操作日志

功能定位
操作日志记录用户在系统中的新增、修改、删除、导出、登录等关键动作，用于安全审计、问题追踪和责任界定。日志正文和客户端信息会脱敏展示。

图 8-8 操作日志筛选、详情、导出与清理

适用角色
系统管理员、安全审计人员和运维人员。

页面入口
系统管理 → 日志管理 → 操作日志（ /system/log/operlog）。

筛选条件
操作地址、系统模块、操作人员、客户端、设备类型、浏览器、操作系统、操作类型、操作状态和操作时间。

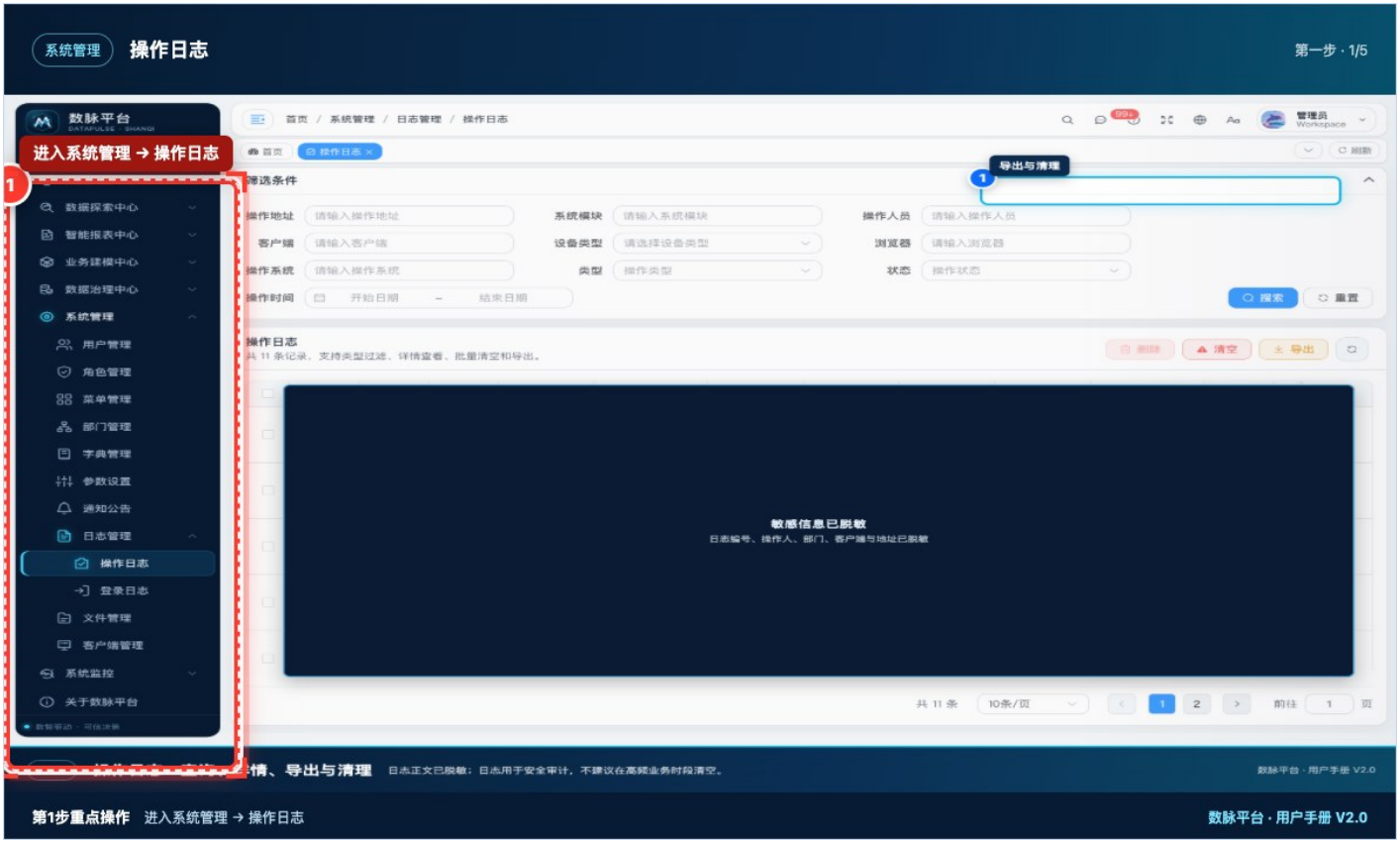
操作步骤
1. 按时间、操作人员或模块缩小范围，避免一次查询全部日志。
2. 点击详情查看请求方法、业务参数摘要、返回结果和耗时。
3. 发现异常操作时记录日志编号、用户、时间、 IP 摘要和影响对象。
4. 需要归档时使用 “导出 ”，导出文件应按敏感级别存放。
5. “删除 ”用于清理单条记录， “清空 ”影响范围更大，必须经过审批并在低峰期执行。
6. 安全事件排查应同时比对登录日志、在线用户和业务审计。

输入与输出
输入是筛选条件和日志记录；输出是审计明细、导出文件和清理记录。

宏澜家电示例
发现某报表被批量导出，审计人员按操作类型 “导出 ”
和时间范围查询，确认操作人属于财务共享中心，导出范围为授权部门；将日志编号和导出用途记录在审计台
账。

客户应用演示：追踪一次报表导出操作
业务情境： 需要确认某份费用报表是否被导出、由谁在什么时间导出。

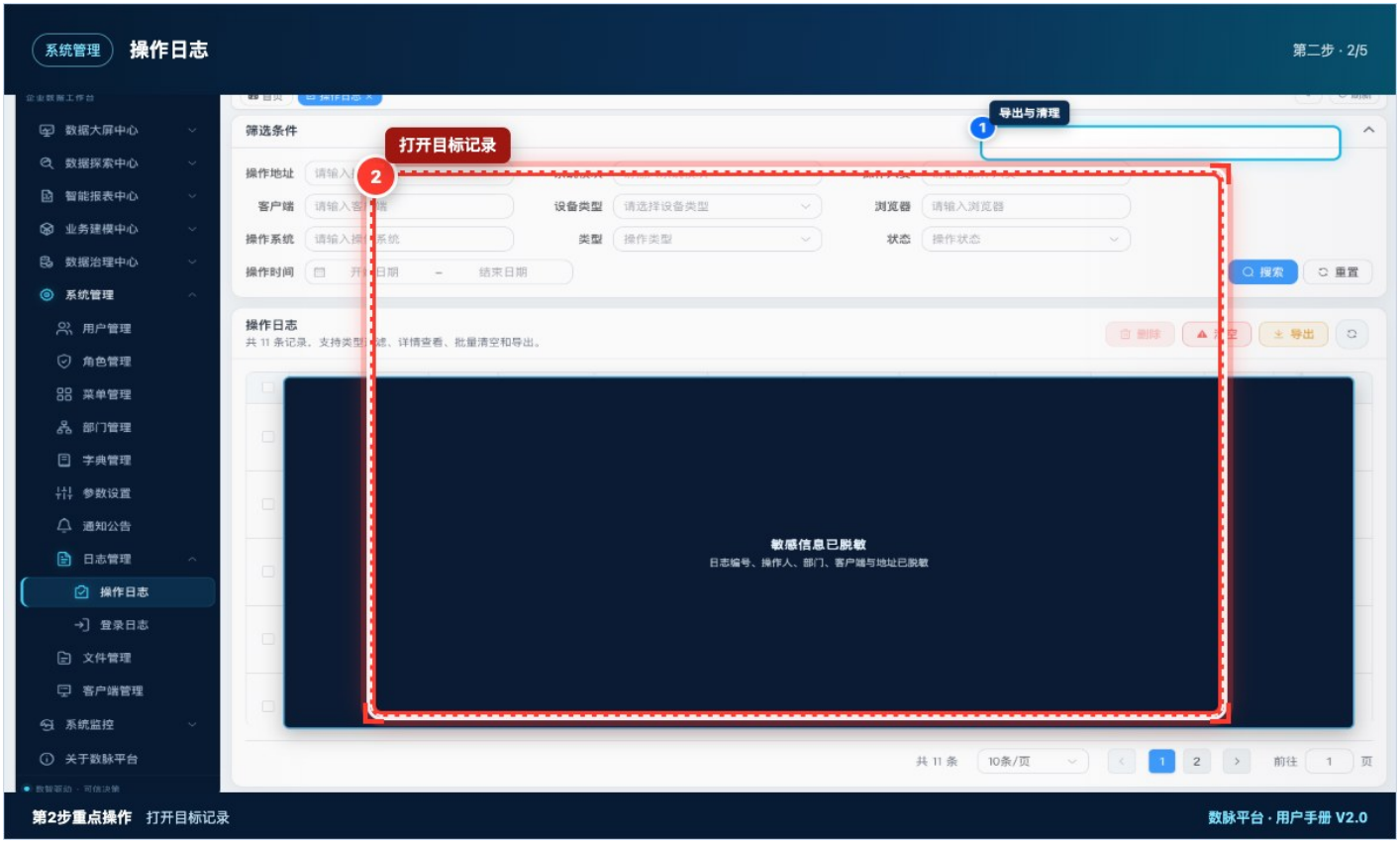
第一步：进入 “系统管理 → 操作日志 ”



步骤图 51-01 第1步：进入 “系统管理 → 操作日志 ”。红框标出进入系统管理 → 操作日志。

进入 “系统管理 → 操作日志 ”，按模块、操作人和时间筛选。

第二步：打开目标记录



步骤图 51-02 第2步：打开目标记录。红框标出打开目标记录。

打开目标记录，查看操作类型、请求路径、结果和来源地址。

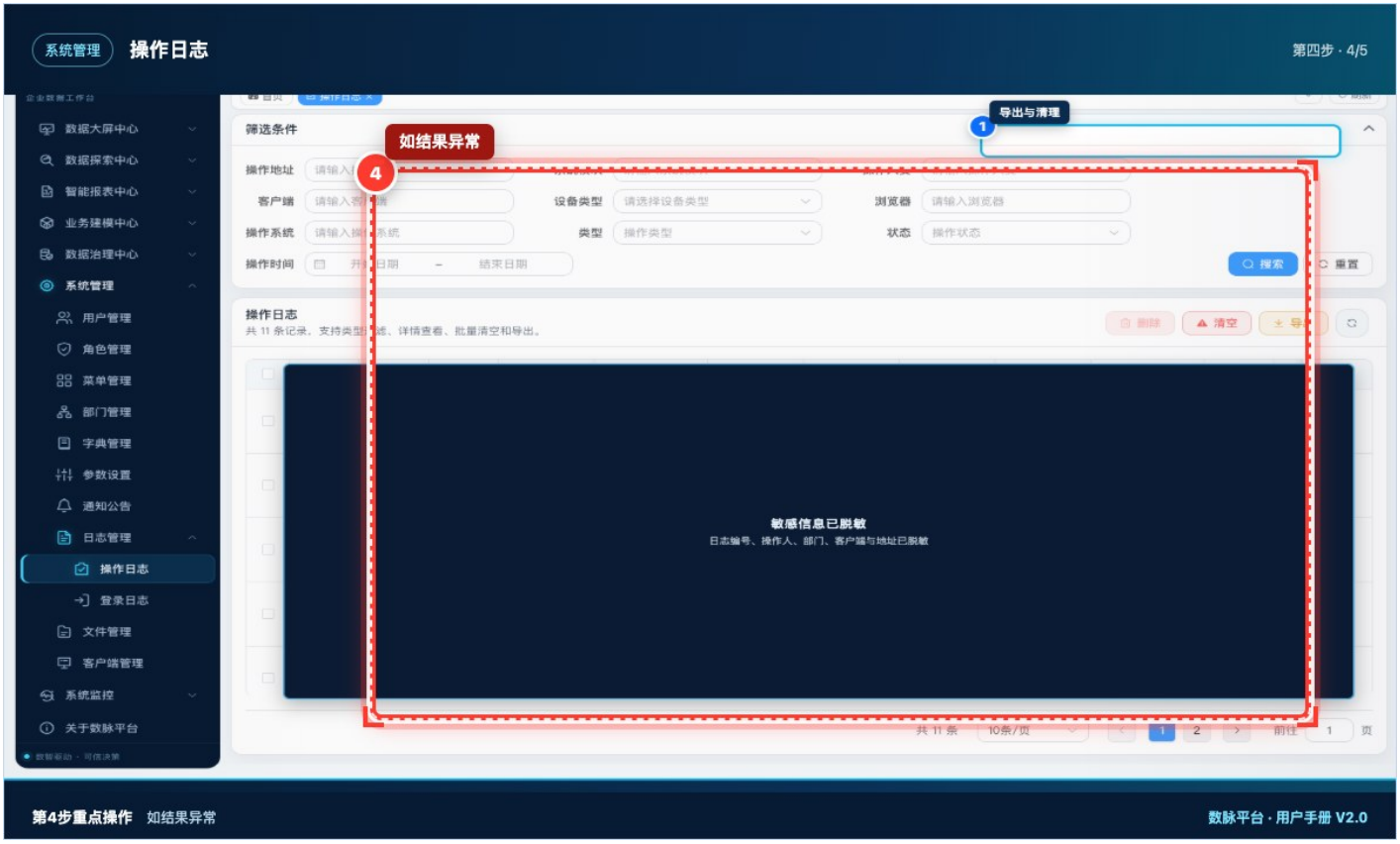
第三步：核对业务对象、导出时间和执行结果



步骤图 51-03 第3步：核对业务对象、导出时间和执行结果。红框标出核对业务对象、导出时间和执行结果。

核对业务对象、导出时间和执行结果。

第四步：如结果异常



步骤图 51-04 第4步：如结果异常。红框标出如结果异常。

如结果异常，记录日志编号并联系对应模块管理员。

第五步：按制度处理敏感导出



步骤图 51-05 第5步：按制度处理敏感导出。红框标出按制度处理敏感导出。
按制度处理敏感导出，不在聊天工具传播日志中的个人信息。

最终结果与效果
能够定位操作人、时间、动作和结果，为安全审计和问题排查提供证据。

操作提示： 日志查询本身也是敏感操作，应按最小权限使用。 “

常见问题
查不到刚发生的操作。 日志可能异步写入，稍等后刷新；也可能是只读查询未记录。
详情中的参数被脱敏。 这是安全设计，确需排查时由授权管理员在受控环境查看原始审计数据。清空后无法恢复。 清空是不可逆操作，必须先导出归档并完成审批。

开发人员参考
接口： /monitor/operlog、 /monitor/operlog/{operlogId}、 /monitor/operlog/export
权限： monitor:operlog:list、 monitor:operlog:query、 monitor:operlog:remove、 monitor:operlog:export
通过注解或切面记录模块、操作类型、方法、参数摘要、结果和耗时。
参数和返回体需脱敏，禁止记录密码、 Token、Cookie 和完整个人联系方式。

版本号 #2
由 Admin 创建于 2026-11-06 00:23:30 UTC
由 Admin 更新于 2026-11-06 03:53:24 UTC