

LeagView ® 安略统一管控平台

用户手册

User's manual

[第1章 管理平台基础功能 1](#_Toc192755277)

[1.1 审批配置 1](#_Toc192755278)

[1.1.1 审批方案 1](#_Toc192755279)

[1.1.2 审批处理 1](#_Toc192755280)

[第2章 数据防泄露 2](#_Toc192755281)

[2.1 敏感数据识别规则 3](#_Toc192755282)

[2.1.1 敏感规则条件库 3](#_Toc192755283)

[2.1.2 敏感规则配置 5](#_Toc192755284)

# 管理平台基础功能

## 审批配置

LeagView内置完善的审批系统，可结合企业内部的管理流程，实现终端安全的管控，例如外发敏感文件需通过审批，才能明文外发出去。

### 审批方案

审批配置主要包括审批方案和审批员方案的配置，进入【全局信息|审批配置|审批方案】，可为系统创建新的审批方案，审批方案的配置流程类似安全策略，需定义进本信息、审批条件和审批范围。审批条件说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 审批内容 | 选择该审批方案适用的审批内容 |
| 分类 | 选择对应审批内容的子类 |
| 值 | 选择子类型对应的值，如安全虚拟磁盘的进盘操作，可以指定哪个安全虚拟磁盘文件进盘才走审批流程 |
| 审批员方案 | 选择已配置好的审批员方案，【注意】审批员需要使用audit账户创建 |
| 审批提醒 | 邮件提醒：系统自动发送审批通知邮件到相关的审批员，审批员点击邮件中的链接即可打开审批页面，下方可设置提醒频率和链接有效期；助手提醒：当审批员的助手在线时，弹窗提醒 |
| 自动审批 | 可选择超过某段时间自动审批或者立即自动审批，并可以定义自动审批执行的动作为允许或拒绝 |

审批范围指审批方案应用的范围，可以配置不同的终端或用户在触发审批流程时，使用不同的审批方案。

### 审批处理

审批员有专属的管理页面进行日常的审批处理。使用系统内置的audit账户登录Web控制台，进入【全局信息|系统基础数据设置|管理员账号与维护】，在此创建审批员。有权限的审批管理员登录Web控制台后，进入【审批处理】页面进行日常的审批操作。

【我的待审批信息】展示所有需要审批员处理的审批申请，如个需要查看特定的审批类型，通过“在列”中选择申请类型进行筛选。审批员审批允许或拒绝时，可以填写审批批注，可以填写允许或者拒绝的原因等，当审批允许或拒绝时，将会通过安全助手通知终端用户。如图 4‑1所示：

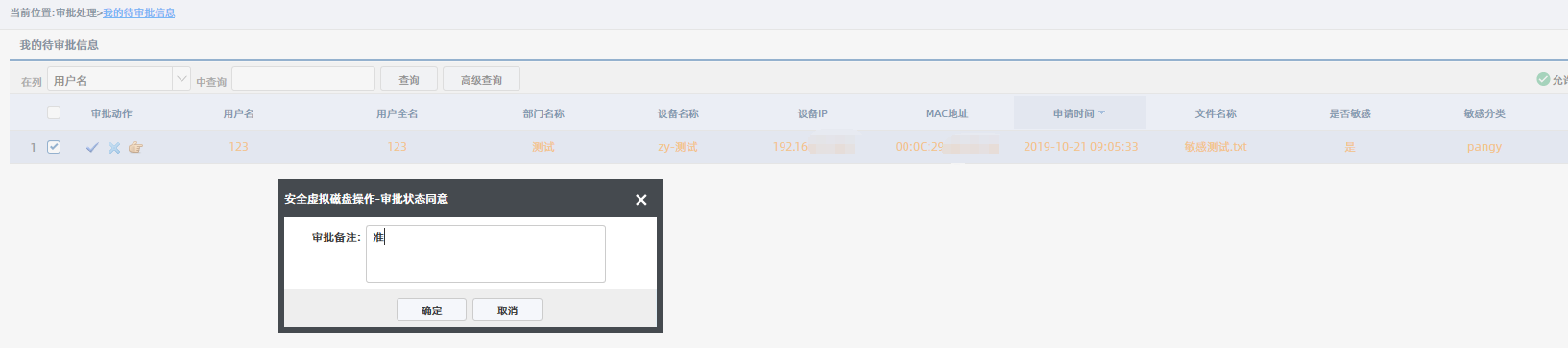


图 4‑1 审批备注

点击，可以委托他人审批，例如某些审批单子当前审批员无法做出最终决定，可以使用委托审批功能，委托其上级或者其它审批员进行审批。

【我的已审批信息】页面记录当前审批员已处理过的申请单。

【审批结果总览】展示审批方案中所有审批员的审批结果。

# 数据防泄露

信息系统在提高工作效率的同时，企业信息和数据的安全性也受到了挑战，数据泄露导致的损失和影响也越来越大。目前大部分的信息安全解决方案，还停留在采用防火墙、入侵检测、网络防病毒等保护网络、限制信息访问或者监控行为的方式，或者采用文档加密系统来对敏感数据进行保护，这类的安全防护都是从数据在传输、存储过程中入手，但是数据在使用过程中的安全却没有很好的得到保护。这些安全威胁不是防火墙、入侵检测和防病毒等传统全手段所能解决的。应该看到信息安全要立足于终端，从源头抓起，才能从根本上解决安全问题；同时信息安全也要和应用系统紧密结合，才能做到有的放矢。

联软数据防泄露系统是专为保护重要业务数据的安全而设计， 防范数据被非法复制、打印、截屏、外传。联软数据防泄露突破业务类型、数据库类型和文件类型的限制，防止各种数据被违规泄露使用；同时，不改变 业务流程、不改造应用系统，不影响内部员工间的数据交换，配合网络准入控制、终端安全管理使用，共同构建全方位的数据防泄密体系。

联软数据防泄露提供了敏感数据识别（DLP）、敏感数据发现、终端数据通道管控、业务数据防泄露、文档追踪、水印、数据可视化等功能，可以从操作、存储和传输各阶段对企业信息和业务数据提供全方位的跟踪和泄密防护。

## 敏感数据识别规则

DLP，即Data Leakage(Loss) Prevention数据泄露防护，其核心能力就是内容识别，通过精准识别企业内重要的、敏感的数据后即可对数据进行保护。LeagView内容识别具备的识别能力包括关键字、数据标识符、正则表达式、文档DNA、智能聚类等，这些能力可以自由组合，形成更灵活、更高效的识别能力。

### 敏感规则条件库

敏感规则条件库是敏感数据识别的基础，配置敏感规则模板之前需先定义好敏感规则条件。

在Web控制台选择菜单【全局信息|敏感数据基础设置|敏感规则条件库】进入敏感规则条件库页面，该页面展示已配置好的敏感规则条件，点击增加进入敏感规则条件配置页面，配置说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 条件名称 | 必填 |
| 条件编号 | 系统自动生成，在组合条件中可引用该编号 |
| 条件类型 | 文件内容：根据文件的内容进行匹配，包括关键字、正则表达式等；文件属性：根据文件的属性进行匹配，包括文件名称、文件大小等；智能聚类：根据智能聚类的结果进行匹配；扩展类型：可以将多个条件进行组合，或者使用Braise脚本匹配 |
| 条件子类型 |  |
| 关键字匹配 | 可以配置多个关键字，每个关键字使用换行分隔。勾选命中个数区间，配置个数；配置命中次数区间，检测时先检测是否有命中关键字，然后再检测配置的关键字个数和次数，同时满足个数和次数才会满足条件  命中次数区间是指每个关键字达到指定的命中次数后才算命中，比如配置了两个关键字，命中次数区间大于等于2，则文本中出现这两个关键字每个关键字的次数至少两次才算命中  关键字命中个数区间是指在配置的多个关键字中，命中数量范围内的关键字即可满足条件，比如总共配置了四个关键字，如果配置区间最小值2，最大值3，则四个关键字中命中2至3个即为满足条件；如果配置区间最小值3，最大值为空，则四个关键字至少命中3个即为满足条件；如果不勾选，则以上关键字都需要命中才能满足条件 |
| 正则表达式 | 需先对正则表达式有一定了解，配置正则表达式和命中次数区间，同时满足条件即为敏感 |
| 姓名/地址等 | 系统内置的数据标识符，即将常见的数据进行归类，用另一个名词代替，例如张三、李四我们统称为姓名，姓名相当于一个变量，它可以是张三，也可以是李四 |
| 文件名称 | 根据文件名称匹配 |
| 文件类型 | 根据文件的类型进行匹配如doc、ppt等，可以识别任何文本类型的文件，勾选“指定其它文本格式”，例如html和log，那么可以这样指定：html|log，即多个后缀用“|”分隔 |
| 加密文件 | 识别目标文件是否加设了打开口令，例如压缩文件加设了加压口令 |
| 文件MD5 | 根据文件的MD5值进行匹配，点击选择按钮选择进行匹配的样本文件的MD5值 |
| 文件DNA | 根据文件的DNA相似度进行匹配，点击选择按钮选择进行匹配的样本文件的DNA值 |
| 文件大小 | 根据文件大小区间进行匹配 |
| 创建日期 | 根据文件创建日期时间区间进行匹配 |
| 修改日期 | 根据文件修改日期时间区间进行匹配 |
| 不可识别文件 | 匹配系统无法识别的文件，目前系统能识别的文件类型包括doc、docx、xls、xlsx、ppt、pptx、pdf、zip、rar、7z、txt等，可指定其他格式（如html、log等） |
| 源代码文件 | 支持对源代码文件（R、Lua、Java、PHP、Objective-C、GO、C#、Swift、HTML、C、JavaScript、Python、Visual Basic）进行识别 |
| 文件容量 | 使用文件信息容量来衡量文件敏感程度，例如文档的字数、行数等 |
| 指定分类 | 根据智能聚类的结果对目标文件进行匹配 |
| 条件表达式 | 使用条件表达式对现有的条件进行组合，形成新的条件，当表达式为真时，表示满足条件，表达式支持的运算符及优先级由高到低是：(),NOT,AND,OR  例如：  C1 AND (P2 OR P3 OR NOT I4) AND NOT E5  其中的C1,P2,P3,I4,E5是已编辑条件的条件编号 |
| Braise脚本 | 根据Braise脚本对目标文件进行匹配 |

### 敏感规则配置

敏感规则主要将敏感条件、敏感级别、敏感分类进行引用，组合成可以直接被策略引用的规则模板。敏感规则还可以定义搜索文件文件的位置，指定搜索特定的业务系统等。

Web控制台选择菜单【全局信息|敏感数据基础设置|敏感规则配置】点击增加，创建新的规则，配置参数说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 敏感规则模板名称 | 必填，起个便于理解的名字，安全策略根据名称引用敏感规则模板 |
| 敏感数据分类 | 定义该模板匹配到的敏感文件属于哪个分类 |
| 敏感级别 | 定义该模板匹配到的敏感文件属于哪个分类 |
| 敏感规则 | 点击从条件库中选择，从条件库中选择相应条件写入规则，一个模板内只有一种规则条件，如果需要多个条件，则到敏感规则库中创建组合条件 |
| 扩展搜索 | 智能识别文件类型：人为将常规文档的后缀修改为其他类型时能准确识别出原文件类型，例如将x.txt修改为x.ttt后仍能识别为txt文件，开启后比较耗终端性能，会降低扫描速度；搜索压缩文件：敏感扫描时，检查压缩包里的文件；搜索图片文件中隐藏的文本：人为将常规txt文档的文本嵌套在图片文件中时能检查txt的内容，例如使用命令：copy /B 123.png + 1.txt 12345.png,将123.png和1.txt合成12345.png, 检查合成后文件，仍能识别1.txt内容 |
| 出现位置 | “页眉”，“页脚”仅对Word 文档格式有效 |
| 精确位置 | 定义查找的范围，例如某些文档的敏感信息仅会出现在前半部分或者后半部分，仅扫描敏感信息所在的部分，提高扫描的效率，只有txt、log等纯文本格式可以精确定位，其它格式如doc、docx、ppt等不一定准确，会存在一定的误差 |
| 业务系统 | 指定来源于某个业务系统的文件 |
| 受控数据盘 | 指定来源于某个安全虚拟磁盘的文件 |