协议时，需要在应用服务器上信任DNS、IDP的服务器证书。