

D11 运营管理域 · 设计文档

本域总览见《账号计费中心 · 结构大纲》。本文为该域完整设计：定位与边界 / 角色与依赖 / 数据模型 / 核心流程 / 接口契约 / 关键约束与验收标准。

本域是运营与管理后台的功能域，覆盖全部功能域的管理面能力：谁可以进运营面、能做哪一类事、每次变更如何留痕。全文按「数据模型 → 核心流程 → 接口契约」排布（先事实结构，再运行路径，最后对外投影）。

1. 定位与边界

定位：运营侧的身份与权限唯一判定者、运营端点统一门禁、运营动作留痕方。回答三问：平台员工是谁、权限范围是什么；某条运营端点在当前请求下是否放行；这次动作留下什么可复核的证据。业务能力本身（钱怎么扣、票怎么开、风险怎么判）不属本域。

核心概念

概念	承载	语义
平台员工	<code>platform_staff</code> 一行	员工不是独立账号：既有账号加绑定行即员工；无绑定行访问运营端点一律拒绝
权限范围	<code>platform_staff</code> 的 <code>scopes</code>	授权唯一真相；每请求查库、不缓存进令牌，停用与改范围即时生效
权限簿	值域常量目录	范围全集（10 值），接口与提权工具双端引用；目录外取值一律拒绝
粗粒度权限	<code>saas:ops</code>	运营全集，隐含全部子域权限；反向不成立
运营面令牌	门户令牌（门户类型）	只证明会话身份、不承载权限——权限每请求另查
内部运营令牌	内部令牌的运营 scope	服务级凭据，供运营代理与部署侧任务调用内部写面
权限载体留痕	应用层审计行加库层审计行	同一事件两行：应用行带操作人，库层行带库执行角色
平台设置与客户端	<code>platform_settings</code> 键值行、 <code>oauth_clients</code> 登记行	平台级配置落点（无记录按默认语义）与单点登录客户端登记（可注册、改配、启停，不删除）

关键口径

- 每请求查库而非读令牌声明：令牌只答「你是谁」，权限每请求点查绑定行，撤销的生效时点即下一请求。
- 未知权限一律拒绝：写入前做目录校验；错拼静默无权比显式拒绝更危险。
- 门禁失败不区分原因：无绑定、已停用、权限不足对外同一响应；库层留痕是应用层审计的兜底，库层行证明「有连接直接改过这张表」。

边界

- 不管被管理能力的业务语义：客户账务、订单与支付、退款与对账、对账台账、发票、风控与实名、通道配置的自有语义在各域（详见 D03~D10），本域只登记入口。

- 不管通知投递与凭据加密落库（通知与触达域）、不管统一登录服务本体（授权码兑换与回调精确匹配在统一登录侧，登记行归属见 D01）、不管账号本体（停用员工只改绑定行状态）。
- 端点语义分属：语义写在能力所属域，索引统一登记在本域（§5.5）。

2. 角色与依赖

能力矩阵

能力	本域	运营面调用方	统一登录服务	门户用户
维护员工绑定与权限范围	✓（唯一写入口）	仅经本域端点	✗	✗
判定运营请求是否放行	✓（唯一实现）	依赖本域	✗	✗
读员工绑定事实	✓	依赖本域	✓（内部点查）	仅本人绑定
平台设置读写与客户端登记	✓	依赖本域	✗	✗
单点登录客户端登记	✓（运营面唯一写入口）	依赖本域	✓（消费登记行）	✗
运营动作留痕	✓	✗	✗	✗

- 运营面有两条鉴权通道：人员通道（门户令牌加绑定加权限范围）与服务通道（内部令牌的运营 scope）；二者互不替代——服务通道不免去权限范围校验，人员通道不获得内部点查能力。身份来自门户令牌，权限不来自令牌，这是「停用即失权」的前提。

上游依赖

上游	依赖内容	语义
账号与身份域	账号行与已验证联系方式	绑定按账号定位；授权入口按已验证邮箱唯一定位；令牌只证明会话身份
通知与触达域	可用短信通道清单	开关开启前置；通道停用触发反向联动
关系库	触发器与守卫函数	库层留痕与清空守卫的执行前提

下游被引用

引用方	引用内容	语义
统一登录服务	内部员工绑定点查端点	登录后判定操作者与调用者角色，只回绑定事实
全部运营面端点	门禁依赖（绑定加权限范围）	每端点执行前统一校验，权限不足即拒绝
各能力域	运营入口与审计行	业务语义由各域实现，留痕口径由本域统一；审计行回答「谁在何时对哪个对象做了什么」
运营门户前端	本人绑定与权限范围	菜单与无权限页渲染依据；运营门户地址随绑定下发

3. 数据模型

3.1 域内关联总览

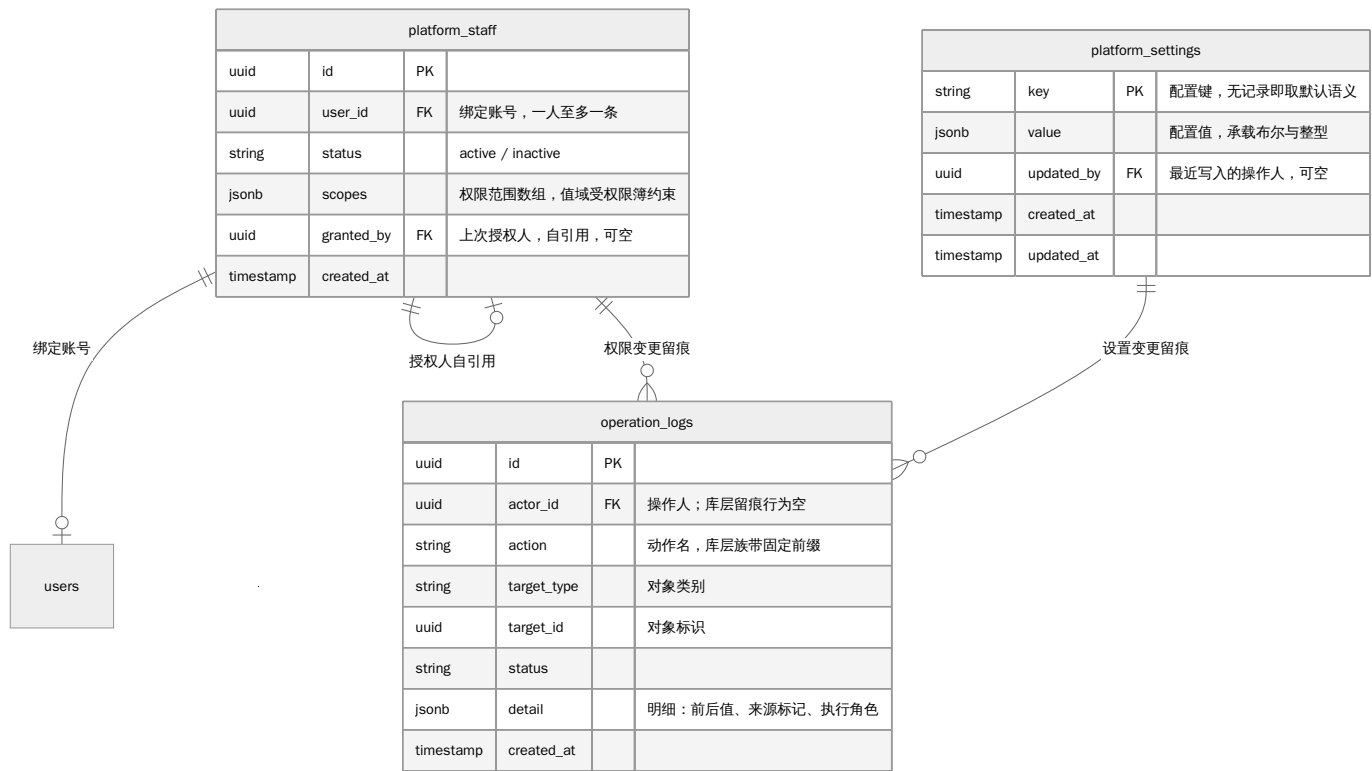


图 1

3.2 域间引用

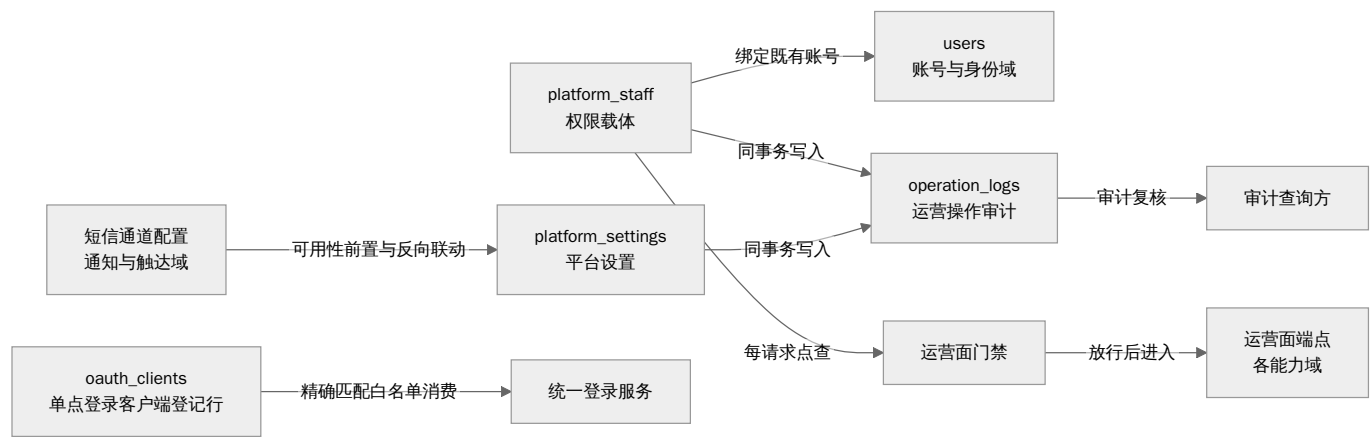


图 2

- 引用是单向的：本域读账号行与通道可用性，反向不存在「谁读本域的表做业务判定」——权限判定唯一实现只在本域。
- `operation_logs` 为平台审计共用表，本域是其两个写入方（应用层写入点与库层触发器）；客户端登记行归属统一登录侧，本域是其运营面唯一写入口。

3.3 表清单

表	职责	关键字段
platform_staff	权限载体：员工绑定行，一人至多一条	user_id / status / scopes / granted_by / created_at
platform_settings	平台设置：键值行，运营门户自助开关的唯一事实源	key / value / updated_by / created_at / updated_at
operation_logs (引用)	运营操作审计：应用层审计行与库层留痕行的共同去向	actor_id / action / target_type / target_id / detail / created_at
oauth_clients (引用)	单点登录客户端登记：回调白名单与申请范围	client_id / client_name / redirect_uris / scope / is_active
users (引用)	绑定主体的账号行，员工身份来源	id / display_name / is_active

3.4 设计约束

1. 权限范围值域封闭：全集 10 值（staff:manage、saas:ops 及其 6 个子域、router:operator），目录外取值拒绝（状态码 422、明细 unknown_scope），值域单处定义、双端引用。
2. 粗粒度隐含子域：覆盖判定为「等于要求值，或以要求值的前缀加分隔符」；子域不覆盖全集，员工管理与运营面角色为独立维度。
3. 绑定行唯一且状态两值：user_id 上有唯一索引 uk_staff_user，账号行不做员工标记；status 仅 active / inactive，停用保留行与范围。
4. 权限不落令牌、空范围非法：门禁每请求点查绑定行；空数组写入拒绝（明细 empty_scopes）。
5. 自锁防护：本人范围不含 staff:manage 即拒（明细 cannot_remove_own_staff_manage）；不得停用本人绑定（明细 cannot_modify_self）。
6. 设置默认语义二分：开关类 key 无记录即假且不预置初始行；时长类无记录或取值非法回落业务原值（验证码 10 分钟、邀请 7 天），取 0 属危险值。
7. 取值时机：每请求读库、无进程内缓存；时长类只影响新签发的行，既有行到期时刻在创建时已落库。
8. 权限载体库层强制留痕：该表需要合法更新（调范围、停复工），不适用只增不改的拒写形态；AFTER 行级触发器把插入 / 更新 / 删除的前后整行值写入 operation_logs，动作名前缀区分三动作，操作人置空（库层无人员身份）、数据库执行角色入明细。
9. 清空语句守卫与留痕同事务：BEFORE 语句级守卫直接拒绝清空（状态码类 23000）；业务回滚则留痕回滚、不留孤儿；旁路须「事务级开关为开」且「当前角色为维护角色成员」（append_only_bypass_authorized 兼查角色存在性）。
10. 客户端登记值域与不留删除：client_id 为小写字母数字与连字符、首尾为字母数字；redirect_uris 须绝对地址且不带片段；scope 限 openid、portal 且不重复；只提供启停（软开关、不删行）。

4. 核心流程

4.1 运营请求的三级门禁

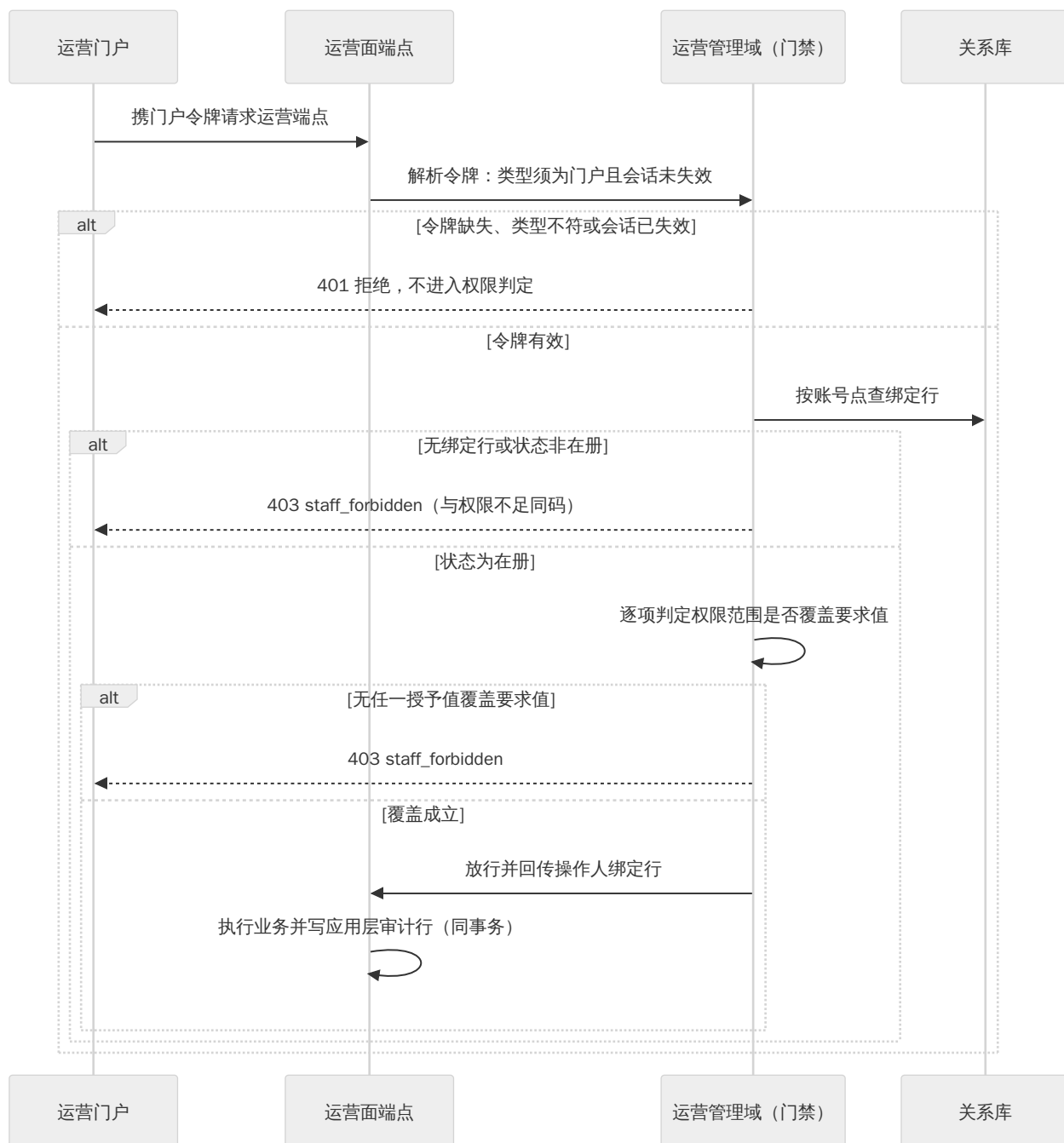


图 3

- 次序固定：先身份、再绑定、后权限；覆盖判定为「任一授予值覆盖任一要求值」，粗细粒度可混用。
- 停用与改范围的生效时点即下一请求；门禁回传的绑定行直接用作操作人标识。

4.2 员工的授权、改范围与停复工

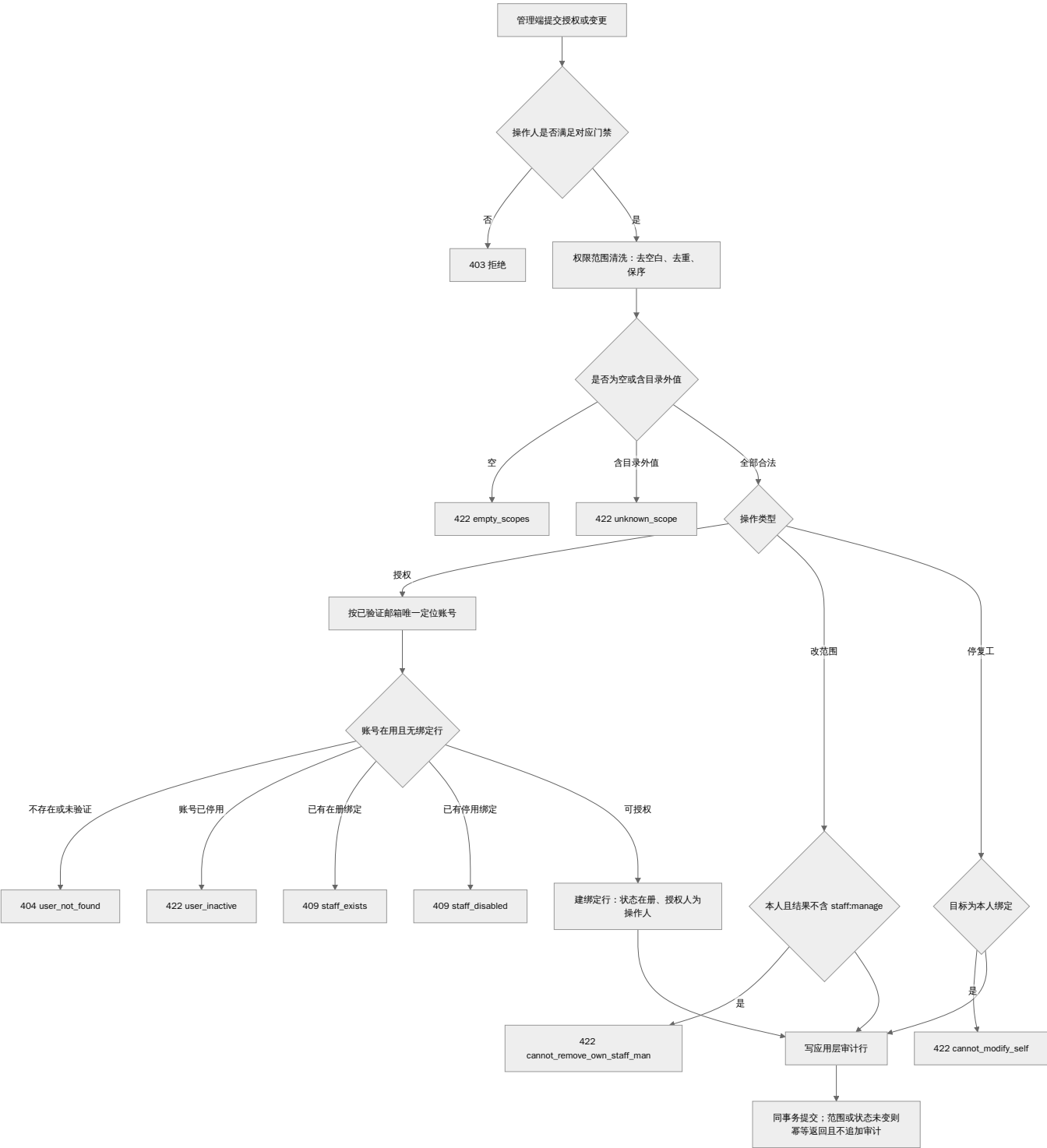


图 4

- 改范围为替换语义并把授权人改写为本次操作人；范围或状态未变即返回未变更且不追加审计行；提权工具走追加语义、不写审计。
- 停用不删行、不清范围，恢复即原权复位，两动作各留一行审计；授权入口对「账号不存在」与「邮箱未验证」返回同一结果。

4.3 权限载体的库层强制留痕

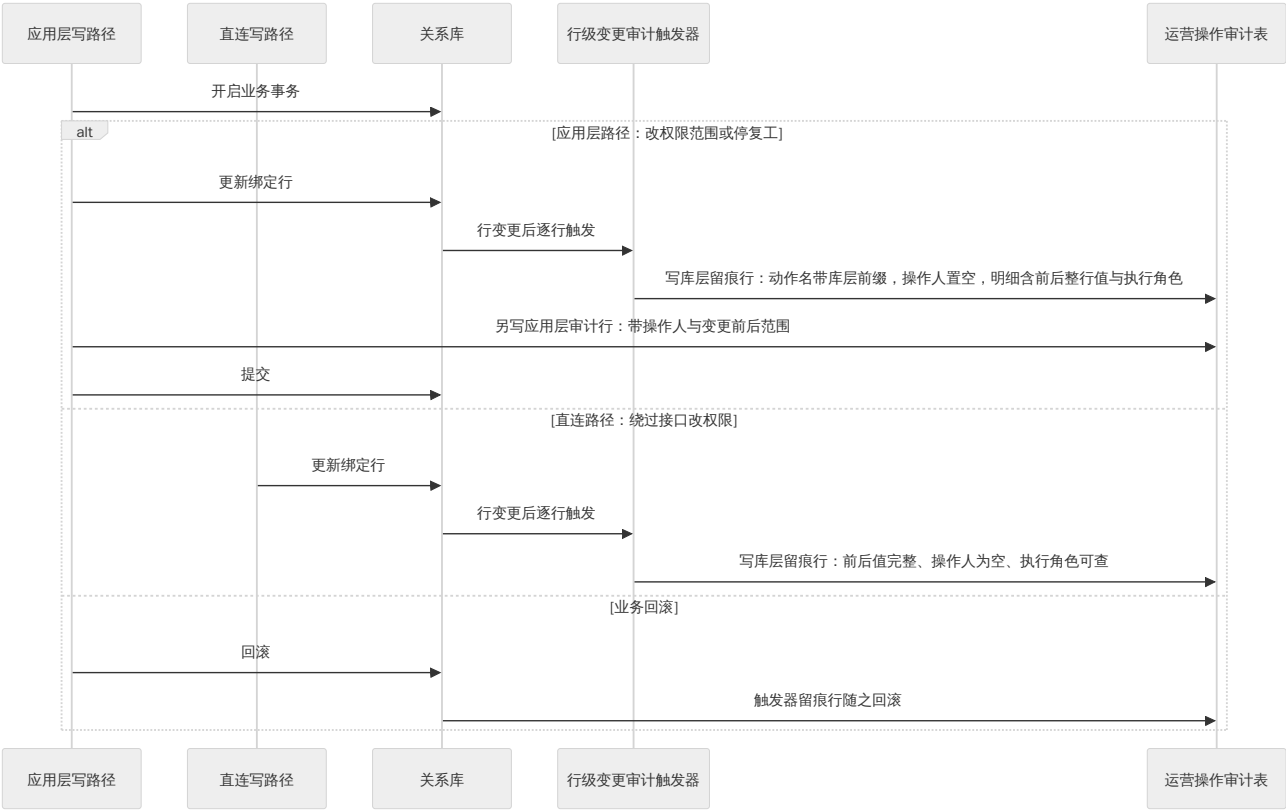


图 5

- 为何不是只增不改：该表需要合法更新（调范围、停复工），拒写式守卫会连正常运营动作一并堵死。
- 动作前缀三分：动作名 `platform_staff.db_insert`、`platform_staff.db_update`、`platform_staff.db_delete` 对应插入 / 更新 / 删除，对象类别固定 `platform_staff`、对象标识取绑定行标识。
- 明细五项：`source` 固定 `db_trigger`、`db_user` 记执行角色、`user_id` 记被绑账号、`old` 与 `new` 为整行快照（插入行旧值为空、删除行新值为空、更新行两侧齐全）。
- 操作人何为空：库层拿不到运营后台的会话身份（属应用层概念），故 `actor_id` 一律为空，人员线索落在并存的应用层审计行上。
- 同事务因果：业务回滚则留痕一并回滚、不留孤儿；多行语句逐行留痕，不塌缩成一条无法定位的记录。

4.4 清空语句的语句级守卫与受控旁路

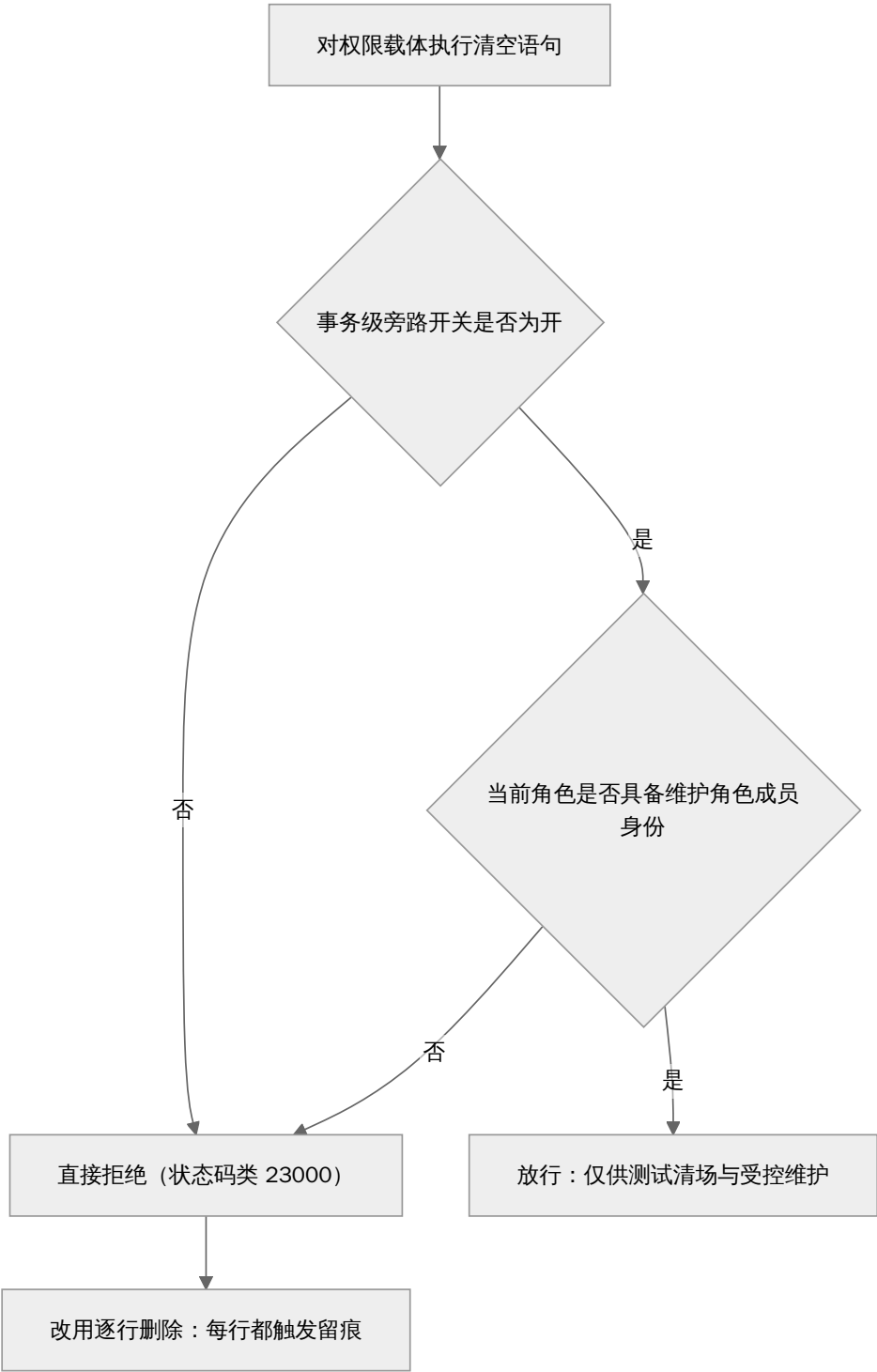


图 6

- 该守卫必须存在：行级触发器只对行级动作触发，缺了语句级那条即可静默清空整张权限表。
- 旁路为双门槛（开关为开且当前角色为维护角色成员；判定兼查角色存在性，不存在即未授权），角色判定用当前角色；维护角色不自动授予任何角色。

4.5 平台设置的读写与前置联动

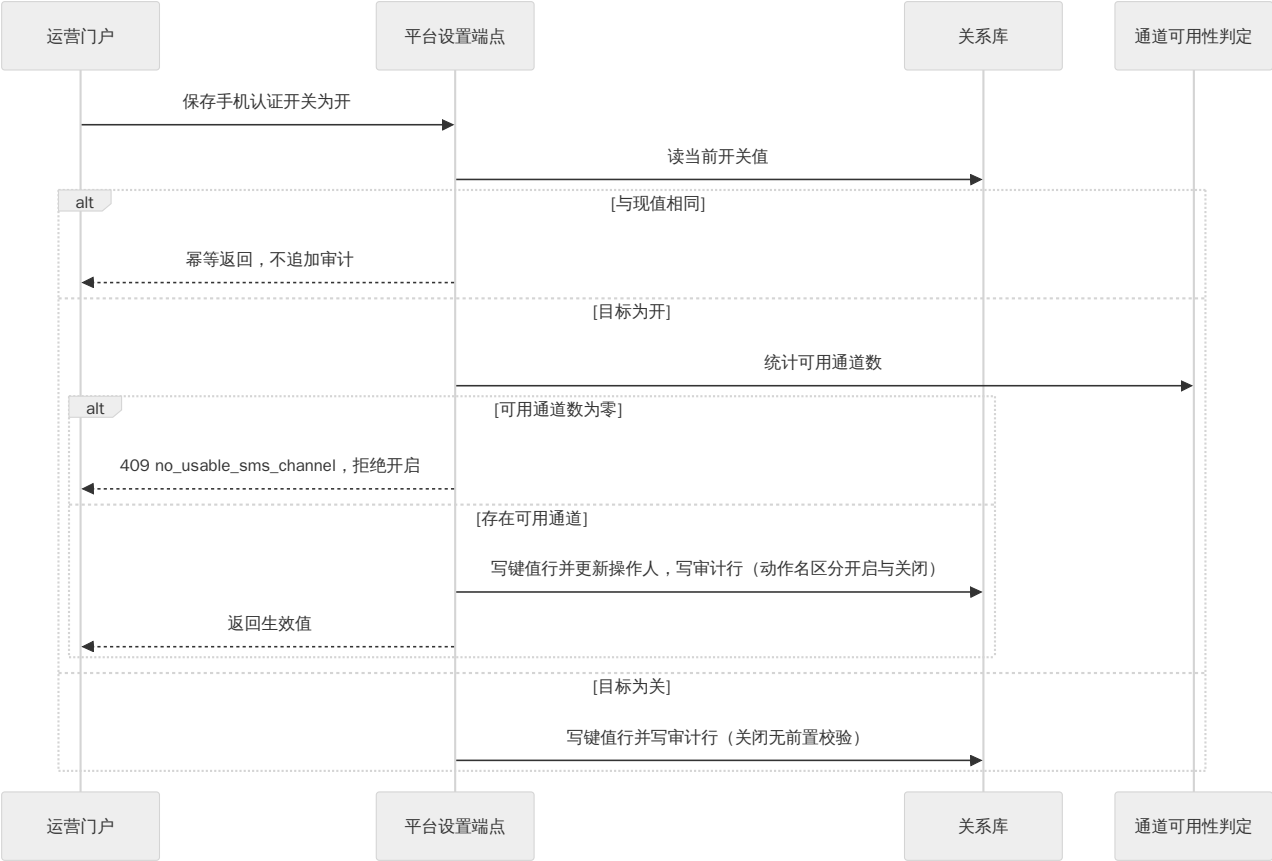


图 7

- 前置单调：开启要求至少一条可用通道（启用且凭据完整），关闭无前置，杜绝「开关开着却发不出凭证」。
- 反向联动：通道停用路径同事务检查，开关为开且已无可用通道即自动置关，并落一行动作名 `platform_setting.phone_auth_auto_disabled`、明细含原因的审计行。

4.6 时长类参数的读取与回落

- 无记录、非整数或越界一律回落业务原值（验证码 10 分钟、邀请 7 天）；回落而非清零——取 0 会让凭证立即失效。
- 区间常量写入与读取同源（验证码 1 至 60 分钟、邀请 1 至 365 天），越界在写入端点先行拒绝（明细 `ttl_out_of_range`）；只影响新签发。

4.7 单点登录客户端的登记与变更

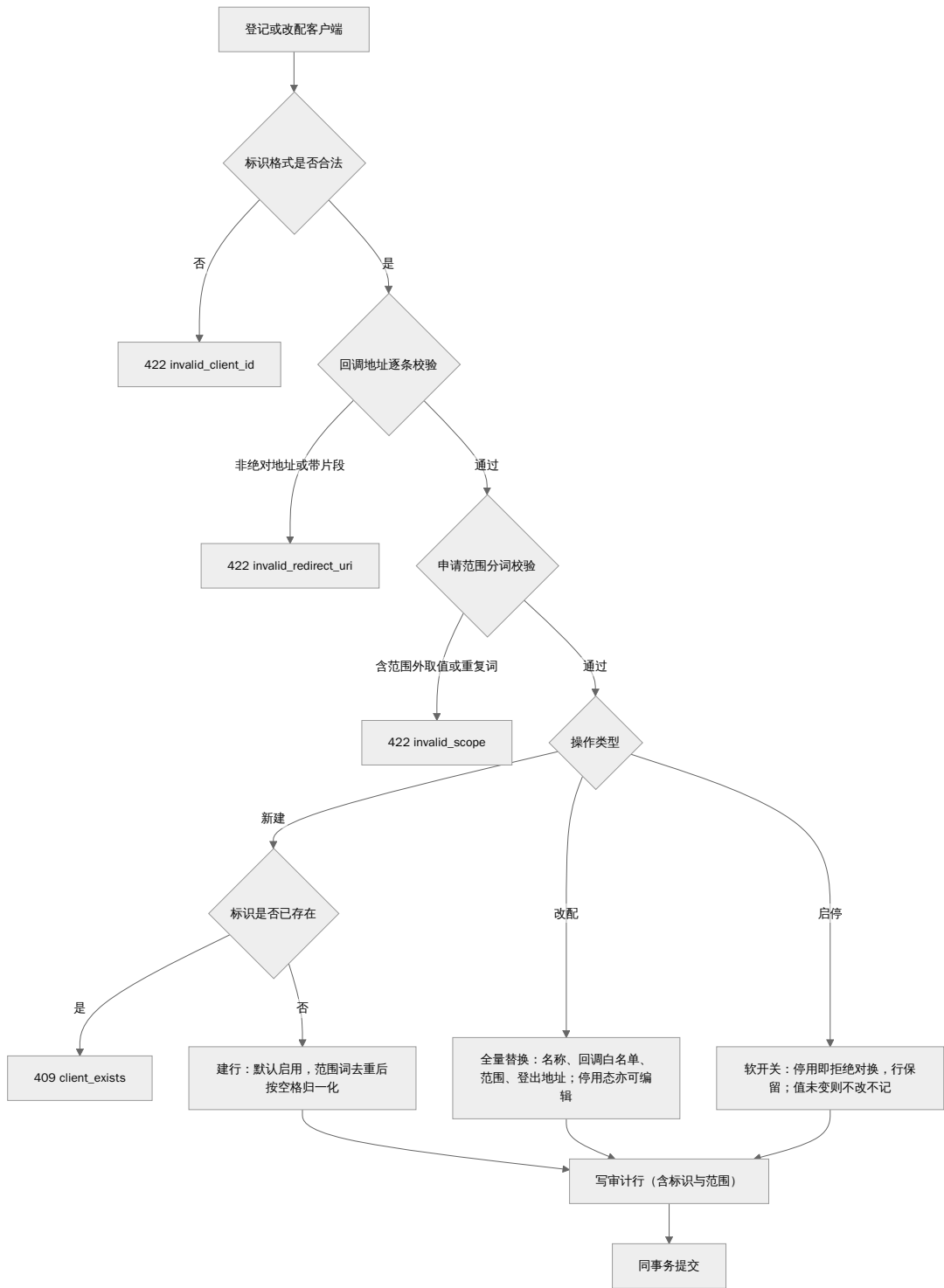


图 8

- 回调白名单：逐条须为绝对地址、主机非空、不带片段；精确匹配在授权侧执行；改配为全量替换，未提交字段视为清空。
- 停用是授权能力回收（授权码兑换与令牌签发按开关拒绝，既有本地会话不受影响）；登记行不含机密字段，响应只出登记事实与存在性。

4.8 运营操作审计的写入与复核路径

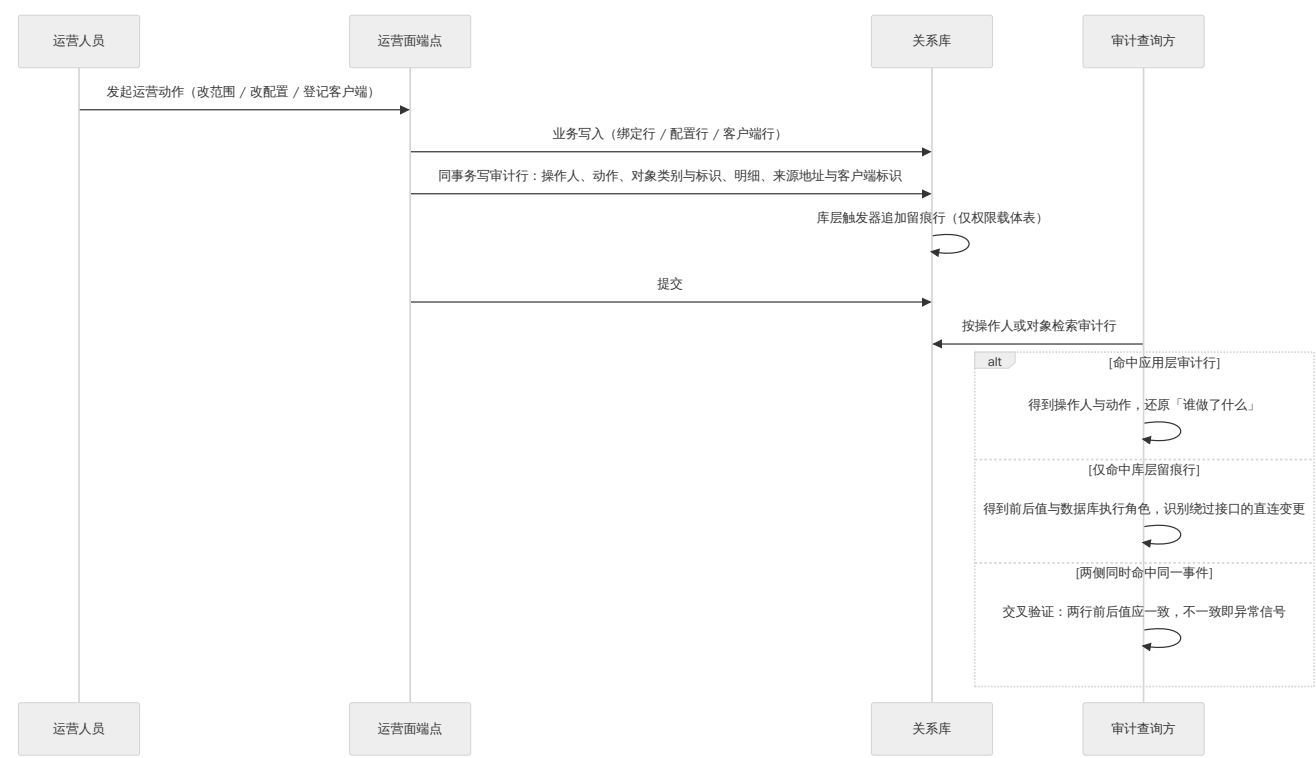


图 9

- 审计四要素：谁、何时、对哪个对象（类别加标识）、做了什么（动作名加明细前后值）；来源地址与客户端标识由接口层显式传入。
- 审计行与业务写入同事务：业务失败不留审计、审计缺位不影响业务提交；复核时用库层行确认权限载体表未被绕过接口改动。

5. 接口契约

5.1 运营员工与本人绑定（门禁：员工管理权限）

方法	路径	语义
GET	<code>/api/account/ops/staff</code>	员工列表：状态筛选、关键词检索、分页
POST	<code>/api/account/ops/staff</code>	授权：按已验证邮箱定位账号建绑定，范围先经目录校验
PATCH	<code>/api/account/ops/staff/{user_id}/scopes</code>	调整权限范围（替换语义、前后留痕；本人不得移除自身管理权限）
PATCH	<code>/api/account/ops/staff/{user_id}/status</code>	停用或恢复（不可作用于本人；停用保留行与范围）

方法	路径	语义
GET	<code>/api/account/ops/staff/me</code>	本人绑定：仅要求有效绑定、不校验范围；回传范围与门户地址

5.2 平台设置（门禁：运营设置权限）

方法	路径	语义
GET	<code>/api/account/ops/settings</code>	设置总览：开关值、可用通道数、两个时长生效值
PUT	<code>/api/account/ops/settings/phone-auth</code>	手机认证开关：开启前置为存在可用通道，关闭无前置
PUT	<code>/api/account/ops/settings/ttl</code>	验证码与邀请有效期：区间校验，与现值相同则跳过不记审计

5.3 单点登录客户端（门禁：员工管理权限）

方法	路径	语义
GET	<code>/api/account/ops/clients</code>	客户端列表：创建时间倒序，不含机密字段
POST	<code>/api/account/ops/clients</code>	新建登记：标识唯一，白名单与范围逐项校验
PATCH	<code>/api/account/ops/clients/{client_id}</code>	改配：全量替换语义，停用态可编辑
PATCH	<code>/api/account/ops/clients/{client_id}/status</code>	启用或停用：软开关不删行；值未变则不改不记

5.4 内部契约（内部令牌的运营 scope）

方法	路径	语义
GET	<code>/internal/platform-staff/{user_id}</code>	员工绑定点查：有绑定回状态与范围，无绑定回未绑定；只回事实不下结论；消费方对非成功响应按未绑定降级

- 与运营面共用同一张绑定行但门禁通道不同：这里认内部令牌的运营 scope，用于登录后判定操作者与调用者角色；运营 scope 与计量 scope 严格互斥（运营 scope 不能用于扣费类内部端点，反向亦然）。

5.5 运营面端点全景索引

按能力所属域分组登记，语义细节写在各域；同一段点不在两篇重复展开。本域自有端点（§5.1~§5.4 共 13 条）不在此重复登记。

客户账务（门禁：客户运营权限）

方法	路径	语义
GET	<code>/api/account/ops/customers</code>	台账（D04）
GET	<code>/api/account/ops/customers/{customer_id}</code>	客户详情（D04）
PATCH	<code>/api/account/ops/customers/{customer_id}/status</code>	经营状态（D04）

方法	路径	语义
PATCH	/api/account/ops/customers/{customer_id}/credit-limit	信用额度 (D04)
PUT	/api/account/ops/customers/{customer_id}/grace	宽限设置 (D04)
POST	/api/account/ops/customers/{customer_id}/adjustment	运营调整与坏账核销 (门禁：额度权限；D04)
GET	/api/account/ops/real-name/verifications	核验台账 (D09)
POST	/api/account/ops/real-name/verifications/{verification_id}/review	人工复核 (D09)

订单与支付 (门禁：额度运营权限)

方法	路径	语义
GET	/api/account/ops/orders	台账 (D03)
GET	/api/account/ops/orders/{order_no}	订单详情 (D03)
POST	/api/account/ops/orders/{order_no}/confirm	手工确认 (D03)
POST	/api/account/ops/orders/{order_no}/query	通道主动查单 (D03)
POST	/api/account/ops/orders/poll	在途订单轮询 (D03)

退款与对账 (门禁：额度运营权限)

方法	路径	语义
POST	/api/account/ops/orders/{order_no}/refund-request	退款申请 (D07)
POST	/api/account/ops/orders/{order_no}/refund-approve	退款通过 (D07)
POST	/api/account/ops/orders/{order_no}/refund-reject	退款驳回 (D07)
POST	/api/account/ops/orders/{order_no}/refund-retry	通道重试 (D07)
POST	/api/account/ops/orders/{order_no}/refund-manual-settle	线下核销 (D07)
POST	/api/account/ops/orders/{order_no}/refund-abandon	放弃结案 (D07)
GET	/api/account/ops/orders/refunds/offline-pending	待确认清单 (D07)
POST	/api/account/ops/orders/{order_no}/refund-offline-confirm	线下确认 (D07)
GET	/api/account/ops/orders/{order_no}/refund-risk	退款风险台账 (D07)

对账台账 (门禁：额度运营权限)

方法	路径	语义
GET	/api/account/ops/reconcile/check	对账校验 (D05)
POST	/api/account/ops/reconcile/scan	对账扫描 (D05)

发票（门禁：发票运营权限）

方法	路径	语义
GET	/api/account/ops/invoices/applications	申请台账 (D08)
POST	/api/account/ops/invoices/applications	代提申请 (D08)
POST	/api/account/ops/invoices/applications/{application_id}/issue	开票 (D08)
POST	/api/account/ops/invoices/applications/{application_id}/reject	驳回 (D08)
POST	/api/account/ops/invoices/applications/{application_id}/void	作废 (D08)

风控（门禁：风控运营权限）

方法	路径	语义
GET	/api/account/ops/risk/rules	规则列表 (D09)
POST	/api/account/ops/risk/rules	新建规则 (D09)
PATCH	/api/account/ops/risk/rules/{rule_id}	更新规则 (D09)
GET	/api/account/ops/risk/events	事件台账 (D09)
POST	/api/account/ops/risk/events/{event_id}/resolve	处置事件 (D09)
POST	/api/account/ops/risk/scan	触发扫描 (D09)
GET	/api/account/ops/risk/keys	密钥视图 (D03)
POST	/api/account/ops/risk/keys/{key_id}/kill	封停 (D03)
POST	/api/account/ops/risk/keys/{key_id}/unblock	解封 (D03)

通道配置与支付通道（仅登记入口）：通知与触达域运营面端点 32 条（前缀 /api/account/ops/channels，覆盖短信与邮件通道登记、改配、启停、优先级、探测、测试发送、模板绑定与发送事件查询，语义见 D10）；订购与支付域 9 条（前缀 /api/account/ops/payments，覆盖状态、通道列表、新建、改配、启用、灰度、停用、探测与删除，语义见 D03）。

6. 关键约束与验收标准

6.1 约束

1. 权限判定唯一实现：各能力域的运营端点共用同一覆盖判定函数，不得另写权限比较。

2. 权限范围不落令牌：每请求点查绑定行，停用与改范围即时生效，无撤销窗口。
3. 值域封闭：只接受权限簿内 10 个值，未知值与空范围一律拒绝；粗粒度覆盖子域。
4. 自锁防护：本人不得移除自身员工管理权限，任何人不得停用本人绑定。
5. 绑定行一人一条：唯一索引保证；停用不删行、不清范围。
6. 设置默认语义二分且即时生效：无记录按默认取值；时长类只影响新签发的行。
7. 开关与通道单调联动：开启要求存在可用通道；通道停用路径同事务自动关开关。
8. 权限载体库层留痕：三动作覆盖、前后整行值入表、操作人置空、执行角色入明细、同事务写入。
9. 两条留痕路径并存：库层行是绕过接口路径的唯一证据。
10. 清空语句必须被拒：语句级守卫加双门槛旁路，生产代码不设置旁路。
11. 审计四要素完整：操作人、动作、对象、明细；来源信息缺失降级并告警。
12. 凭据只写不读、客户端不删除：只启停并逐项校验白名单与范围。
13. 两条鉴权通道互不替代：内部运营 scope 不免去权限范围校验，人员通道不获得内部点查能力。

6.2 验收标准

#	验收口径
1	无绑定行的账号访问任一运营端点返回同一拒绝结果，不泄露绑定状态
2	权限范围含权限簿外取值被拒且不产生绑定行；仅空格与空串视为空
3	授予运营全集即可调用全部子域端点；仅授一个子域时调用其它子域端点被拒
4	员工被停用后下一请求即失去运营端点访问权，无需等令牌过期
5	操作人把自身范围改为不含员工管理权限被拒；停用本人绑定被拒
6	范围或状态与现值相同时返回未变更且审计表不新增行
7	同一账号第二次授权被拒，且在册与停用两种状态给出不同明细
8	已停用账号被提权被拒；不存在邮箱与未验证邮箱返回同一结果
9	应用层与直连改权限范围都留库层留痕行，明细旧值与新值齐全
10	留痕行操作人为空、执行角色为当前库角色、来源标记固定；删除行可从旧值还原整行
11	一条语句改两行绑定落两行留痕；事务回滚后无新增留痕行
12	留痕行事后被同一连接改写或删除被拒
13	清空语句被拒（状态码类 23000）且行数不变；非维护角色开旁路仍被拒
14	无可用通道开启手机认证被拒；通道停用后开关同事务自动置关并留带原因的审计行
15	时长参数越界被拒、库内脏值回落原值而非 0；改小后既有凭证到期时刻不变
16	回调地址或申请范围非法被拒；停用后授权码兑换被拒且行仍在；响应不含机密字段

6.3 待后续设计细化的开放项

1. 引导期提权工具（追加语义、不写审计）与运营面替换语义的收敛路径与截止口径。
2. 绑定行删除是否纳入常规管理能力（现仅停用不删行）；库层留痕行的保留期是否与运营操作审计同寿命。
3. 权限簿扩展形态（新增子域时全集覆盖是否显式白名单化）；客户端回调地址是否按环境分组校验；设置变更是否需旁路通知订阅方。