Perkinelmer’s SSO 使用手册

# 一：原理介绍

单点登录平台，分为两个部分，一个是认证中心服务端，一个是chrome插件客户端。认证中心主要负责：处理认证逻辑，提供关键信息；客户端主要负责，收集用户需求，引导认证通过，并实现用户应用的自动登录

流程简单介绍：首次点击chrome客户端插件，会出现登录按钮，用户点击登录，就会跳转到认证中心的登录页面，登录成功后，进入认证中心的管理页面；之后再点击客户端插件，就会出现为此用户分配的应用组，点击其中一个应用，客户端自动跳转到此应用的登录页面，同时自动输入为此应用配置的用户名密码再自动登录。

# 二：功能介绍

1. 一个单点登录账户可以管理多个其他系统账户（通过网页，插件两种方式管理）
2. 提供接口注册单点登录账户

<http://127.0.0.1:8080/SSO>/registerUser

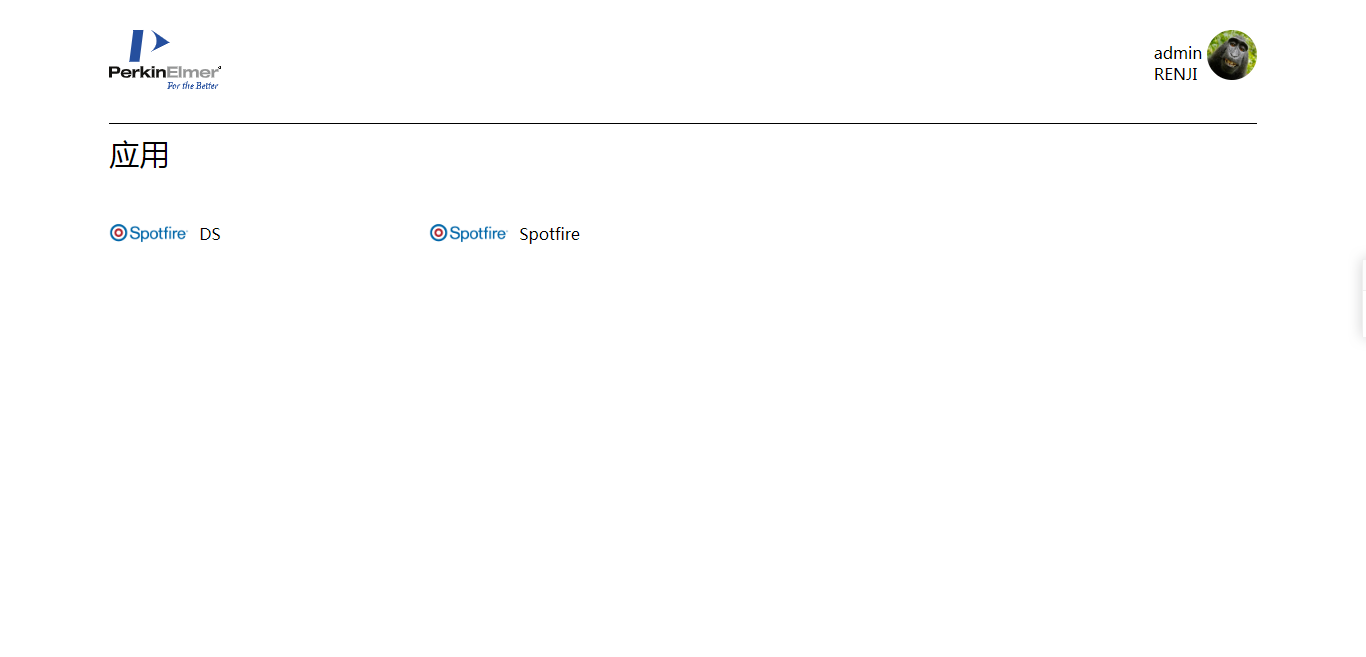
1. 记录日志（用户登录注册等于后台交互的操作）方便后续分析用户使用数据

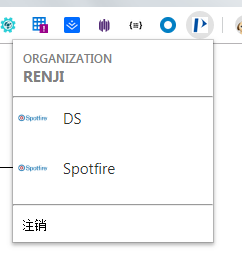
# 三：操作方法

## 1.点击插件

## 2 .首次认证中心登录

## 3 登录后展示的应用列表（可通过点击对应应用自动跳转自动登录对应应用）





## 4 带参数方式实现认证（无登陆页面）

调用链接：[http://localhost:8080/SSO/loginInner?username=admin&password=admin](http://localhost:8080/SSO/loginInner?username=admin&password=admin1)

如果验证通过则通过认证同时直接跳转到主页面

## 5 之后通过数据库，或者spotfire对后台数据进行管理（用户，应用，用户应用对象关系）

注意：其中应用的密码通过base64转码，如果应用A的账户密码为123，怎录入数据库中为123的base64编码MTIz，以此类推（这里用base64方式加密原因是为了后续能方便解密，后续也可以自行更改加密解密规则）

## 6. 操作视频



# 四：实施流程

1. 在指定服务器搭建认证中心（SSO）
2. 在需要配置单点登录的客户机，上安装谷歌浏览器
3. 安装对应谷歌插件（SSO\_client）
4. 在服务器或者spotfire上配置信息（配置应用信息，用户信息，应用用户对应信息）