

档案软件 - 登录日志查询功能【云丰档案软件功能介绍】

档案管理软件 · 安全管理功能介绍

谁在什么时候登录过系统、从哪里登录，是安全监控的起点。云丰档案提供登录日志查询：记录每次登录的账号、时间、地点与成功失败状态，管理员可据此发现异常登录、排查盗用，掌握系统访问的整体情况。

一、为什么需要登录日志查询

登录是所有操作的入口，登录记录是安全监控最基础的线索：

登录无记录：谁什么时候登过系统，毫无记载；

异常难发现：有人盗用账号异地登录却毫无察觉；

失败无人管：反复登录失败的撞库行为无人关注；

审计缺数据：安全检查需要登录记录时拿不出来。

登录日志要把每一次进入系统的尝试都记下来，让异常登录浮出水面。

二、怎么用

系统记录每次登录行为，管理员在日志模块按条件查询分析：

表1 登录日志记录内容

记录项	说明
登录账号	记录尝试登录的账号
登录时间	精确记录每次登录发生时间
终端信息	记录登录来源与终端信息
成功失败	区分登录成功或失败及失败原因
异常标记	对异地、失败频繁等情况辅助识别

登录日志与操作日志分开记录，专看账号进出。管理员应重点关注非工作时间登录、异地登录和连续失败记录，及时发现盗用或撞库迹象。

按人、按时间、按地点或终端检索登录记录，能看出某人何时从何处登录成功或失败。异常时段、异地登录被自动标记，供管理员排查。

查询结果可按人导出，作为安全检查材料；对同一账号的异地、异时登录可重点比对，发现异常即锁定核查。登录记录是判断账号是否被盗用的第一手线

索，定期回看能把可疑访问在造成损失之前发现，而不是等档案外泄后才事后追溯。

查询结果可按人导出作为安全检查材料，对异地异时登录重点比对，及早发现可疑访问。

支持按失败登录单独筛选，管理员据此定位被反复尝试的账号，重点加固。

支持按异常时段、失败次数、来源地址组合筛选，管理员可快速发现非本人登录和异地尝试。日志与账号、终端信息关联，安全事件发生时可逐层还原，日常巡检与专项核查都在一个页面完成。

三、核心能力

表2 核心能力一览

能力	一句话价值	关键细节
进出可查	谁登过有数	记录每次登录的账号与时间。
异常识别	发现盗用	辅助识别异地、频繁失败等异常登录。
成败都记	撞库可见	失败尝试也记录，暴露攻击行为。
多条件查	快速定位	按账号、时间、结果组合检索。
长期留存	审计备查	登录记录作为安全审计依据。

登录记录是账号是否被盗用的第一线索，定期查看能及早发现可疑登录。

四、典型使用场景

- 日常巡检：管理员查看近期登录情况，发现异常；
- 盗用排查：账号可疑时按登录记录定位异常登录；
- 合规审计：安全检查调取登录日志备查。

五、价值与产品定位

登录日志查询让系统的每一次进出都有迹可循：谁登过、何时登、从哪登、成功与否，一目了然。它帮助管理员及时发现盗用和撞库，是账号安全监控最直接的抓手。它让谁什么时候进来过清清楚楚。

它与操作日志、访问日志共同构成审计日志体系：登录看谁进了系统，操作看在系统里做了什么，访问看动了哪些档案。三者叠加，使档案系统安全可监控、事件可复盘。云丰档案把登录行为纳入可审计视野。