**IUAP平台使用指南**

**功能权限组件**

用友网络科技股份有限公司

二○一八年五月

**此文档为保密文档，未经用友软件股份有限公司书面同意，不得向任何单位或个人提供、转让本文档中的任何内容，用友软件股份有限公司将保留对泄漏文档内容的起诉权利。**

**IUAP平台使用指南**

|  |  |  |
| --- | --- | --- |
| 文件状态：  [ ] 草稿  [**√**]正在修改  [] 正式发布 | 文件标识： |  |
| 当前版本： |  |
| 作者： |  |
| 完成日期： |  |

版本历史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 作者 | 参与者 | 起止日期 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

审核记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 姓名 | 职位 | 审阅日期 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目 录

[第一章概述 1](#_Toc515717715)

[1.1业务场景 1](#_Toc515717716)

[1.2开发方案 1](#_Toc515717717)

[第二章环境准备 2](#_Toc515717718)

[2.1开发环境配置 2](#_Toc515717719)

[2.1.1设置编译路径 2](#_Toc515717720)

[2.2数据库脚本配置 2](#_Toc515717721)

[2.2.1业务表 2](#_Toc515717722)

[2.3应用中心配置 2](#_Toc515717723)

[2.3.1启动按钮权限控制 2](#_Toc515717724)

[2.3.2配置需要控制权限的按钮 3](#_Toc515717725)

[2.3.3按钮授权 4](#_Toc515717726)

[2.4效果展示 4](#_Toc515717727)

[第三章代码开发示例 6](#_Toc515717728)

[3.1前台配置 6](#_Toc515717729)

[3.1.1 html页面配置 6](#_Toc515717730)

[3.1.2 js代码配置 6](#_Toc515717731)

# 概述

## 业务场景

用户在登陆系统时，需要做身份认证以保证安全，此为系统的认证功能。同时，登陆到业务系统后，需要根据用户的身份，确认用户可以访问的系统功能点——功能权限。

## 开发方案

在运行平台中，登录认证功能已经完备。在我们的项目中，对于项目的页面拦截，只需要保证访问服务时，如果尚未有登录信息，则页面需要跳转到运行平台的登录页面。应用开发平台已经提供了一套机制，可以结合应用开发平台的统一登录，并且各个应用通过使用登录认证组件，结合下文中的相关配置，将应用开发平台和各个应用部署到同一个域名下就能够解决，实现各自应用的身份认证问题；

# 环境准备

## 开发环境配置

## 功能权限模型

**rbac权限模型**

rbac是指以角色为核心的权限体系。关于用户、角色和功能的关系描述如下图所示



用户：登录到系统的用户，往往真实的对应到一个人员，一个人员可以有多个用户。

角色：往往指的是一种职能或者职责的集合。

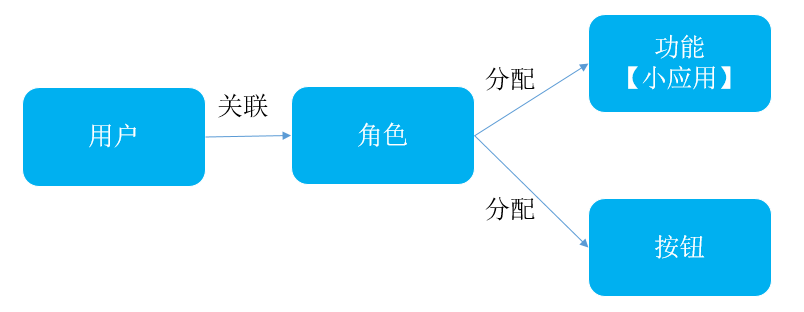
功能：功能点

我们的功能权限要求：

* 在用户登录时，不同的用户需要看到不同的功能点。也就是只能看到自己有权限的功能点。

所以我们需要增加用户、角色、功能、菜单等节点。增加他们的对应关系

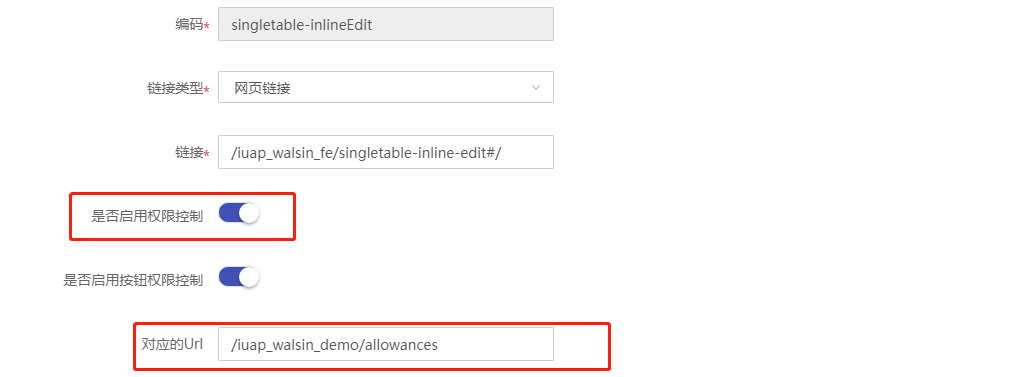
在的demo中，业务上要求增加用户、角色、功能节点，通过可视化界面建立好关系后，提供根据用户查询对应功能以及按钮的API，提供给登录认证功能使用。



## 应用中心配置

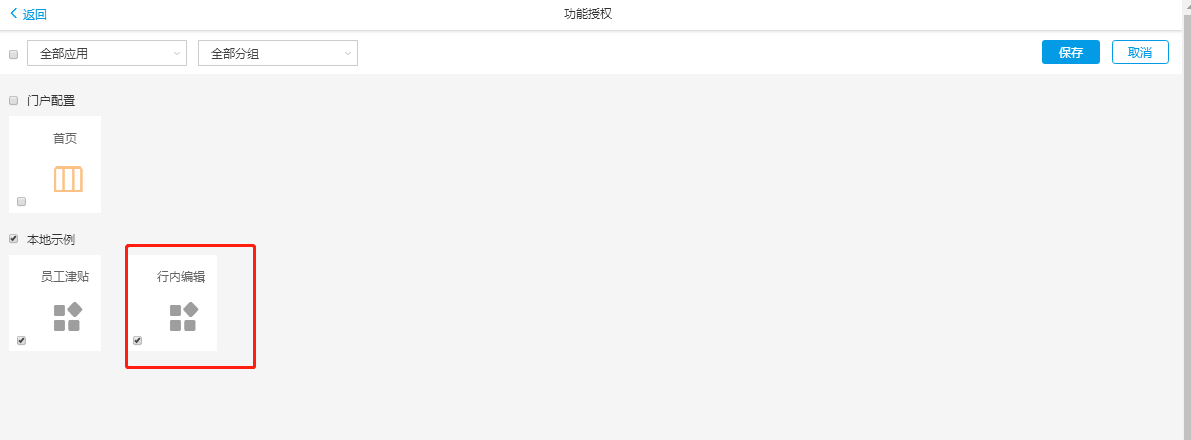
### 启动功能权限控制

1.在管理中心-功能管理下，新建或者编辑已有的的功能，将“是否启用权限控制”，并在对应的URL中输入url的值；这个地方的url的格式为“/项目名/对应的Controller的RequestMapping“，如本例中的” /iuap\_walsin\_demo/allowances”，如下图所示：



2. 在管理中心-功能授权下，将功能授权给角色，点击“功能授权”按钮勾选需要授权的功能，点击保存即可，如下图：





## 效果展示



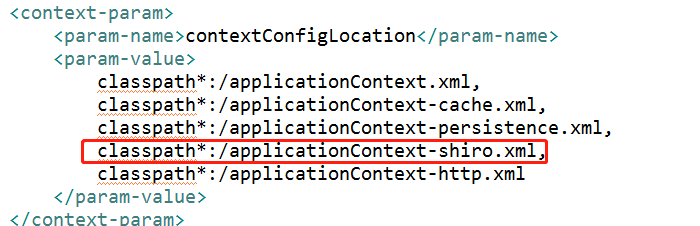
注意：功能权限位置处的对应url必须配置;

# 代码开发示例

## 后台代码

### web.xml

加载shiro配置文件



配置Shiro拦截

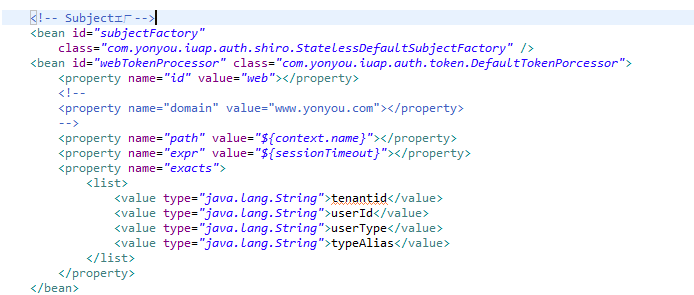
权限拦截器用于实现请求控制，即对url非法请求后台服务进行拦截，该拦截器需要配置在src/main/webapp/WEB-INF/web.xml中的shiroFilter的后面即iuap-auth认证组件的之后，只有请求经过登陆认证组件验证过的请求，才需要进行权限拦截；在拦截器中需要验证当前用户是否具有当前请求即操作功能节点的权限，并且对于该功能的按钮操作是否有权限的验证；

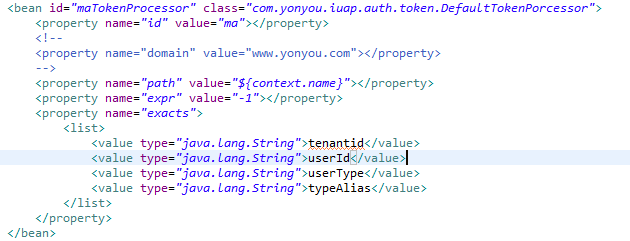


### Shiro配置文件

applicationContext-shiro.xml

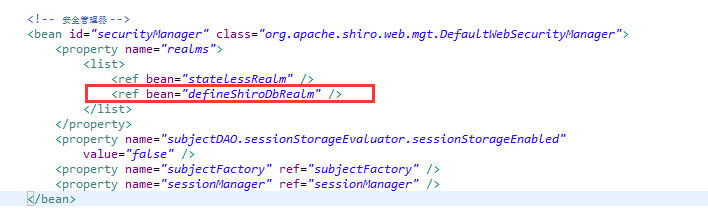
需要把tenantid/userId/userType/typeAlias属性放入



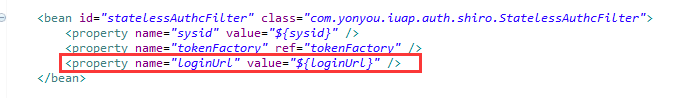


增加权限验证的Realm

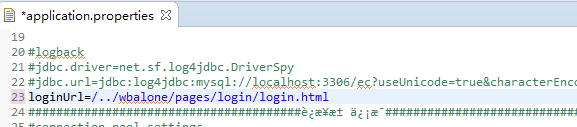




增加跳转的登录路径



loginUrl为跳转的登录页面，配置在src/main/application.properties文件中

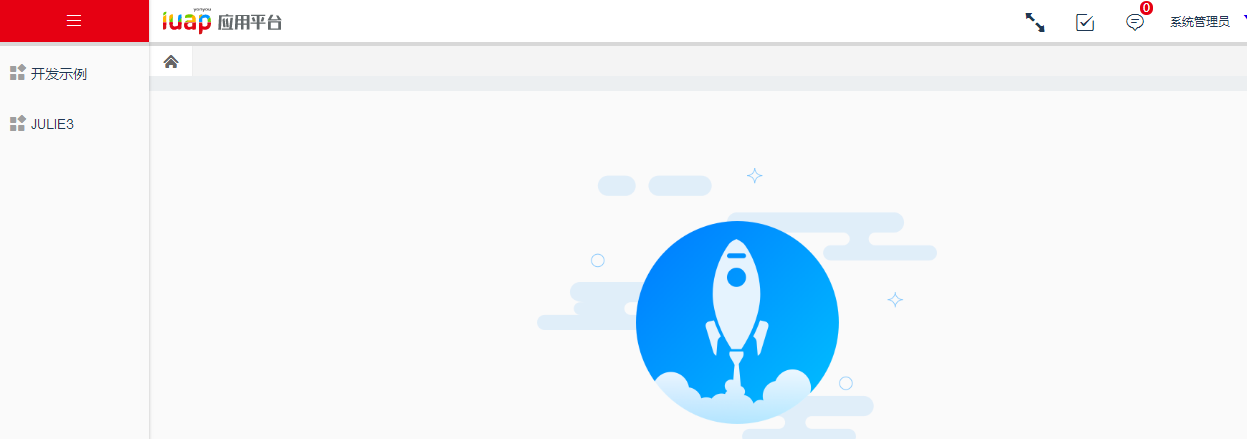


loginUrl配置为应用平台的登录页面

loginUrl=/../wbalone/pages/login/login.html

### 运行效果

如果访问<http://127.0.0.1:8080/appdemo>，并且未登录，则会自动跳转到我们配置的登陆页面



如果访问

<http://172.20.52.215:8888/iuap_walsin_demo/allowances/list?pageIndex=0&pageSize=25>，功能权限没有分配，则会提示没有权限

