客户端管理

功能定位
客户端管理维护接入数脉的 OAuth/OIDC 客户端，包括客户端 Key
、密钥、授权类型、回调地址、状态和权限范围。它用于第三方系统单点登录或 API 接入。

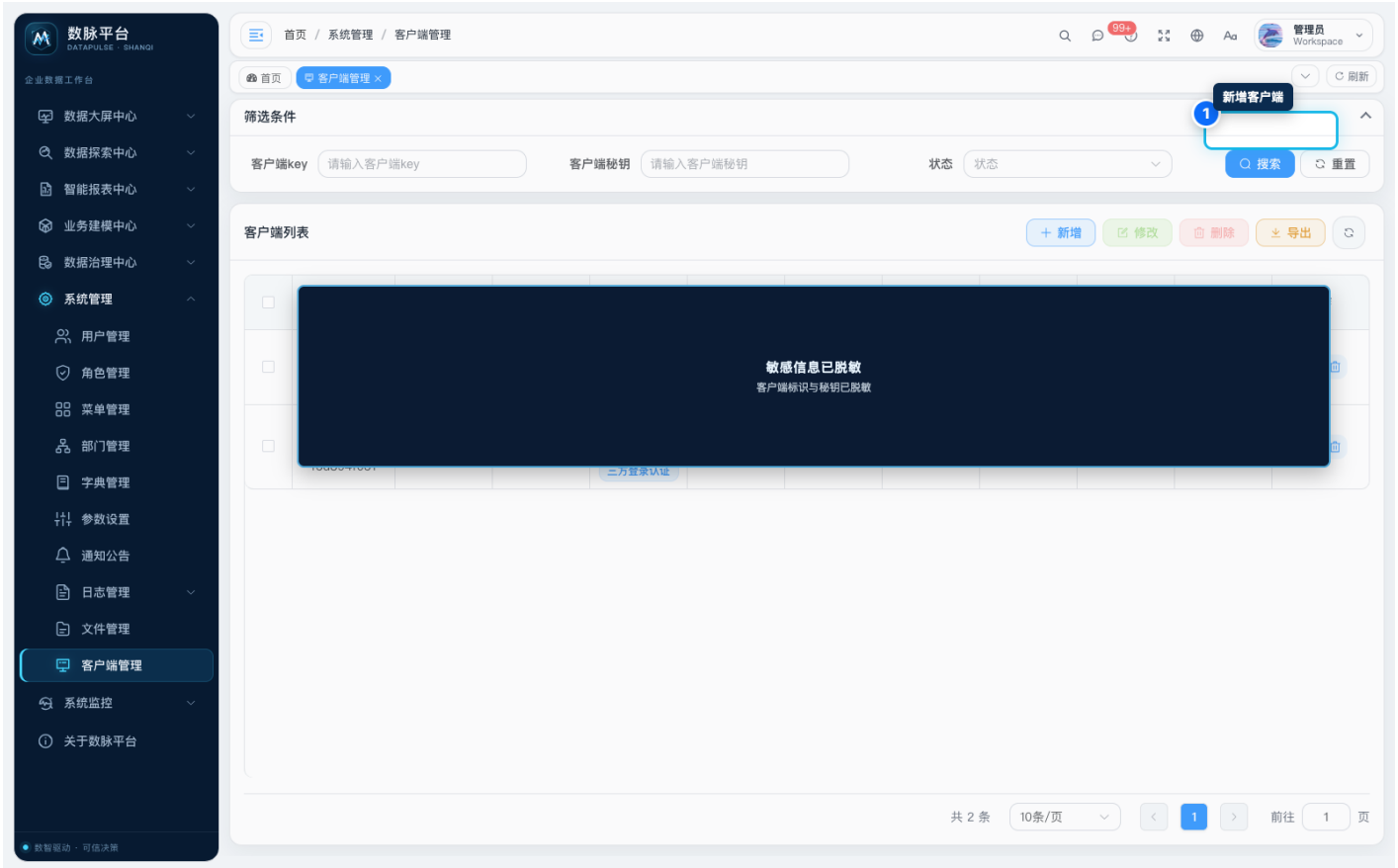


图 8-11 客户端标识、密钥和授权配置

适用角色
系统管理员、集成开发人员和安全管理员。

页面入口
系统管理 → 客户端管理（ /system/client）。

操作步骤
1. 点击 “新增 ”，填写客户端名称、 Key、授权类型、回调地址和权限范围。
2. 密钥由系统生成或安全注入，页面和日志只显示脱敏值。
3. 回调地址必须精确匹配，禁止使用任意通配符或未登记域名。
4. 选择最小权限范围，第三方系统不应获得全量用户和 BI 权限。
5. 保存后先在测试环境完成授权码或客户端凭证流程，再上线。
6. 定期轮换密钥；停用客户端前通知接入方并确认没有在线会话。

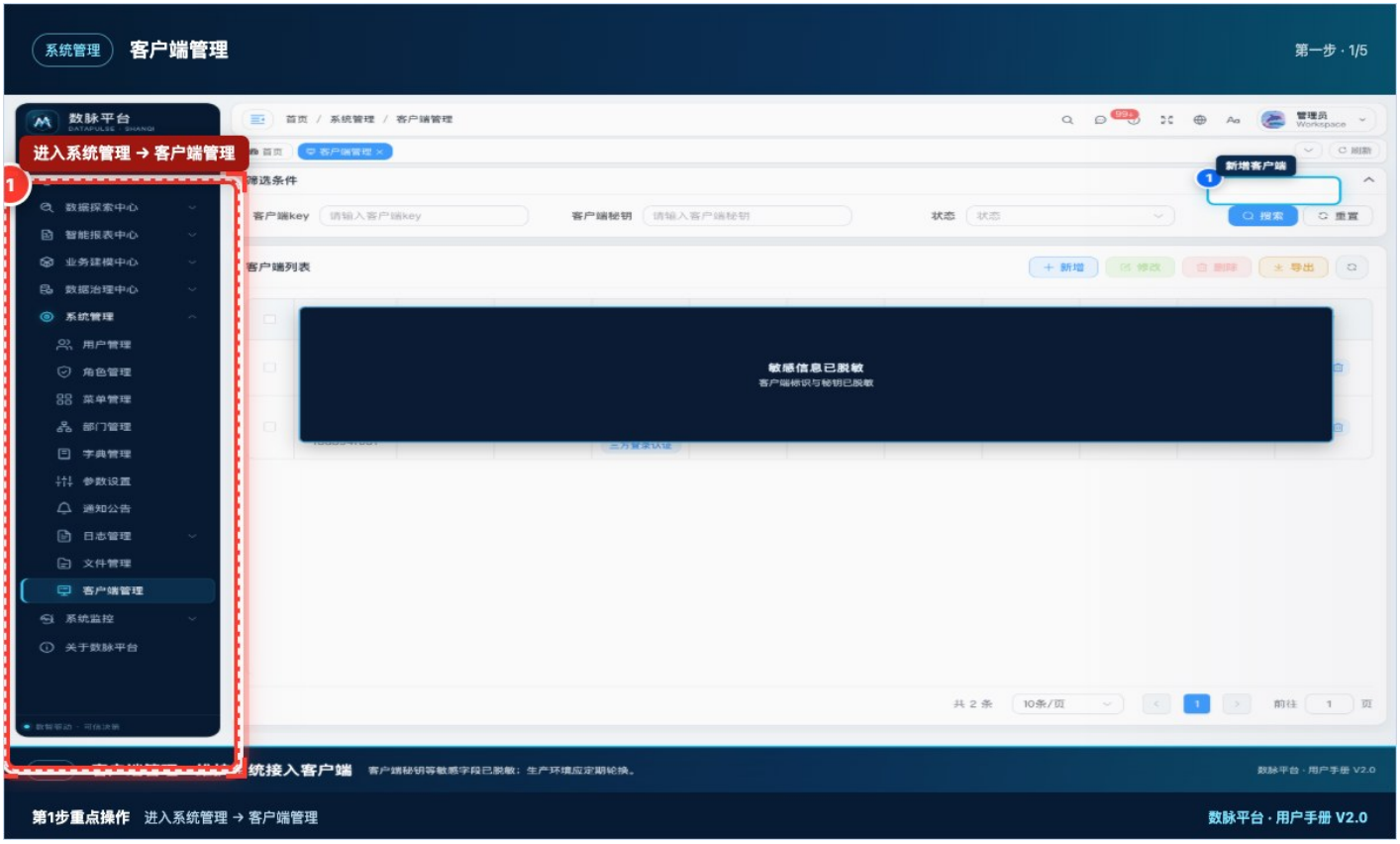
输入与输出
输入是客户端元数据、密钥、回调和权限范围；输出是接入凭据、授权记录和访问审计。

宏澜家电示例
ERP 门户通过 OIDC 单点登录进入数脉，只申请用户基本信息和 “查看已发布大屏 ”
权限。客户端密钥由密钥管理服务注入，回调地址限定为 ERP 门户的固定域名。

客户应用演示：停用不再使用的测试客

户端
业务情境： 安全检查发现旧的测试客户端仍可访问接口，需要停用。

第一步：进入 “系统管理 → 客户端管理 ”



步骤图 54-01 第1步：进入 “系统管理 → 客户端管理 ”。红框标出进入系统管理 → 客户端管理。进入 “系统管理 → 客户端管理 ”，按名称和时间找到测试客户端。

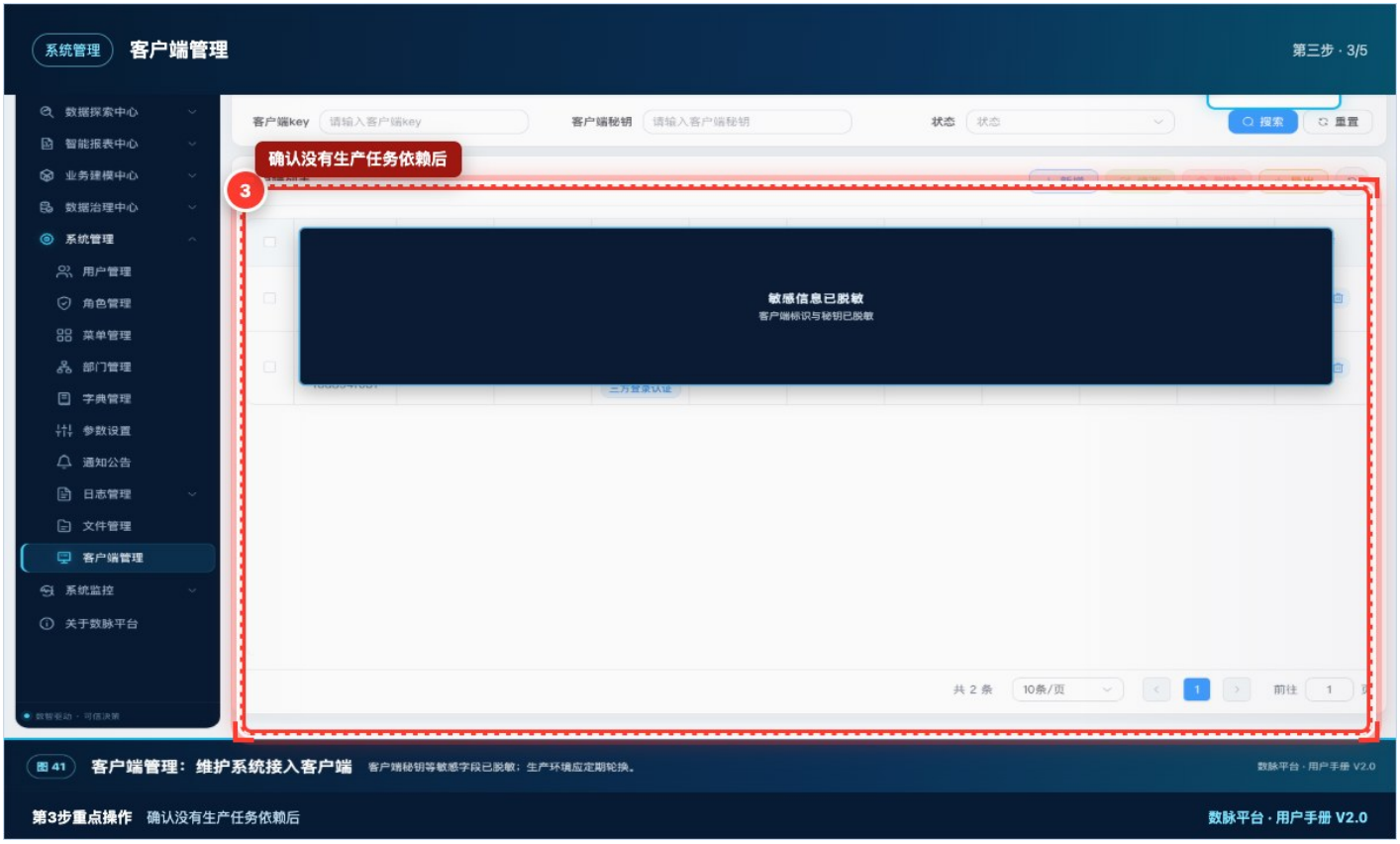
第二步：查看授权类型、有效期、状态和关联
用户



步骤图 54-02 第2
步：查看授权类型、有效期、状态和关联用户。红框标出查看授权类型、有效期、状态和关联用户。

查看授权类型、有效期、状态和关联用户。

第三步：确认没有生产任务依赖后



步骤图 54-03 第3步：确认没有生产任务依赖后。红框标出确认没有生产任务依赖后。

确认没有生产任务依赖后，点击 “修改 ”并将状态设为停用。

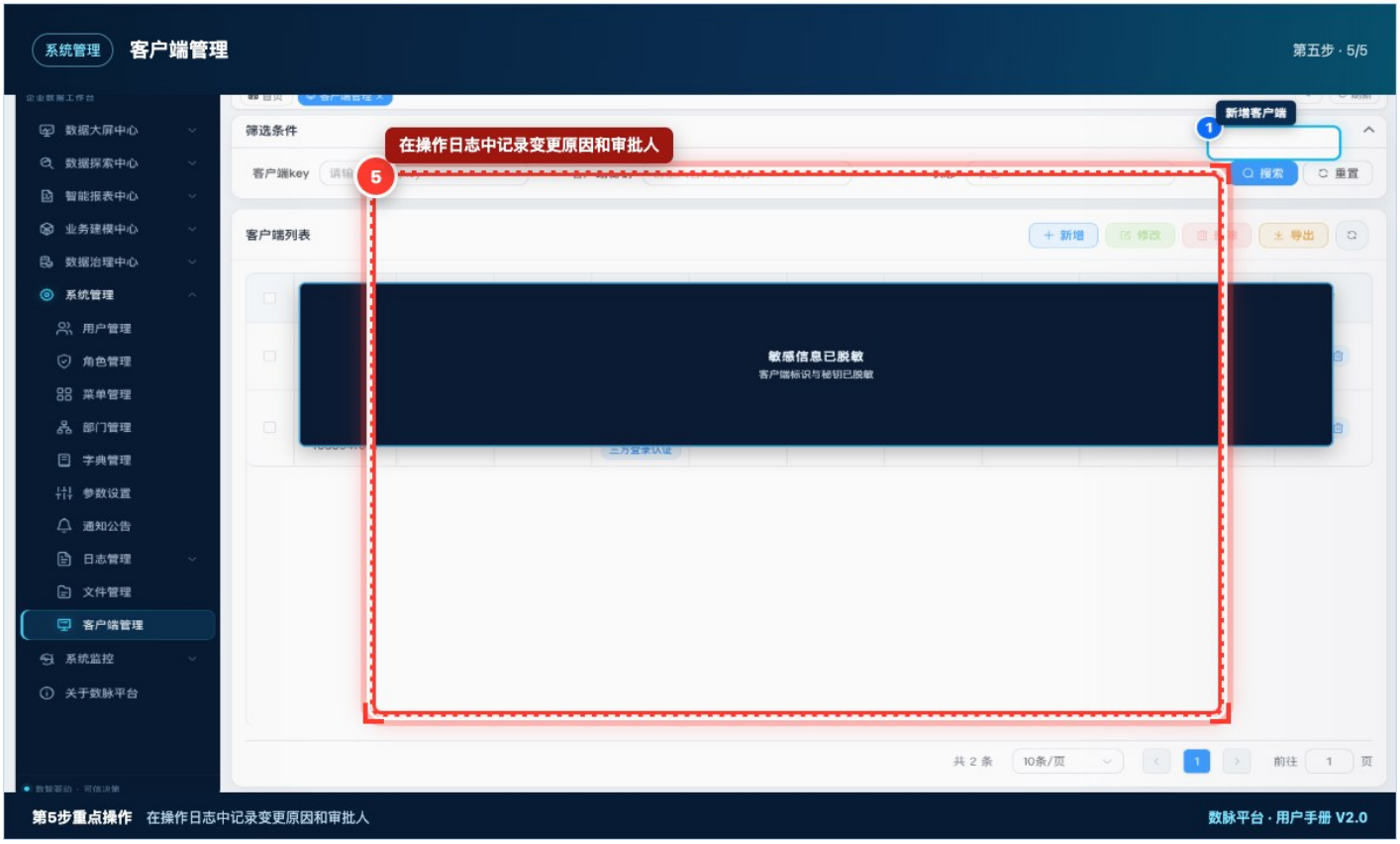
第四步：保存后验证生产客户端仍可正常访问



步骤图 54-04 第4步：保存后验证生产客户端仍可正常访问。红框标出保存后验证生产客户端仍可正常访问。

保存后验证生产客户端仍可正常访问。

第五步：在操作日志中记录变更原因和审批人



步骤图 54-05 第5步：在操作日志中记录变更原因和审批人。红框标出在操作日志中记录变更原因和审批人。
在操作日志中记录变更原因和审批人。

最终结果与效果
测试客户端失效，生产调用不受影响；配置变更可追溯。

操作提示： 客户端密钥属于高敏感信息，不截图、不复制到文档或聊天工具。 “

常见问题
授权回调报 redirect_uri_mismatch。 回调地址必须与登记值完全一致，包括协议、端口和路径。第三方能登录但看不到数据。 客户端只解决身份认证，数据权限仍由数脉角色和数据范围决定。
密钥泄露。 立即停用客户端、轮换密钥并检查访问日志。

开发人员参考
接口： /system/client、 /system/client/{clientId}
权限： system:client:list、 system:client:add、 system:client:edit、 system:client:remove
、 system:client:export
客户端密钥使用加密存储，接口不回显明文。
授权服务器应校验 PKCE、回调白名单、 Token 有效期和作用域。

版本号 #2
由 Admin 创建于 2026-11-06 00:23:32 UTC
由 Admin 更新于 2026-11-06 03:53:28 UTC