



DATABLAU · DAM

安全网关

产品模块用户手册

版本 9.1.2

目录

01 安全网关

02 快速开始

03 访问审计与排查

04 兼容性检查

05 配置 Datablau JDBC 客户端

06 配置网关组与服务端网关

07 验证动态脱敏与查询审计

安全网关

安全网关是数据安全（DDS）下的动态脱敏模块。服务端提供网关组、网关、服务端口、运行状态和日志审计；客户端通过 Datablau JDBC Driver 连接网关并访问后端数据。

“动态脱敏”指在符合策略的访问链路上，按访问身份和规则控制查询结果中的敏感值呈现；它不是修改或删除源数据库中的原始值。配置了脱敏规则也不等于客户端已经经过网关，必须通过实际查询结果和审计日志共同核对。

客户端基础

- JDBC URL 形式：jdbc:datablau://[host]:[port]
- Driver Class：com.datablau.jdbc.Driver
- 已有资料覆盖 JDBC 虚拟账号、DAM 用户登录、DBeaver 和 FineBI 接入。

按任务阅读

- [快速开始：验证一次动态脱敏查询](#)
- [配置网关组、端口与登录模式](#)
- [配置 JDBC 工具与 BI 客户端](#)
- [验证访问结果与日志审计](#)
- [审计网关访问并排查问题](#)
- [数据类型与客户端兼容性检查](#)

兼容范围

产品负责人确认当前兼容 Oracle、Hive、MySQL、PostgreSQL、DB2、Vertica 等数据库。历史测试报告直接验证过 MySQL、Oracle 和 Hive；具体数据库与 Driver 的版本组合只记录资料中明确的信息，不推测未给出的版本。

参见[兼容性说明](#)。

安全网关快速开始

目标是让一个测试账号通过 JDBC 网关读取少量样本，并看到预期的动态脱敏结果。

开始前准备

准备项	完成检查
测试数据源与样本	DAM 中可用，目标表字段存在，查询范围已获准
访问身份	确定使用 DAM 用户登录还是虚拟账号；明确本次要验证谁的权限
脱敏预期	明确哪些行可以返回、哪些字段应脱敏、哪些字段应保持原样
网关与驱动	管理员提供可用网关地址、服务端口和 Datablau JDBC 驱动包
数据库客户端	具备添加自定义 JDBC 驱动及测试连接的操作权限

不要用管理员的查询结果代替业务身份验证。也不要为了制造测试结果去修改真实敏感数据；可以选择已有授权样本。

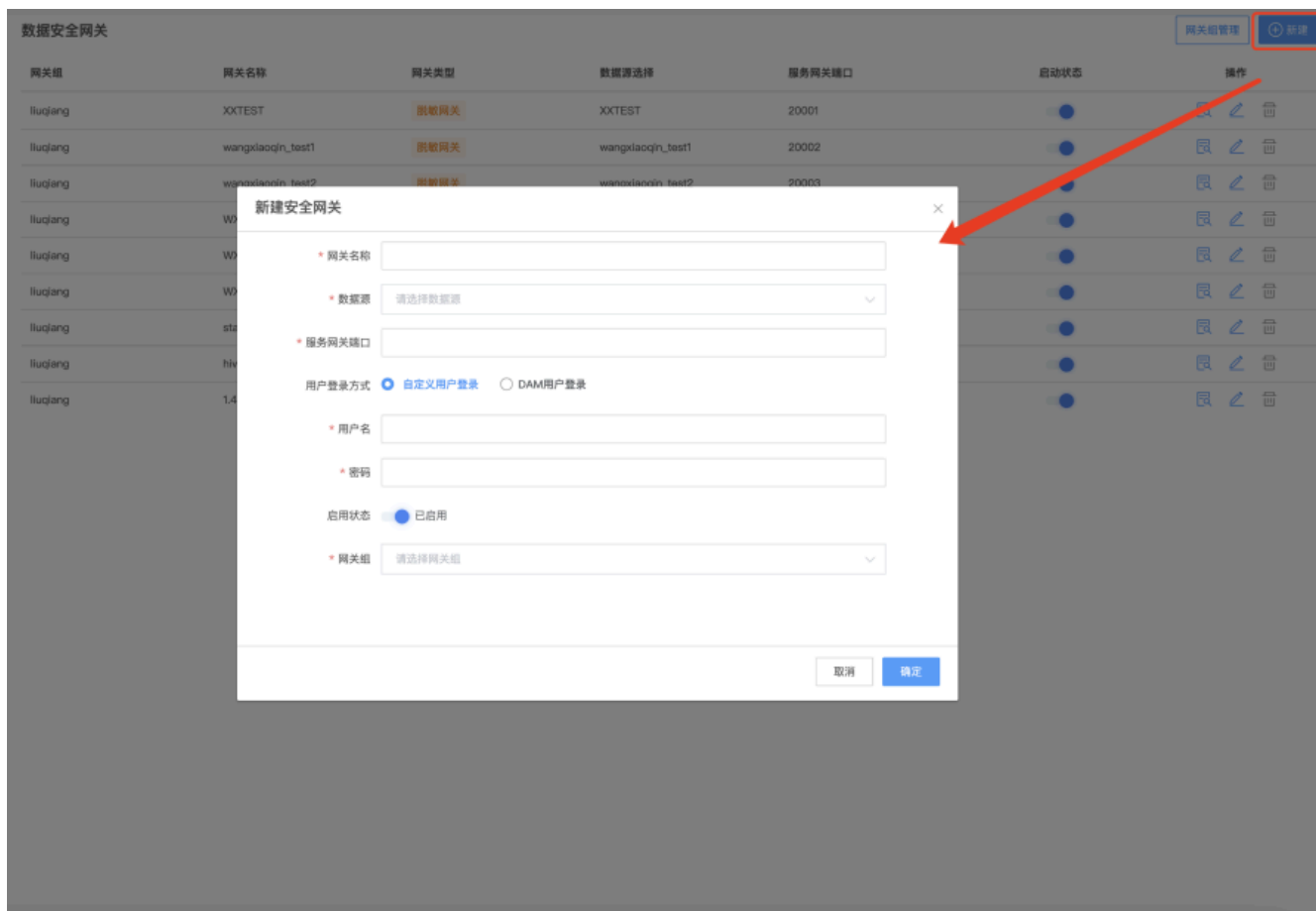
1. 配置访问范围与脱敏方式

按[脱敏规则](#)与[访问策略](#)设置目标账号、对象范围和脱敏方式。记录每个测试字段的预期呈现，后续逐项核对。

完成检查：规则与策略对应同一批表字段和访问身份。只建立脱敏规则，不能作为最终查询已脱敏的证明。

2. 建立服务端网关

按[服务端配置](#)新建网关，选择数据源、端口及登录模式，启用后核对状态。



图示标出新建入口。重点核对数据源、服务端口和用户登录方式，再在客户端填写相应连接参数。单击图片可查看原图。

完成检查：详情中的“服务网关链接信息”与拟使用地址一致，端口属于本次代理的数据源，用户登录方式与凭据来源匹配。

3. 连接 JDBC 客户端

按JDBC 客户端配置驱动。以 DBeaver 为例，先在“数据库 → 驱动管理器”添加驱动包与类 `com.datablau.jdbc.Driver`，再新建连接。

连接 URL 使用 `jdbc:datablau:///[host]:[port]`，将方括号部分替换为网关详情中的实际值。使用与所选登录模式匹配的账号，执行连接测试。

完成检查：测试成功后能查看预期数据库对象。若连接失败，先排查网络、服务、驱动和认证，不直接修改脱敏规则。

4. 查询样本并核对审计

1. 选择已配置策略的目标表与字段，执行范围明确的查询。

2. 将返回行、脱敏字段及非目标字段与准备阶段的预期逐项比较。
3. 记录本次使用的网关、访问身份、查询时间和结果。
4. 进入“日志审计”查找同一次查询，核对 SQL 详情。
5. 按[验证指南](#)补充其他获准访问身份及限制场景。

完成检查：结果符合预期且能够与审计记录对应。动态脱敏改变的是访问时的呈现，不表示源数据库数据已被改写。

完成标志与下一步

连接成功、策略保存成功、脱敏结果正确是不同检查点。全部通过后再逐步扩大对象及用户范围。需要将 BI 用户身份传递到网关时，继续阅读 [FineBI 接入准备](#)，另行验证用户映射与默认权限。

访问审计与排查

安全网关服务端的日志审计用于确认连接、认证、SQL 请求和结果处理；它与 DDS 平台的安全操作日志不是同一份记录。

核对一条访问记录

- 1. 记录测试账号、客户端、网关地址、目标库表和查询时间。
- 2. 在网关管理页按时间、网关、用户和结果状态筛选日志。
- 3. 检查请求是否经过 Datablau JDBC Driver、命中的策略和返回状态。
- 4. 对比客户端看到的原值/脱敏值，确认策略作用于正确字段。
- 5. 将日志导出或截图时脱敏账号、地址和数据内容。

常见失败路径

现象	先检查	进一步处理
无法连接	网关状态、端口、防火墙和 JDBC URL	用最小查询验证网络与认证
认证失败	身份模式、DAM 用户或虚拟账号	重新确认账号是否被禁用、权限是否过期
返回原值	策略对象、字段映射、优先级和生效时间	使用明确敏感字段做单字段测试
查询失败但网关正常	后端数据库账号、驱动参数和 SQL 方言	直接用后端账号验证数据库连接
日志没有记录	请求是否实际经过网关、筛选时间和代理账号	与客户端连接日志按时间对照

不要通过重复执行查询来“测试”脱敏效果；优先使用专用测试数据和最小权限账号。

留存审计证据

一条可复核的验证记录至少包含：测试目标、访问身份、网关与后端对象、策略名称、执行时间、客户端结果、服务端日志编号和结论。性能测试报告不能替代单条策略的功能验证。

兼容性检查

安全网关的兼容性由后端数据库、Datablau JDBC Driver、客户端工具和具体 SQL 方言共同决定。已确认的数据库类型包括 Oracle、Hive、MySQL、PostgreSQL、DB2、Vertica 等；没有明确给出的版本号不在手册中推定。

建立客户验证矩阵

维度	客户应记录
后端数据库	类型、部署方式、字符集和连接方式
JDBC Driver	Driver 类名、JAR 来源、连接参数
客户端	数据库工具或 BI 产品、运行方式
SQL 场景	查询、分页、聚合、函数、事务和大字段
安全策略	字段脱敏、表脱敏、行级过滤及例外账号
结果	连接、认证、查询、脱敏、审计是否通过

验证顺序

1. 用最小权限账号通过 JDBC Driver 建立连接。
2. 查询非敏感测试表，确认方言和字符集正常。
3. 在单字段上配置脱敏策略，验证原值与返回值。
4. 增加分页、聚合和大结果集场景，观察客户端行为。
5. 检查网关审计与后端数据库日志是否能关联。

具体版本组合、性能阈值和生产上线结论必须来自客户测试报告或产品确认，不能从数据库类型列表推导。

配置 Datablau JDBC 客户端

客户端通过 Datablau JDBC Driver 连接安全网关，再由网关访问后端数据源。直连数据库不会自动经过此网关的访问策略。

连接参数

参数	设置
JDBC URL	<code>jdbc:datablau://[host]:[port]</code>
Driver Class	<code>com.datablau.jdbc.Driver</code>
host	实际网关部署地址
port	该代理数据源在网关中配置的服务端口
用户名、密码	按网关的 DAM 登录或虚拟账号模式提供

方括号表示需要替换的值，不应原样填入连接。使用管理员提供的驱动包，不将其他数据库原生驱动类名填成 Datablau 驱动类。

接入数据库工具

1. 在 DBeaver 选择“数据库 → 驱动管理器”，新建自定义驱动定义。
2. 添加 Datablau JDBC 驱动包，填写驱动类。
3. 选择“数据库 → 新建数据库连接”，使用该驱动，设置网关 URL 和相应凭据。
4. 测试连接，成功后查看目标数据库对象。
5. 选择已知样本查询，按[结果验证](#)检查可见范围与脱敏效果。

如果工具使用驱动模板自动补充 URL，最终仍应核对实际生成的地址和端口。

连接参数应与 DAM 网关详情的“服务网关链接信息”和所选登录模式相符。连接后展开数据库、Schema、表和字段，选择已明确配置策略的字段测试；先确认正确连接，再检查脱敏，便于区分驱动问题与权限问题。

FineBI 接入准备

FineBI 接入除 JDBC 连接外，还涉及用户身份传递。由管理员按适配安装包部署 `datablau-driver-jdbc-bridge.jar`、配套线程上下文代理及 Datablau JDBC 插件，在实际启动配置中加入配套代理参数后启动服务，再建立 Datablau JDBC 数据源。

原集成方案通过桥接与线程上下文把当前 BI 用户传递到 JDBC。BI 登录名与 DAM 用户名一致时使用该 DAM 用户策略，两边密码可以不同；不一致时使用默认权限。因此必须检查实际登录用户对应的效果，不能只测试管理员连接成功。

安装目录、启动脚本和配套包应与部署方案一致，不复制其他环境的绝对路径。升级或调整插件后需要重新验证身份传递、连接和查询结果。

常见问题

现象	检查内容
找不到驱动类	驱动包是否加载、类名是否正确
连接被拒绝	网关启用状态、服务地址、端口和网络
认证失败	网关登录模式与凭据是否对应
看到的数据与预期权限不符	实际连接是否经过网关、实际访问身份和策略范围
BI 用户结果相同	检查用户身份是否传递、用户名映射及默认权限

配置网关组与服务端网关

安全网关代理后端数据源，为客户端提供受策略控制的 JDBC 访问。开始前应准备可用数据源、部署地址、可用服务端口以及访问和脱敏策略。

建立网关组

进入“数据安全 → 安全网关”，打开“网关组管理”，添加名称和编码。已有组可编辑或删除，调整前核对归属网关。

网关组编码须与已部署 JDBC 网关服务配置一致。只在页面增加一个组不会自动部署或启动服务；先由运维确认服务已启动并使用相同的组配置。

新建网关

1. 单击“新建安全网关”。
2. 填写网关名称，选择数据源和网关组。
3. 配置服务网关端口；客户端连接此端口，不是后端数据库原始端口。
4. 选择用户登录方式，按模式配置账号信息。
5. 设置启用状态并确定。
6. 在列表或查看页面检查配置与运行状态，再从客户端测试连接。

查看详情中的“服务网关链接信息”，将实际连接信息交给客户端使用。存在多个服务地址时，逐个验证可达性及策略效果。编辑表单中的端口配置与详情展示的连接信息用途不同，不要求详情页仍单独显示“服务网关端口”或“网关类型”。

具有安全网关管理权限的用户可通过“下载 datablau-jdbc.jar”取得驱动。客户端替换驱动后重新测试连接，不以下载成功作为接入成功的判据。

两种身份方式

方式	使用凭据	策略身份
DAM 用户登录	DAM 用户名及密码	使用该 DAM 用户的权限策略
自定义用户登录（JDBC 虚拟账号）	网关中设置的自定义账号及密码	手工用户名与 DAM 用户名一致时，使用该用户策略；密码为网关设置值，不是 DAM 用户密码

虚拟账号常用于应用程序，DAM 登录常用于人员操作数据库工具。选择方式应与客户端用途一致，不能在两种模式间混用密码。

调整与停用

使用“编辑”维护数据源、端口、登录方式等配置，保存后重新验证客户端。启用中的网关不能删除，需要先从管理员确认影响并停用。

下一步：[配置 JDBC 客户端](#)。

验证动态脱敏与查询审计

网关验证需要同时检查连接身份、查询结果与审计记录。使用经过授权的样本及测试账号，分别验证应允许和应限制的情况。

准备验证用例

明确目标数据库、网关、表字段、测试用户及预期结果。至少包含以下适用情况：

场景	预期检查
允许访问	能读取获准范围
限制访问	范围外对象不能按普通允许路径读取
行级控制	返回记录符合配置条件
字段脱敏	指定字段按规则呈现
非目标字段	没有被错误套用其他字段规则
不同用户	结果符合各自访问身份和策略

不要为验证方便直接使用管理员账号代替所有业务角色。

执行并核对

- 按JDBC 配置连接目标网关。
- 确认登录模式和用户名，执行范围明确的查询。
- 将实际行、字段及值的呈现与预期比较。
- 更换需验证的访问身份，重复对应场景。
- 进入“日志审计”搜索本次查询，核对经网关执行的 SQL 详情。
- 记录成功与失败用例、错误信息和实际结果。

动态脱敏控制访问时的呈现，不应把显示变化当作源数据库数据已被改写。

区分日志

网关日志审计记录经网关查询的 SQL；安全操作日志追溯用户在安全模块的管理动作。查询没有出现在审计中时先核对是否直连了后端、是否选错网关，以及查询时间范围。

兼容性检查

已确认的数据库范围包括 Oracle、Hive、MySQL、PostgreSQL、DB2、Vertica。实际接入还需核对数据库、JDBC 客户端、驱动和网关的组合，并执行本页用例。历史测试通过不等于任意 SQL 或并发规模都已验证，不据此承诺固定性能。