# 子系统接入统一登录步骤

（v 1.2）

# 阅读对象

子系统相关开发人员、运维、技术支持等。

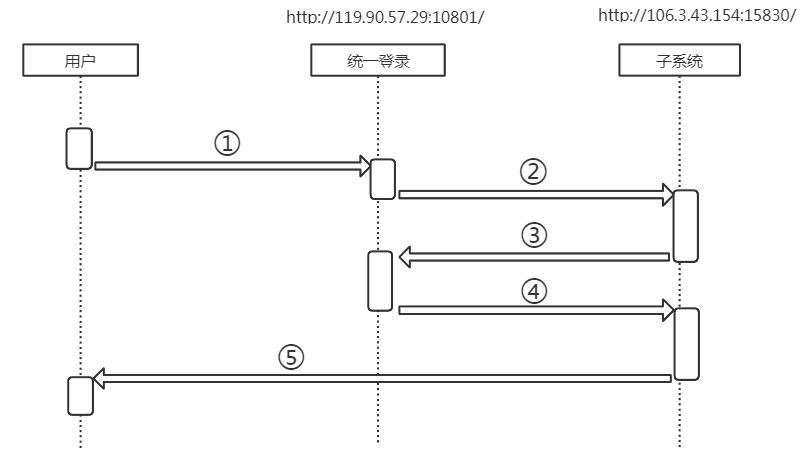
## 1.1相关术语

|  |  |
| --- | --- |
| 术语 | 解释 |
| 站点 | 即子系统，银农直连、三资、产改等。 |
| appkey | 为对应子站点的唯一标识码 |
| appsecret | 为对应子站点的唯一标识码 |

# 总体介绍

## 跳转流程

**统一登录与子系统的跳转流程如下：**



如上图举例：

统一登录地址为 http://119.90.57.29:10801

子系统访问地址为 http://106.3.43.154:15830

**具体文字对应说明如下：**

1. 当用户访问统一登录http://119.90.57.29:10801后，会看到具体的子系统模块，在授权基础上可以访问子系统。
2. 当点击子系统模块后，统一登录后台会生成一个具有时效性的令牌A，并将该令牌和要求子系统返回地址B，拼接到当前站点提供的拦截页面地址里，如<http://106.3.43.154:15830/index.html?code=A&exiturl=B>这样。
3. 子系统前端页面对于index.html访问过程中获取到code和exiturl的情况下，会调用自己系统中的验证令牌接口，在该接口的后台逻辑中，需要向统一登录系统，发起http请求验证令牌A的真伪（**能内网访问优先使用内网地址**）。该接口URI地址固定为(/api/sso/token)，如<http://119.90.57.29:10801/api/sso/token>。需要子系统维护在自己的配置文件中。其中还需子系统维护的有appkey、appsecret，这三个参数都是提前由统一登录提供，已对接过的系统appkey、appsecret值不变。
4. 当通过上一步验证后，统一登录正常情况下会返回用户信息，子系统需要将以下信息同步到数据库中，如果用户存在需要重新更新，以免统一登录用户修改过用户信息，造成与子系统不一致的情况。：

|  |  |
| --- | --- |
| 字段名 | 字段介绍 |
| ssousername | 统一登录用户名 |
| username | 用户名 |
| roleid | 角色id |
| xzqh | 行政区划代码 |
| nickname | 昵称 |
| tel | 电话号码 |
| isBindUser | 是否绑定用户 |

1. 当验证成功后，子系统相当于完成了用户登录密码校验的逻辑，可以进行下一步的身份存储工作，并返回给用户登录成功后的页面。

# 接入步骤

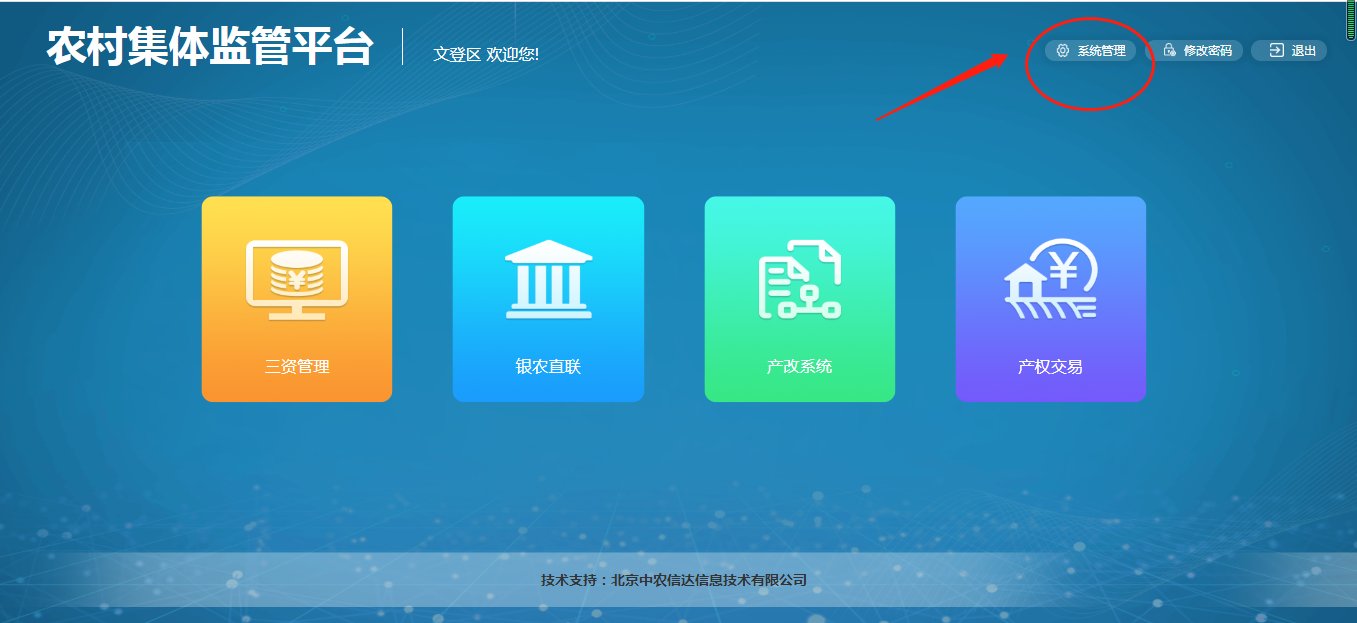
统一登录部署后，一般会提供出两个账户。

**超级管理员：**拥有操作站点中心的权限（新建站点、配置站点，以及首页显示站点等）。此管理员默认为znxd znxd2018，注意超级管理员不能给用户。

**普通管理员：**一般以地区命名，如果部署的为文登区统一登录，基本提供的账号为wendeng a123456！

以上两个账号如果没有提供，可以联系相关的部署人员，目前统一登录的部署及后期维护，暂时由银农直连项目负责，有问题的话，北京找凌树峰、威海找于新义。

## 新增站点

用超级管理员登录统一登录系统后，可选择下图位置【系统管理】

进入【系统配置】--【站点中心】--【站点管理】，会看到有如下列表：



【站点管理】里需要修改下站点对应的地址和图标，如下图：



上图中，appkey和appsecret，需要与子系统中对应，一般情况下，已对接的基本不变，除非是部署了多个相同系统，才会需要修改。

1. **跳转地址：**

为统一登录点击子模块跳转到子系统时，需要调用子系统拦截统一登录token的初始化页面，如上图，三资系统要求的路径为/sso/index.html页面。

对应传参主要有两个：(%s为占位符，这里配置好后，统一登录会自动将%s替换为真正的值)

**code=%s**：为统一登录跳转子系统前生成的唯一令牌，用作子系统回调验证身份时用的参数。其中%s会在统一登录跳转前，由后台替换为真正的令牌。

**exiturl=%s**:对于新版统一登录，考虑到子系统点击自己系统退出按钮时，应该退回到对应的统一登录系统，因此需要一个回退回统一登录的地址，该地址由统一登录提供，因此新版统一登录额外扩充了这个exiturl参数，该参数为非必填。即假如三资系统需要，则可以如下填写：

[http://ip:port/index.html?code=%s&exiturl=%s](http://ip:port/index.html?code=%25s&exiturl=%25s)

如果赋值为%s，表示可替换参数，对于exiturl则会取当前统一登录的ip和port地址。

**当为域名部署时，此处如果需要exiturl，必须要写为具体的统一登录域名对应地址。因为前端获取的只能是ip端口或者域名，至于下一级的路径拿不到。**

**对于有的系统需要from值的，也可以在路径中直接拼接即可。**

**2）退出地址：**

**子系统**的退出地址，用做统一登录点击退出时，退出授权下的子系统。此地址必须由子系统放开登录限制，并且为get请求。

北京系统统一都是：<http://ip:port/api/user/logout>

如果出现子系统与统一登录不在同一域下，退出子系统会出现失败情况。

**3）获取角色方式：**

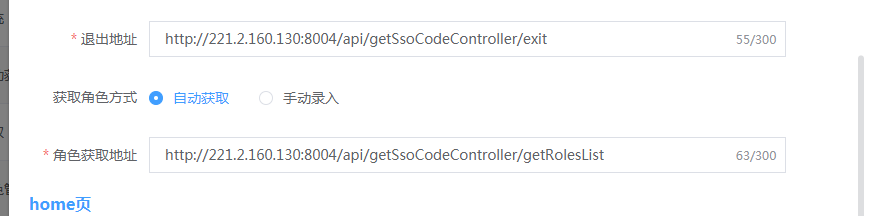
除了银农直连，其他系统都选手动获取，并且到站点角色中录入对应的角色名、角色值。其中角色值为子系统中的对应数据库中的角色id。

获取的角色为当前子系统的角色id、角色名称，因为统一登录跳转子系统时，需要提前知道对应的角色值，因此需要统一登录这边能够查询到。

有自动获取和手动录入两种方式。按照实际情况选择即可。

**自动获取**：由子系统按照统一登录约定的获取接口规范（见最后附内容），提供的角色获取接口。当【站点管理】里对应站点设置为自动获取时才有效。目前仅有银农直联真正启用了自动获取角色的方式。其他系统暂不支持。

自动获取接口如果对接了，子系统新增完角色后，统一登录这边不需要再次录入即可看到。如下图，为三资系统提供的角色获取接口。注意该接口必须要提前放开。需要统一登录约定的子系统角色获取接口文档的，联系对应开发人员。



**手动录入**：当选择该模式下，是为了兼容旧版统一登录，有的子系统角色少或没有可提供自动获取角色接口的条件，则需要在保存当前站点后，子系统也建完对应角色后，需要到统一登录【站点中心】--【站点角色】中手动对相应站点录入角色id、角色名。

当配置完上边的内容后，还需要配置一下图标，如下图，滚动到最下方：



修改显示名称和图标。显示名称为在统一登录首页显示的子系统名字。

Logo为首页显示子系统的图标（见最后附内容，挑选合适的模块图）。

站点建好之后，保存即可。

## 配置站点角色

站点角色仅在站点管理对那些站点角色获取方式配置为手动录入时，这里才生效。如果获取方式为自动获取，站点角色则没必要录入角色了。目前除银农直连以外系统，都需要进行配置。

另外，站点角色必须要在站点管理之后操作。

如果下图站点角色中没有站点，则表示【站点中心】--【站点管理】中没有建立当前地区下的站点。



## 配置登录页首页

统一登录的登录页、首页看到的图片文字，都为可配置项，它们都在统一登录系统配置里的【站点管理】--【登录页首页配置】里。如下图所示：





上图中，左边为登录页配置，右边为首页配置。首页多出一个开启子系统的多选框。这里对应的是需要在首页展示的子模块，勾选自己新增的站点子系统，点击保存即可。如下图回到首页即可看到：



此时虽然显示出自己的账号，但是还不能进行登录，因为没有对相应的用户进行授权。

## 用户创建

进入到【系统管理】--【用户管理】，如下图：



当含有统一登录时，子系统的用户管理编辑功能（新增、修改、删除）应该予以关闭。用户应统一在统一登录维护创建。

提示：统一登录创建完的用户，在子系统登录页面中是无法登录的。

点击新【新建】，如下图：



当选择到上图的角色时，有如下几种角色：

超级管理员、普通角色、访问角色三种。

**超级管理员**：拥有一切统一登录权限，一般是给技术支持或开发人员使用。不能授权给用户。

**普通角色**：给客户的管理员提供，拥有系统管理后台模块的部分功能，用户新增、修改、删除等。

**访问角色**：仅用于统一登录跳转，不包含统一登录后台模块。

## 用户授权

用户新建完之后，需要对其进行授权才能拥有跳转子系统的权限。找到【系统管理】--【用户管理】，点击【授权】按钮，如下图：



当需要授权某个站点时，则点击右侧未授权项目：



在对相应站点授权时，可以查看到对应的捆绑角色。

**提示：如果此处捆绑角色没有数据，无非两个原因：**

**角色是否为自动获取？**

则首先要确定的是当前站点获取角色方式是否为自动获取，可通过【站点中心】--【站点管理】中找到相应站点，查看角色获取方式，如果为自动，那这里获取不到角色信息，则需要从接口上排查，可能是子系统未创建角色，也或者角色接口有问题；

**站点角色中是否已经录入？**

当为手动录入时，那肯定就是【站点中心】--【站点角色】，对应的子系统角色未录入。只要录入进去，这边就可以看到了。

另外注意捆绑用户名的功能。

捆绑用户名针对的是一种情况，比如客户最开始只有一个三资系统，并且已经使用了一段时间，里边有了一些用户及数据，现在客户又想买我们的另一个系统，比如银农直联，这种情况下，就需要统一登录系统来将两个系统的用户打通。但是又不能丢掉客户以前走过的数据及用户，这种情况下就需要捆绑用户名。

比如以前三资系统里有个zhangsan用户，现在要想他能够在统一系统登录，又不丢掉以前的数据，就需要首先在统一登录中创建zhangsan 用户，然后授权三资系统时，在捆绑用户名处填写为zhangsan，并授权实际zhangsan对应的角色，才能做到。

# 4子系统开发

## 4.1 前端开发

子系统前端需要用一个页面进行url截取code、exiturl参数的操作。对应3.1中的跳转地址，比如银农的访问地址为<http://106.3.43.154:15830>，银农直连提供的这个页面为<http://106.3.43.154:15830/index.html>。

将来统一登录跳转银农的时候，实际路径大概是下图这样：

<http://106.3.43.154:15830/index.html?code=34342errer&exiturl=http://106.3.43.154:8081>

其中exiturl为统一登录的地址。

子系统在index.html页面初始化的时候，需要先从路径上拦截，是否携带code、exiturl值，如果携带，则需要将exiturl存入到前端缓存中，另外将code当做参数，传给自己系统的后台，调用后台的接口参照（见5.3）。

## 4.2 后端开发

### 4.2.1 开发内容

子系统需要添加一个接口，该接口最终的目的，需要根据自己系统账号密码登录接口，来模拟一个类似功能的接口，无非自己登录用的是账号密码，这个接口用的是统一登录给的code值。

另外，还需要在自己系统里配置appkey、appsecret值，可以配置到配置文件中。对应2.1中的appkey、appsecret值，如果不对应，则跳转失败。

在开发的这个接口里，需要接收前端传入的code值，该code值为前端从统一登录跳转过来后，在url里截取获取的，将这个code值传给这个接口后，子系统需要将code,以及appkey、appsecret值，三个参数进行封装，首先回调统一登录的一个身份验证接口获取用户信息，如果获取成功，则再参照自己系统的登陆接口中，账号密码验证成功后的逻辑即可。

参照接口请参考 5.3。

### 4.2.2 注意事项

#### 4.2.2.1 回调地址

回调地址为子系统将从统一登录接收到的code回传统一登录验证身份时的校验接口地址，**此地址最好写内网地址**。（参考5.4 回调接口地址）

如果子系统与统一登录部署在一个机器上，如果在统一登录部署完之后，提供出来时，没有特殊说明，一般为<http://localhost:10019/api/sso/token>。

#### 4.2.2.2 appkey、appsecret值

此两个值为子系统的身份，来源参照3.1描述，需要与3.1中建的对应站点里的值匹配。

#### 4.2.2.3 跳转失败

跳转失败的原因，绝大部分都是因为回调地址、appkey、appsecret值填写不正确导致。

# 5 附内容

## 5.1子站点提供给统一登录获取角色列表的接口

如果需要子系统录入完角色，统一登录系统在授权时，能自动查到，则需要子系统按照以下要求提供一个外放接口，供统一登录调用。

**接口要求：**

（1）POST请求。

（2）数据交互都是json格式。

（3）传入参数和返回格式必须按照下边的接口要求提供，不能抛出异常，接口名不限制。

|  |  |
| --- | --- |
| 服务地址或方法 | sso/getRolesList（接口名无需固定） |
| 参数说明 | 行政区划代码，分页条件 |
| 调用方法 | POST |
| 方法概述 | 子站点需要提供的角色列表获取接口 |
| 输入格式 | 需要有三个参数，  {  "pageNo":1,  "pageSize":10,  "xzqhdm":"370702" /**/统一登录对于省市县都为6位，以0补全**  } |
| 返回格式 | 成功时返回：  {  "totalcount":"",  "msg":"查询成功",  "data":[  {  "id":"", //角色id(用户组id)  "rolename":"县级管理员"  }  ],  "success":true  }  失败时返回：（失败时只需要返回success,msg即可）  {  "msg":"", //错误信息  "data":[],  "success":false  } |
| 备注 |  |

## 5.2跳转子系统失败原因

### 5.2.1 无权限访问

统一登录用户登录后，如果点击某个子系统时，显示无权限访问，则表示该用户没有授权当前系统的角色，这种情况，需要用管理员登录统一登录系统，找到【系统管理】--【用户管理】，找到该用户，然后对其授权子系统的一个**有效**角色即可。

### 5.2.2 统一登录不显示子系统模块

如果统一登录用户登录后，没有显示子系统的模块，则表示统一登录没有添加该子系统。

需要用统一登录超级管理员登录，找到【站点中心】--【站点管理】，先确认是否已录入子系统记录，如果没有录入，则按照3.1操作录入，如果已录入，确认是否开启。

然后，再到【站点中心】--【登录页首页配置】，对首页布局中，找到开启子系统位置，勾选子系统，保存即可。



### 5.2.3 统一登录跳转子系统失败

统一登录跳转失败原因如下：

1. 配置的子系统跳转地址是否正确，是否缺少参数，比如有的系统需要from参数。
2. 子系统配置的appkey、appsecret是否与统一登录配置的当前子系统的一致（参照3.1 配置站点管理）。
3. 子系统配置的统一登录回调地址是否正确。

## 5.3子系统开发接口

参照下面代码的 OauthAccessToken/oauth接口。



右击上图图标---选择“包装程序外壳对象”—激活对象，下载这个java类即可。

## 5.4子系统回调统一登录接口

此接口为子系统验证身份的接口，对接前，需要联系统一登录开发人员，沟通可用服务地址，接口结构如下图所示：

|  |  |
| --- | --- |
| 服务地址或方法 | /sso/token |
| 参数说明 |  |
| 方法概述 | 子站点需要提供的角色列表获取接口 |
| 输入格式 | 需要有三个参数，  appkey 子系统身份key (需要与统一登录系统提前约定)  appsecret 子系统身份secret (需要与统一登录系统提前约定)  code 统一登录传过来的身份code |
| 请求方式 | http协议，POST请求，传参不是json格式 |
| 返回格式 | 成功时返回：  {  "access\_token":"",  "expires\_in":"查询成功",  "values":  {  "ssousername":"znxd\_1923718293433", //统一登录用户名  "nickname":"中农信达", //真实名称  "roleid":"3", //角色id //对应当前子系统角色值  "isBindUser":"true", //是否绑定用户名  "username":"", // 真实用户名  "xzqh":"", //用户所属行政区划代码  "tel":"", //电话号码  "ssotoken":"" //统一登录token  }  }  失败时返回：（失败时只需要返回success,msg即可）  {  "error":"", //错误信息  "error\_description":""  } |
| 备注 | 以上注意isBindUser，如果为true，表示子系统用户与统一登录用户需要绑定用户名，如果为true，则username为绑定的用户名值  ssousername为防备统一登录与子系统有用户名冲突的问题，返回的是加了时间戳的用户  具体调用示例，参考4.3介绍。 |

## 5.5子模块图

用于统一登录首页，对应子系统展示的图片

