

任擎安全保障措施

措施类别	措施描述
身份验证	支持用户名+密码、手机号+短信验证码、APP 扫码和 UKey（需要单独购买第三方硬件和系统）等多种身份验证机制。
数据传输	支持基于 HTTPS 协议的数据加密传输，身份验证等关键数据采用 AES 算法进行单独加密传输。
会话安全	每次访问都会用时间戳进行加密签名，并自动进行超时校验，如果登录后超过指定时间不做任何操作，再访问服务器会要求重新登录。
权限控制	系统提供模块、操作、数据三个级别的精细化访问权限控制，可以按用户、部门和角色群组详细设置具体可以访问哪个模块、进行什么操作、访问哪些数据。
日志记录	系统提供完备的日志记录和跟踪服务，可以详细记录系统所有的访问记录和运行状况，包括网络连接、请求数据、响应数据、数据库操作、文件上传下载、错误堆栈等等，可以随时复盘整个系统的运行过程。并且系统内提供日志查询统计模块，可以随时查询分析各种日志，包括登录日志、静态请求日志、动态请求日志、数据库操作日志、文件上传日志、文件下载日志、错误日志等。
数据访问	系统自带防 SQL 注入机制，所有请求参数默认都会进行 SQL 注入检测，发现异常自动终止服务。数据添加和修改采用专有的 ORM 技术自动进行数据类型校验和格式转换，防止插入非法字符。
数据存储与备份	密码等关键数据加密存储。支持实时主从备份、定时自动备份等多种数据备份方式。
系统稳定性	系统应用服务器采用一主多从的多进程架构，主进程负责启动和监管多个子进程，实时监控各个子进程占用的运行状态，包括 CPU、内存、网络连接、数据库连接、文件句柄等软硬件资源，发现超限或者运行异常，主进程会自动回收并重建，可以保障系统长期稳定运行。