



DATABLAU · DAM

数据安全

产品模块用户手册

版本 9.1.2

目录

01	数据安全
02	快速开始
03	配置访问、行级过滤与脱敏策略
04	管理识别算法与算法库
05	建立安全分类、分级与信息项
06	在分类分级工作台处理结果
07	协同梳理并评审分类分级结果
08	维护法规条文与安全判定依据
09	维护脱敏规则与安全运行配置
10	管理策略目录与安全操作日志
11	配置识别算法、规则 and 任务

数据安全

数据安全属于数据安全（DDS），覆盖安全分类分级、识别算法与任务、结果评审与发布、访问策略、授权和脱敏规则等治理活动。

本模块帮助回答三类问题：哪些数据属于哪种安全类别和级别、分类结论由谁确认、哪些访问者可以看到哪些数据及呈现形式。分类、评审和访问控制是相互关联但需要分别完成的工作。

理解主要对象

对象	用途	与后续操作的关系
安全分类	按业务含义组织待治理的数据	先设计层级，再建立分类节点并挂载对象
分类信息项	作为分类与识别的载体	可供识别规则使用，不等同于某个具体数据库字段
安全等级与判定依据	记录安全要求及其依据	分类相同的对象仍可能需要不同等级
识别算法、规则 and 任务	批量获得候选分类分级结果	运行后仍需核对结果并完成评审
访问策略	指定访问者、可访问范围及控制方式	区分直接访问、行级控制、表脱敏和字段脱敏
脱敏规则	定义敏感值的呈现方式	由策略引用，并通过实际访问链路验证

开始使用的准备

先确认目标数据已进入元数据管理，业务人员能够说明其含义，安全责任人已明确分类、级别和判定依据。需要通过网关验证访问效果时，还应准备实际访问身份及授权样本。

建议由业务责任人解释数据含义，安全治理人员维护分类与策略，评审人员确认分类结论，平台或网关管理员配置执行链路。这是职责分工建议，不是要求系统必须存在这些固定角色名称。菜单与操作权限由组织实际配置。

首次建设从[快速开始](#)选择少量表字段完成手工梳理和评审，再扩展到批量识别，便于先确认分类口径。

与安全网关的边界

本模块管理安全治理规则和结果。[安全网关](#)是 DDS 下用于动态脱敏的独立模块，包含服务端配置、JDBC Driver 客户端和日志审计。

按任务阅读

目标	指南
完成一组数据的安全治理	快速开始
建立分类框架、信息项、级别和依据	分类分级设计
维护法规和分类判定依据	法规条文与判定依据
人工梳理并评审结果	协同分类分级 与 分类分级工作台
使用算法批量识别	算法、规则与任务
维护算法库和识别能力	识别算法管理
限定访问者、记录范围和敏感呈现	访问策略
管理策略目录和操作证据	策略目录与安全日志
维护规则、同步配置和统计	脱敏与运行配置

阅读安全概览

安全概览主要统计已发布分类分级结果。这里的“已发布”指数据资产与安全分类、级别的挂载关系已经评审通过，不是资产目录模块中的目录发布，也不是访问策略已经验证通过。

图表	统计范围与阅读方法
数据资产分级概览	各安全等级中已发布数据资产的占比；待确认结果不能当作已经完成
数据资产分类分级概览	按一级安全分类，分别查看其中各等级的资产数量
数据资产分级情况：业务系统	按已发布资产所属业务系统统计各等级数量
数据资产分级情况：业务部门	按表或字段所在业务系统的业务部门属性统计；不是操作人所属部门

统计数量不符合预期时，先对齐对象范围、分类层级和评审状态，再检查业务系统的部门属性。分类覆盖率用于发现治理范围缺口，不能代替实际用户查询的权限和脱敏结果验证。

数据安全快速开始

以少量已采集表和字段完成分类分级，再验证一个明确的访问或脱敏要求。先由安全与业务责任人确认分类体系、级别和依据。

开始前准备

准备项	如何检查
少量已采集表和字段	在元数据中能够定位，来源、表名和字段含义准确
分类与分级依据	业务与安全责任人能解释选择某一类别、级别的原因
梳理及评审人员	具备对应页面的操作权限，明确由谁核对和通过结果
访问验证身份	若本次还验证访问控制，明确测试用户及其应见数据范围

本指南先完成分类分级，再按需要进入访问控制。若已有经确认的分类框架，可直接从梳理步骤开始，不必创建重复框架。

1. 建立安全分类框架

进入“系统设置 → 数据分类设计”，按[分类设计](#)确定层级名称和支持的资产类型，再在“数据分类分级 → 数据分类”建立实际节点。在“数据分级”维护所需等级和判定依据；需要法规文件支持时，在“法规条文”维护关联资料。部分界面将前两个入口显示为“安全分类设计”和“安全分类”。

层级管理

层级

一层

两层

三层

四层

五层

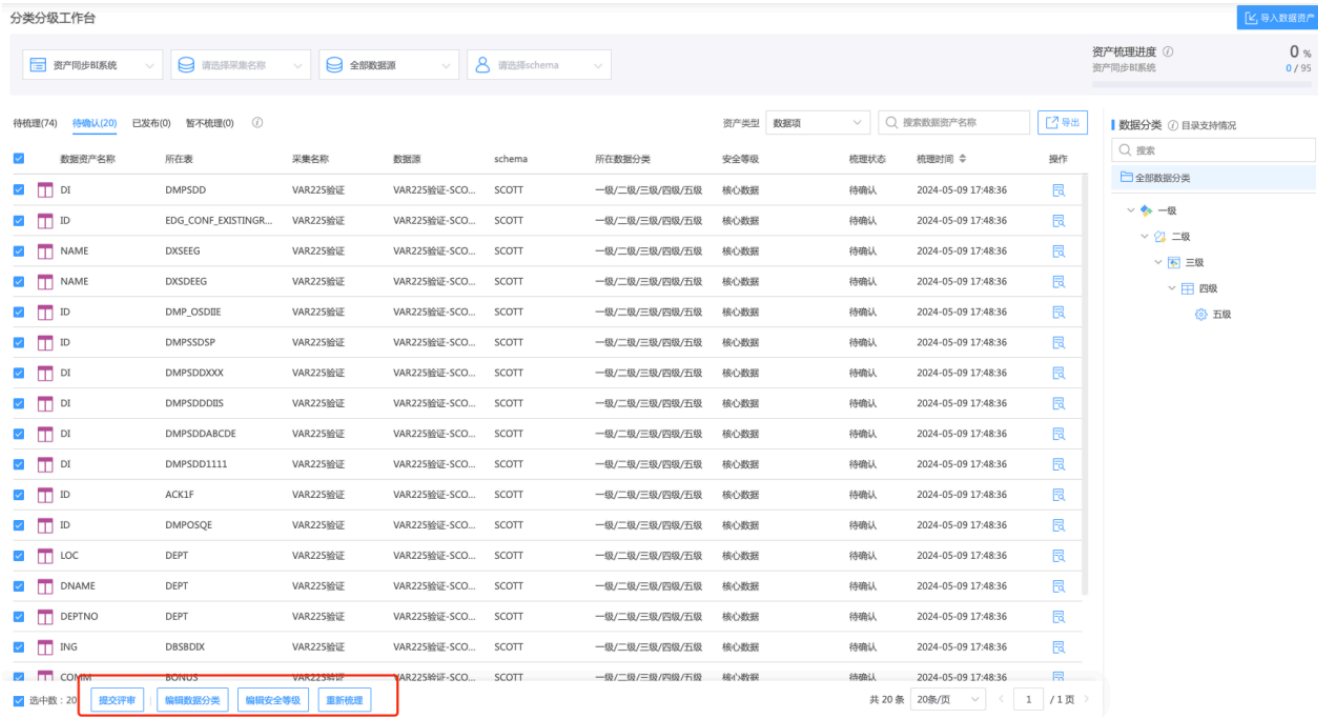
资产目录		支持数据资产类型	相关配置	图标
安全一级分类	①	目录	扩展属性	
安全二级分类	①	目录	扩展属性	
安全三级分类	①	目录	扩展属性	
安全四级分类	①	目录, 数据项, 数据表, 视图	扩展属性	
安全五级分类	①	数据项, 数据表	扩展属性	

图示用于识别层级、名称和支持类型的位置，不要求采用图中的层数。

完成检查：目标层级允许挂载本次要梳理的对象，实际分类节点及等级已准备好。已有节点后不能随意减少层级或支持类型，因此应先确认范围。

2. 梳理少量表字段

1. 进入“分类分级工具 → 协同分类分级”，在“待梳理”找到目标对象。
2. 核对来源和业务含义，选择右侧安全分类并确认加入。
3. 切换到“待确认”，检查分类和安全等级。
4. 错误项使用“编辑安全分类”或“编辑安全等级”修正；需要重做的对象使用“重新梳理”。



图中底部操作针对已选对象。先检查选择范围，再提交评审；不要因某个分类整体正确而忽略其中个别字段的等级差异。

完成检查：所有参与本次试点的对象都有可解释的分类及等级，暂不处理的对象已与本次范围区分。详细操作见[协同分类分级](#)。

3. 评审并检查发布结果

1. 对待确认结果执行“提交评审”。
2. 由具备权限的评审人员进入“分类分级工具 → 评审与发布”。
3. 核对对象、分类、级别及依据，通过正确项；错误项驳回后重新梳理。
4. 检查成功和失败数量，确认目标对象已发布。
5. 回到对象及[安全概览](#)，对照分类、等级及统计范围。

完成检查：发布的是目标对象的正确关系，未通过或部分失败的项仍有处理记录。提交评审成功不能替代评审通过。

4. 按需验证访问与脱敏

明确一个用户应看到的数据范围，按[访问策略](#)选择访问、行级控制或脱敏方式。需要动态脱敏时按[网关快速开始](#)完成服务端和 JDBC 客户端配置，以实际使用账号查询样本并核对日志。

完成检查：分类分级经过评审，访问链路也呈现符合策略的结果。两项分别验证，不能用分类覆盖率代替访问控制验证。

扩大治理范围

小范围结果正确后，按[算法](#)、[规则与任务](#)配置智能识别。先使用已知正反样本测试条件，再运行任务、检查候选结果及评审发布。智能识别的推荐分数不是最终安全结论。

第一次接触算法测试时，可先完成[虚构代码正则测试](#)，认识匹配与未匹配结果。该体验不保存算法，也不更改资产分类，之后再按实际业务要求准备识别规则。

配置访问、行级过滤与脱敏策略

访问策略定义哪些访问者能够访问哪些数据，以及访问时如何过滤或脱敏。它针对数据值的访问控制，与手册门户权限、资产目录浏览权限不同。

选择策略类型

类型	用途
访问策略	允许或限制访问指定数据范围
行级访问策略	在可访问表中限定记录范围
表脱敏策略	从表或视图出发，为字段设置脱敏规则及访问者
字段脱敏策略	从字段出发，为不同访问者配置脱敏规则

先准备策略目录，填写名称和描述；目录内有策略时不能直接按空目录处理删除。

使用前准备

确定本次控制的数据对象、需要约束的访问者及其业务用途。行级限制需要明确字段与取值，脱敏需要先准备可用的[脱敏规则](#)。账号、用户组和机构来自[组织管理](#)，策略所需对象来自已采集元数据。

实施时先在已获准的小范围内验证，再扩大到完整对象或人员范围。尤其要区分“拒绝某些对象”和“允许排除某些对象后的剩余范围”，两者不能互相替代。

创建访问策略

1. 进入数据安全的“安全策略 → 访问策略”，选择“新建 → 访问策略”。
2. 填写策略名称、描述及目录，按业务要求设置访问有效期。
3. 在访问数据配置中选择执行动作、访问动作和数据范围。
4. 核对范围模式：“包含”仅限所选对象，“不包含”为排除所选对象后的范围，“全部”为相应来源下全部对象。
5. 在访问者配置中选择用户、用户组或机构，按需要设置黑名单以剔除白名单中的部分用户。
6. 确定后查看最终生效范围，并以目标访问者验证。

执行动作与数据范围应共同核对，不能只检查策略名称。

① 基本信息

② 访问数据配置

访

* 数据执行动作

SELECT

* 数据访问动作

☒ SELECT

☐ INSERT

☐ UPDATE

☐ DELETE

* 采集名称

▼ 数据源

☒ 全部

☐ 包含

☐ 不包含

暂无数据

图为实际表单中的访问数据配置，尚未选定采集范围，不能直接作为已生效策略。

设置	如何填写与检查
策略名称、目录	为必填项；名称用于识别用途，目录用于组织策略
访问有效期	页面说明仅允许访问策略可设置，到期后自动收回；清空表示永久。按审批的授权期限填写，不直接沿用空值
数据执行动作	当前表单提供 SELECT、INSERT、UPDATE、DELETE，按获准操作选择；不要把查询权限扩大为写入权限
数据访问动作	选择“允许”或“拒绝”，与执行动作和对象范围一起核对
采集名称	先选正确采集，再核对下方数据源、表/视图和字段范围
范围模式	各层级分别检查“全部”“包含”“不包含”，不把默认“全部”当作已确认范围
访问者	按用户、用户组或组织机构配置；设置黑名单时核对从白名单剔除后的实际人员

访问有效期是此访问策略的设置，不是数据市场申请单自动完成交付或回收线下权限的证明。到期行为还需由管理员在实际访问链路验证。

创建行级访问策略

1. 选择“新建 → 行级访问策略”，填写基本信息。
2. 添加表或视图，再添加访问者。
3. 在该访问者的行级数据中单击“添加”。
4. 填写条件组，检查系统拼接出的 SQL 条件。
5. 确定后用该访问者查询已知样本，检查应可见与应不可见记录。

行级数据 | 数据表: pty_conp

新增条件组 | 数据行数限制 100

det_addr_desc(详细地 = 北京

取消 添加

在条件弹窗中通过字段、比较关系和比较值定义条件。页面提供相应控件时，可新增条件组或增删单条条件。图中字段、地点和“数据行数限制”的数值均为示例，不是默认值。

在弹窗单击“添加”后，先检查访问者列表中显示的 SQL 条件，再完成整个策略。一个访问者的条件不能自动代表其他用户、用户组或机构的条件；多个条件存在时，要检查组合逻辑是否与业务要求一致。

创建表脱敏策略

- 1. 选择“新建 → 表脱敏策略”，填写基本信息。
- 2. 添加表或视图，检查展开的字段列表。
- 3. 对需脱敏字段添加脱敏规则。
- 4. 进入访问者配置，选择规则适用的用户、用户组或机构。
- 5. 确定后检查目标字段及未选择字段的结果。

创建字段脱敏策略

- 1. 选择“新建 → 字段脱敏策略”，填写基本信息。
- 2. 添加字段及访问者。
- 3. 在各访问者对应行中添加脱敏规则。
- 4. 确定后核对同一字段在不同用户下的处理结果。

验证与维护

策略列表可按名称搜索，通过查看检查最终范围和脱敏内容，编辑时逐步核对回显设置。策略生效还需实际访问链路配合，按[网关验证](#)使用对应账号检查；仅在管理页保存不代表客户端已正确接入。

存在多条重叠策略时，应使用目标账号及实际查询验证最终效果，不自行假设统一的优先级顺序。删除或调整前记录原范围与受影响访问者。

现象	核对顺序
策略已保存但查询仍未受限	实际是否经过网关 → 使用的身份 → 目标对象是否在策略范围 → 执行动作和允许/拒绝
某用户的结果与同组人员不同	用户、用户组和机构范围 → 黑名单 → 其他重叠策略
行级结果全部为空	条件字段、比较值和组合逻辑 → 源数据是否有符合条件记录 → 查询范围
只对部分字段脱敏	策略类型 → 选定字段 → 对应脱敏规则 → 当前访问者
到期后行为不符合预期	是否为允许策略 → 有效期实际值 → 访问链路 with 策略处理日志

管理识别算法与算法库

智能分类分级由算法、识别规则和识别任务组成。算法只负责提供候选识别能力，不能代替安全责任人确认和发布结果。

算法类型

类型	适用方式	管理重点
算法库	自定义文本、字段或模式识别	维护算法目录、表达式、测试样本和说明
血缘级联算法	根据已确认对象沿血缘传播候选分类	先确认血缘质量和传播范围
机器学习算法	根据训练或内置模型给出候选结果	核对模型适用范围和人工复核比例

血缘级联和机器学习能力是否在当前租户可见，取决于部署和许可。页面没有显示时先检查 License 与功能权限。

新建算法库条目

1. 进入“数据安全 → 识别算法 → 算法库”。
2. 先在目录树中建立用途清晰的算法目录。
3. 选择“新建算法”，填写名称、编码、描述、适用字段或数据类型。
4. 配置识别表达式或算法参数，使用测试样本验证命中和未命中结果。
5. 保存后检查状态、目录归属和可被识别规则选择的范围。

测试样本只用于验证算法逻辑，不应包含真实敏感值。正则等表达式应同时测试空值、边界值、中文字符和异常格式。

导入、导出和维护

导入前使用系统提供的模板，保持编码唯一、目录存在、参数格式正确。导入完成后检查失败行并修正，不要因为任务创建成功就认为每条算法都已生效。导出文件用于评审和备份，不能代替版本记录。

被识别规则引用的算法不建议直接删除。需要停用时先停用规则或建立替代算法，再观察识别任务结果。

发布前检查

- 算法名称、编码与业务含义一致。
- 测试样本覆盖正常、异常和空值场景。
- 识别结果中能说明命中依据和建议的分类等级。
- 识别规则引用的是预期算法目录。
- 任务执行范围和负责人已明确。

下一步：[配置识别规则与任务](#)。

建立安全分类、分级与信息项

分类描述数据属于什么业务范围，分级描述其安全等级。“分类信息项”是可复用的安全语义条目，用来描述一类待识别信息并关联分类，不是某张表里的实际字段；识别或人工梳理后，才把具体对象与分类、级别关联。先建立适用制度和分类框架，再对实际对象梳理。

设计分类层级

- 1. 进入“数据安全 → 系统设置 → 数据分类设计”。部分界面使用“安全分类设计”名称。
- 2. 选择层级数，填写各层名称及支持的资产类型；支持数据项时同时支持信息项。
- 3. 配置扩展属性和图标，保存设计。
- 4. 在“数据分类分级 → 数据分类”中建立实际目录节点。

已有分类节点后，层级只能增加，不能减少；支持的资产类型也只能增加。修改扩展属性的类型会清空已有值，将选填改为必填后需要补齐分类属性，调整前检查影响。

复用资产目录结构

如业务确定安全分类与资产目录共用结构，可选择已启用的资产目录空间，设置立即同步或实时同步并保存。

同步一次只选择一个空间，其层级不少于安全分类层级。安全分类已经挂载资产或信息项时，不允许同步目录空间。开启同步后不能再独立编辑层级设计。

同步主要带入目录名称和描述，不自动复制全部业务属性；安全等级、重要程度等需设置默认值或在分类中补充。同步后的可挂载资产类型还应核对，不假定与源目录完全相同。

资产目录原支持范围	同步后的安全分类支持范围
仅目录	目录
目录与数据表	目录与数据表
目录与数据项	目录与数据项
目录与标准、数据服务、指标、文件或报表	按安全分类的表、数据项、视图范围处理，不复制这些业务对象类型

源目录切换目录类型后，后续同步会跟随新的类型。执行前先核对层级和允许挂载的对象，避免只检查名称相同。

维护分类信息项

1. 进入“分类信息项”，先建立目录并填写名称、描述。
2. 单击“新建”，填写信息项属性并保存。
3. 需要自定义字段时在“更多 → 扩展属性”维护，再填写具体值。
4. 批量录入在“更多 → 导入”下载模板；选择自动编码或在模板填写编码后上传。
5. 在任务进度中核对成功、失败及原因，按名称或编码查找结果。

已挂载安全分类的信息项不能删除；目录含信息项时也不能删除。导出未勾选对象时为全量，勾选时仅导出选中范围。

维护安全分类

进入“数据分类分级 → 数据分类”维护安全分类节点，按页面新建入口填写属性。部分界面使用“新建安全分类”名称。选中节点可编辑、添加信息项、按模板导入及导出。分类下有信息项、已挂载资产或相关数据正在审批时不能删除。

分类结构导出与分类下资产导出范围不同：后者包含当前分类及其子分类的数据资产，应在操作前核对范围。

定义级别与依据

在“数据分级”维护安全等级、数据重要程度参考和安全判定依据。内置属性值允许按组织制度编辑；已被分类引用的等级不能删除。

在“法规条文”上传依据文件并填写属性，使用下载查看原文。已被分类引用的条文不能删除。条文应与当前治理范围相关，上传文件本身不代表已完成合规判断。

下一步：[协同分类分级](#)或[智能识别](#)。

在分类分级工作台处理结果

分类分级工作台把资产处理分为待梳理、待确认、评审中、已发布和暂不梳理等状态。状态表示治理动作是否完成，不表示数据库中的数据已经被修改。

手工协同分类分级

1. 进入“数据安全 → 分类分级工具 → 协同分类分级”。
2. 在“待梳理”中按系统、目录、资产类型和名称筛选对象。
3. 选择一个或多个资产，再选择安全分类和安全等级，检查对象数量后提交。
4. 对暂不纳入范围的对象选择“暂不梳理”，填写原因并保留后续复核依据。
5. 在“待确认”中检查分类、等级、依据和责任人，必要时编辑后提交评审。

同一安全分类下的资产可以有不同安全等级。批量操作前务必复核选择数量，避免把不同业务含义的对象归为同一等级。

评审与发布

评审人进入“待评审”列表，按资产详情、分类层级、等级依据和识别来源逐条抽查。评审通过后对象进入“已发布”，评审驳回后返回待确认并填写驳回原因。发布结论只代表分类分级结果生效，不代表访问策略或动态脱敏已验证。

已发布对象需要重新梳理时，先确认现有访问策略和数据市场展示是否会受影响，再执行“重新梳理”。

导入和导出

1. 在工作台下载导入模板，保持列名、编码和状态字段不变。
2. 选择“资产审核”时，导入对象进入待确认；选择“直接发布”时，需确认组织允许绕过人工评审。
3. 导入后查看错误行，修正对象标识、分类编码和等级编码后再导入。
4. 导出时未选择对象表示导出当前状态的全部数据，已选择对象则只导出选择项。

导入和导出文件可能包含资产名称、字段和安全等级，只能通过批准的存储和传输渠道处理。

状态排查

现象	检查
对象不在待梳理	元数据是否采集、当前筛选条件和用户目录权限
提交评审失败	是否填写分类、等级、依据及必填责任人
评审后仍不可见	发布状态、资产目录权限和 License
重新梳理按钮不可用	当前状态、本人角色及是否存在进行中的评审

协同梳理并评审分类分级结果

协同分类分级适用于需要人员逐项判断的数据表、视图和数据项。准备好分类、级别与判定依据，并明确梳理和评审职责。

从待梳理到待确认

- 1. 进入“分类分级工具 → 协同分类分级”。
- 2. 在“待梳理”选择对象，核对来源和业务含义。
- 3. 选择右侧安全分类，确认把所选数据加入分类。
- 4. 在“待确认”核对分类及安全等级。
- 5. 需要修改时使用“编辑安全分类”“编辑安全等级”；同一分类中的资产允许具有不同安全等级。
- 6. 核对后“提交评审”。

分类分级工作台

资产同步和系统

请选择采集名称

全部数据源

请选择schema

资产梳理进度 0 %
资产同步和系统 0 / 95

导入数据资产

待梳理(74) 待确认(20) 已发布(0) 暂不梳理(0)

资产类型 数据项 搜索数据资产名称 导出

数据资产名称	所在表	采集名称	数据源	schema	所在数据分类	安全等级	梳理状态	梳理时间	操作
DI	DMPSTD	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
ID	EDG_CONF_EXISTING...	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
NAME	DKSEEG	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
NAME	DKSDEG	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
ID	DMP_OSDIE	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
ID	DMPSSDSP	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
DI	DMPSTDXXX	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
DI	DMPSTDDBS	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
DI	DMPSTDABCD	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
DI	DMPSTD1111	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
ID	ACKIF	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
ID	DIMPOSQE	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
LOC	DEPT	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
DNAME	DEPT	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
DEPTNO	DEPT	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
ING	DMSBDD	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良
COMB	BONUS	VAR225验证	VAR225验证-SCO...	SCOTT	一级/二级/三级/四级/五级	核心数据	待确认	2024-05-09 17:48:36	良

选中数: 20

提交评审 编辑数据分类 编辑安全等级 重新梳理

共 20 条 20条/页 1 / 1 页

数据分类 目录支持情况

搜索

全部数据分类

一级

二级

三级

四级

五级

页面提供提交评审、编辑分类、编辑等级和重新梳理等操作时，先核对选中数量与数据范围。

暂不参与本次梳理的对象可设为“暂不梳理”。选错分类时可“重新梳理”回到待梳理；已发布和暂不梳理对象也可按业务要求重新梳理。

导入已有梳理结果

在“导入数据资产”下载模板，填写后上传。选择“资产审核”时，导入后进入待确认，仍需手动提交评审；选择“直接发布”时不再经此页面评审，应符合组织授权要求。

按导入提示处理失败项。导出时未勾选则导出当前状态全部资产，勾选则限定为所选对象。

评审与发布

1. 进入“分类分级工具 → 评审与发布”。
2. 按资产名称、系统、数据源、采集名称、盘点模式和梳理时间筛选。
3. 检查对象、分类、级别及依据，不能只根据推荐分数决定。
4. 对正确对象“评审通过”，结果成为已发布。
5. 对错误对象“评审驳回”，回到待梳理重新处理。
6. 核对成功和失败条数；元数据已删除等情况可能导致部分失败。

结果核对

在对象上检查实际分类与级别，再从安全概览查看已发布数据的分布。分类分级发布不等于访问策略已设置，动态访问和脱敏还需[访问策略](#)及[安全网关](#)。

维护法规条文与安全判定依据

法规条文为安全分类、数据分级和评审提供可追溯的判定依据。它是治理证据，不会自动把数据标记为某个安全等级。

上传法规条文

1. 进入“数据安全 → 法规条文”。
2. 选择“上传法规文件”，上传组织批准使用的文件。
3. 填写法规名称、发布机构、适用范围、生效信息和说明。
4. 保存后打开详情，确认文件可下载且元数据完整。

文件命名应包含主题和发布日期等可识别信息；正式环境不要上传含客户隐私或未公开内容的临时材料。

关联判定依据

在安全分类或安全等级的判定依据字段中选择已上传条文，并补充适用条款、解释和组织内部决策记录。一个分类可以引用多个依据，引用关系应能回答“为什么这样分类”以及“由谁确认”。

建议为每次口径变更保留新文件或新条款说明，不直接覆盖历史依据。评审时同时检查分类对象、等级、依据和评审人。

下载、替换与删除

- 选择条文后的“下载”用于留存原始证据。
- 更新文件前先确认已有分类是否引用该条文，并在变更记录中说明影响范围。
- 已被安全分类或安全等级引用的条文通常不能直接删除；先解除引用或按组织归档流程处理。

结果检查

打开一个引用该条文的分类详情，检查依据名称、条款和文件下载是否一致。若详情没有显示依据，先检查分类是否保存成功、当前用户是否具备查看法规的权限，不要把“未显示”解释为分类无依据。

维护脱敏规则与安全运行配置

脱敏规则描述敏感数据如何呈现，访问策略决定对哪些数据和访问者使用规则。只创建规则不会自动对所有数据生效。

创建和复用规则

- 1. 进入“数据安全 → 安全策略 → 脱敏规则”，建立规则目录。
- 2. 单击“新建规则”，按页面提供的规则类型填写属性并确定。
- 3. 查看结果，核对规则用途与预期呈现方式。
- 4. 在表或字段脱敏策略中引用，再通过对应访问链路验证。

被引用规则不允许编辑或删除。调整时先检查引用策略，明确替换方案，不直接修改其他业务正在使用的规则。

选择脱敏方式

按字段值的风险和业务可用性选择规则，不要把“隐藏”当作唯一目标：

场景	验证重点
身份标识类字段	是否保留业务需要的前后缀，是否仍可定位同一主体
联系方式	是否满足展示、客服或分析的最小可见范围
金额、日期等数值	是否保持统计精度和排序要求
需要完全隐藏的字段	是否在查询、导出和异常提示中都不泄露

具体算法名称和参数以当前规则表单为准。创建后先在非生产测试数据上验证空值、中文、超长值和异常格式，再由访问策略引用。

目录与引用关系

先建立脱敏规则目录，再将规则分配给维护人员。策略引用规则后，规则列表中的引用信息用于查找影响范围。修改目录名称不会改变规则执行效果，但会影响维护人员和审计检索，应记录变更。

Ranger 同步的边界

开启 Ranger 同步只表示平台尝试向目标环境同步策略。需要在目标平台检查同步对象、策略内容、失败原因和生效时间；如果目标环境没有对应数据源或策略，先处理映射关系再重试。

批量维护

“更多操作 → 导入”用于导入规则文件。“全部脱敏规则”节点下的导出为全部内容，勾选后底部导出为选中内容。按规则名称搜索定位。含规则的目录不能删除。

编码与 Ranger 同步

在“系统设置 → 参数配置”配置分类信息项自动编码。部分界面将此入口称为“参数设置”。开启时设置格式，关闭时需手工填写编码。

同页可为对应数据源开启 Ranger 同步，将策略同步到 Ranger。开启前应检查目标环境、数据源对应关系及同步配置；同步是否成功应到目标平台核对，不能仅以开关开启作为依据。

查看安全概览和日志

安全概览按已发布分类分级结果统计各等级占比、一级分类下的等级分布，以及业务系统或业务部门维度分布。待确认或待评审结果不应视为已发布统计。

安全操作日志用于追溯用户在安全模块的操作；网关日志审计用于查看经网关执行的 SQL，二者用途不同。参见[网关结果验证](#)。

管理策略目录与安全操作日志

访问策略和脱敏规则都可以按目录组织。目录用于授权管理和检索，不会自动改变策略的执行范围。

建立访问策略目录

进入“数据安全 → 访问策略 → 目录管理”，按业务系统、数据域或责任部门建立目录。为目录分配维护和查看权限，再在目录下创建访问策略。目录删除前检查是否被策略引用。

检查策略对象

创建或编辑策略时，至少核对以下信息：

- 策略类型：直接访问、行级访问、表脱敏或字段脱敏。
- 生效对象：系统、数据源、库、表、字段或标签。
- 适用用户、用户组或角色。
- 生效时间、失效时间和优先级。
- 引用的脱敏规则及冲突处理方式。

保存后用实际测试账号验证允许和拒绝两条路径。能看到策略详情不等于实际查询一定执行该策略。

查看安全操作日志

进入“数据安全 → 日志审计”或“安全操作日志”，按时间、操作人、对象、动作和结果筛选。记录问题时同时保存查询条件、操作时间、对象标识和失败提示，便于与网关访问日志对应。

日志审计记录平台操作；动态脱敏查询的访问记录还需要到[安全网关审计](#)中核对。两类日志的时间、用户标识和对象名称不一致时，先确认时区、代理账号和请求链路。

配置识别算法、规则 and 任务

智能分类分级按“算法 → 规则 → 任务 → 结果确认 → 评审发布”运行。一般规则使用的正则算法可在算法库维护；血缘级联和机器学习的具体入口、可选规则以环境提供的功能为准。

维护算法库

1. 进入“系统设置 → 识别算法 → 算法库”，准备算法目录。
2. 在算法列表区域单击“新建”，填写算法名称、目录及正则表达式。目录树中的“新建”用于创建目录，不是算法。
3. 输入一条测试数据验证匹配，再用正反例检查误判。
4. 确定后按名称或描述查找，按需编辑。

已有引用的算法编辑会提示影响；被规则引用或具有子算法的父算法不能删除。可按模板导入算法；导出时未勾选为全部，勾选为部分。

批量导入从“更多操作 → 导入算法”下载模板后填写，上传文件须保持模板结构。在任务进度浏览中查看导入、导出进度，遇到错误按提示修正记录。列表可按算法名称和描述搜索；算法目录填写名称和描述，目录内仍有算法时不能删除。

如果环境提供“机器学习算法 → 牛刀小试”，可以输入内容查看候选分类及评分。评分范围为 0 至 1 时，数值越高表示相对匹配可能性越大；评分不是业务合规结论或已发布等级。没有该入口时，可先使用一般规则及其条件测试。

用虚构代码验证正则表达式

首次使用可先做下面的小样例。它只验证表达式是否匹配输入文本，不查询真实业务数据，也不把算法保存或发布为治理规则。

1. 在新建算法表单填写一个能识别测试用途的名称，选择有权限的算法目录。当前页面在测试前也会校验这些必填项，不能只填表达式。
2. 识别算法类型选择“正则表达式”，在“识别算法内容”填写 `^[A-Z]{2}[0-9]{4}$`，表示完整文本由两位大写字母和四位数字组成。
3. 在“测试”输入框填写 AB1234，单击“测试”，检查“符合规则”的结果。
4. 将测试文本改成 AB12，再次测试，检查“没有识别到符合规则的内容”。
5. 体验完成后单击底部“取消”返回列表。正式使用时，应替换为经业务确认的表达式和正反样本，完成检查后再保存。

识别算法类型 正则表达式

识别算法内容 `^[A-Z]{2}[0-9]{4}$`

测试 `AB1234`

测试

测试结果 符合规则

测试输入	本样例的实际结果	说明
AB1234	符合规则	两位大写字母加四位数字
AB12	没有识别到符合规则的内容	数字不足四位

样例仅演示匹配方向，不代表企业编码规则。算法测试通过后，还需要在一般规则中选取对象进行条件测试，并检查任务结果；不能直接据此批量确认安全分类。

配置识别规则

进入“分类分级工具 → 智能分类分级 → 识别规则”，创建目录后选择页面实际提供的规则类型。当前核对的新建菜单提供“一般规则”；其他环境提供血缘级联或机器学习规则时，再使用对应配置。不要将不同规则类型套用到一般规则表单。

类型	操作重点
一般规则	选择依赖信息项或直接按安全分类识别；多个条件按与/或组合，选择少量对象进行条件测试
血缘级联规则	按已有血缘向下游推荐；不要套用资产盘中上游与下游都可选的规则
机器学习规则	选择学习目标：表、依赖已分类表的字段、不依赖表的字段或信息项；填写目标分类/信息项、目录、优先级、评分阈值和推荐条数

被任务引用的规则不能删除。调整算法和规则后，重新运行前应检查受影响数据范围。

一般规则的条件测试

- 在“识别规则 → 新建”选择“一般规则”。
- “识别目标”选择“信息项”或“数据分类”。选择信息项时填写识别信息项；选择数据分类时，先选择“表/视图/实体”或“数据项”，再选择目标分类。

- 3. 填写规则名称、目录、描述和优先级，再填写子条件，检查条件组之间的“与”“或”关系。
- 4. 单击“条件测试”，在弹出的元数据选择界面选取少量已知对象。
- 5. 比较预期命中、预期不命中与实际测试结果，确认后保存。

条件测试的样本应同时包含正例和反例。选择范围过大会增加等待时间，先通过小样本检验条件，再配置正式任务。

基本信息

* 规则名称

请输入

0/40

* 识别目标

☐ 信息项

☒ 数据分类

* 识别资产类型

☒ 表/视图/实体

☐ 数据项

* 选择数据分类

+ 选择数据分类

共选 0 条

* 选择目录

请选择

描述

请输入

* 优先级

☒ P3

☐ P2

☐ P1

图示展示新建表单的目标配置区域。部分界面的“安全分类”在此显示为“数据分类”。改变识别目标或资产类型后，重新检查已经选择的分类与条件，避免用字段的识别依据处理整张表。

字段或控件	操作要点
规则名称	按实际识别目的命名，遵守输入长度提示
识别目标	信息项与数据分类两种方式，决定后续需选择的依据
识别资产类型	数据分类方式下选择对象粒度，表/视图/实体与数据项分开
识别信息项或选择数据分类	选择已维护的对应对象，不能只填写分类说明代替选择
选择目录、描述	确定规则归属，记录适用范围与依据
优先级	表单提供 P1、P2、P3；不从标签自行推断多规则冲突后的唯一结果
新增条件组、条件测试	先组合条件，再以少量已知对象检查命中和未命中情况

机器学习规则的目标与参数

参数	如何选择
对表进行分类	选择表要进入的目标安全分类
对字段进行分类（依赖已分类的表）	先确认父表已有可用分类，再用对应目标处理字段
对字段进行分类（不依赖已分类的表）	选择字段要进入的目标安全分类
信息项	选择字段要依赖的分类信息项
规则目录、描述、优先级	记录归属及用途，核对多个规则同时命中的处理配置
评分阈值	限制候选结果分数，不等同于最终安全等级
推荐结果	指最终识别结果中推荐的分类条数，不是取样数据行数

选择不同学习目标后，需选择的分类或信息项不同。保存前确认目标与对象粒度匹配，不能把表级分类直接当成每个字段的最终等级。

创建和运行任务

1. 切换“识别任务”，新建任务目录。
2. 单击“新建识别任务”，填写基本信息并添加识别规则。
3. 确认后检查配置，按需要开启任务。
4. 单击“运行”，随后查看结果；“发起成功”仅表示已提交任务。
5. 复用时可复制任务并修改名称，重新核对规则及范围。

“开启/关闭”用于切换任务状态，“运行”用于发起本次执行，两者应分别检查。列表按任务名称模糊查询；复制任务的默认名称带“副本”，应改成能区分用途的名称。任务目录有任务时不能删除；删除任务前保留仍需追溯的运行及评审依据。

确认识别结果

在“识别结果确认”按资产名称、系统、数据源、采集名称、表或安全等级筛选；部分界面将该页称为“识别结果”。核对每项来源、分类和级别，必要时通过分类和等级的修改入口调整。

确认正确后提交评审；需要重做时“重新梳理”回到待梳理，仍在范围内的对象会参加后续识别；暂不处理时设为“暂不梳理”。最后由评审人员按[评审与发布](#)完成结果确认。

处理选择	适用情况	处理后检查
修改分类或等级	对象正确，但推荐结果与依据不符	调整的是所选对象，分类与等级分别准确
提交评审	已复核本批对象及建议	进入评审流程，不以提交提示替代已发布状态
重新梳理	需要调整依据后再次识别	回到待梳理；对象仍在识别范围时会参与下次任务
暂不梳理	本轮暂不处理	对象显示为暂不梳理，并记录业务处理原因

评审人员通过后分类分级结果才完成发布；驳回的对象回到待梳理。若元数据更新导致某些对象已不存在，批量处理可能同时出现成功和失败项，应按返回明细逐项处理，不只记录整体提示。

没有结果时依次检查任务运行、识别范围、算法测试和规则条件；大量误判时先修正规则和依据，不批量发布以填满覆盖率。