

单点登录

- 1. 概要说明
- 2. 第三方系统单点登录时的几种方法

1. 概要说明

单点登录是指需要在第三方系统中不使用用户名和密码来打开Smartbi的各种资源时，此时可以采取单点登录的方式，在第三方系统登录的同时登录到Smartbi系统。

2. 第三方系统单点登录时的几种方法

可以通过以下六种方法之一，在第三方系统中单点登录到 Smartbi 系统。请根据实际需要，选择其中一种登录方法。

单点登录名称	方案简述	优点	缺点	适用系统
浏览器端SDK单点登录	通过JSLoader加载 bof.usermanager.UserService 的js方法登录。	1. 简单方便 2. 通用性高	1. 集成方式较麻烦 2. 用户名和密码暴露在前端，安全性差 3. 需要解决跨域问题。	1. 安全性要求不高的系统 2. 没有跨域问题的系统
服务器端SDK单点登录	在第三方系统中编写 JSP 页面/Java代码调用 Smartbi 的服务器端 SDK获取Cookie进行登录。	不会暴露用户的真实密码，安全性高	1. 不支持集群部署 2. 不支持从第三方系统链接转到Smartbi系统首页进行登录。	1. 安全性要求高的系统 2. 不需要集群部署的系统 3. 只适用于在第三方系统中打开和新建Smartbi资源以及在第三方中打开功能模块进行登录。
Login Token 扩展包单点登录	在第三方系统中编写JSP 页面/Java代码调用Smartbi 的服务器端SDK方法进行登录后获取Token再使用Token登录。	1. token只能使用一次且60秒内有效，不会暴露用户的真实密码，安全性高 2. 支持集群	需要加载扩展包并修改登录验证类。	1. 安全性要求高的系统 2. 集群部署的系统
Form 表单单点登录	在页面中提交form表单传递用户密码参数登录，并传递参数告知smartbi登录成功和失败跳转的地址。	集成方式简单	用户名和密码暴露在前端，安全性差。	1. 安全性要求不高的系统 2. 集成部署的系统
CAS单点登录	将Smartbi接入到统一登录认证平台进行登录。	1. 安全性高 2. 多系统集成时登录方便	1. 需要加载扩展包 2. 需要修改扩展包配置文件和登录验证类。	1. 用户已有CAS服务器的情况 2. 安全性要求高的系统 3. 集成部署的系统
令牌登录	第三方系统使用密钥对用户登录信息进行DES加密来形成token，当客户端发起的请求携带有令牌登录参数以及目标跳转地址时，Smartbi服务器拦截到请求后，对token信息进行解析和校验，如果成功解析出用户信息并校验成功，则将用户设置为登录状态，再重新定向到对应地址，后续访问其他地址无须重新登录。	1、支持配置令牌超时时间，不会暴露用户的真实密码，安全性高 2、支持集群	需要客户端使用jar包对用户信息进行加密	安全性要求高的系统