API、鉴权与权限模型

鉴权流程
用户登录后获得平台会话。访问业务 API
时，前端在受控请求层携带会话令牌；后端验证身份、菜单权限、按钮权限和数据范围。打开嵌入式分析工具时，另行申请短时一次性票据，票据只能用于指定目标页面。

浏览器 → 门户登录 → 会话令牌 → 业务 API
浏览器 → 点击分析菜单 → 后端校验权限 → 一次性票据
浏览器 → 目标系统交换票据 → 建立受控会话 → 打开指定页面

API 约定
项目 约定

基础路径 门户后端统一前缀，按模块分组

请求格式 JSON；文件上传使用 multipart/form-data

响应格式 业务码、消息、数据；分页数据包含 rows 与 total

时间格式 ISO 或统一的 yyyy-MM-dd HH:mm:ss

幂等 创建类接口支持请求号或业务唯一键

分页 pageNum、 pageSize；服务端设置最大页大小

错误码 401 未认证、 403 无权限、 404 不存在、 409 状态冲突、 422
校验失败、 429 限流、 502 下游异常

权限模型
平台权限分四层：

1. 菜单权限 ：控制目录和页面是否可见；不能代替接口鉴权。
2. 按钮权限 ：控制新增、修改、删除、审核、导出、运行等操作。
3. 数据权限 ：按全部、本部门、本部门及以下、本人或自定义部门限定数据范围。

4. 服务端资源权限 ：对数据源、项目、数据集、报表和发布目标分别校验归属与角色。

用户 → 角色 → 菜单/按钮/数据范围
用户 → 部门 → 数据范围
用户 → 项目成员 → OWNER / EDITOR / REVIEWER / VIEWER

典型接口分组

模块 接口前缀 示例

用户与个人中心 /system/user /system/user/profile

角色与部门 /system/role、 /system/dept /system/role/{roleId}

在线会话 /monitor/online 列表与强制退出

业务建模 /bi/bm 项目、字典、质量、审核、发布

数据治理 /bi/etl 调度、同步、加工、外部源、元数据

数据探索 /bi/superset 状态检查、受控启动

智能报表 /bi/jimu 状态检查、受控启动

AI 对话与分析 /bi/ai 会话、方案、确认、样式调整

安全要求
所有写接口校验 CSRF/重复提交策略和当前用户权限。
文件下载和导出再次校验数据范围，不信任前端传入的查询条件。
SQL 只读、字段白名单、行数上限、超时与取消机制必须由服务端强制执行。
跳转子系统的目标地址从服务端白名单生成，禁止开放任意 URL 重定向。
日志不得记录密码、 Token、Cookie、API Key、完整 SQL 中的敏感常量和个人联系方式。
对 AI 输入做长度与内容限制；对 AI 输出做 JSON Schema 校验和操作白名单校验。

最佳实践
1. 前端权限只用于改善体验，最终授权以后端为准。
2. 对重要业务动作使用二次确认、幂等键和审计事件。
3. 对跨服务错误返回稳定的诊断码，不把下游堆栈和内部地址暴露给浏览器。
4. 对敏感字段采用脱敏视图，原始数据访问单独授权并记录。
5. 接口变更保持向后兼容；废弃字段先标记版本，再逐步移除。

□□□ #2
□ Admin □□□ 2026-11-06 00:23:36 UTC
□ Admin □□□ 2026-11-06 03:53:33 UTC