

User's manual

用户手册

[第1章 前言 1](#_Toc104967357)

[1.1 声明 1](#_Toc104967358)

[1.2 联系方式 1](#_Toc104967359)

[第2章 产品简介 1](#_Toc104967360)

[第3章 桌面管理 2](#_Toc104967361)

[3.1 桌面管理策略 2](#_Toc104967362)

[3.1.1 长期未运行事件 2](#_Toc104967363)

[3.1.2 配置变更事件 3](#_Toc104967364)

[3.1.3 节能管理策略 5](#_Toc104967365)

[3.1.4 非工作时间开机事件 9](#_Toc104967366)

[3.1.5 业务门户策略 11](#_Toc104967367)

[3.1.6 公告信息配置 15](#_Toc104967368)

[3.1.7 消息通知任务 16](#_Toc104967369)

[3.1.8 终端性能监控策略 20](#_Toc104967370)

[3.2 远程协助 21](#_Toc104967371)

[3.2.1 远程协助策略 22](#_Toc104967372)

[3.2.2 远程协助请求 22](#_Toc104967373)

[3.2.3 远程协助审计 24](#_Toc104967374)

[第4章 软件管理 24](#_Toc104967375)

[4.1 软件资产与授权管理 25](#_Toc104967376)

[4.1.1 软件信息与授权管理 25](#_Toc104967377)

[4.1.2 软件安装列表 26](#_Toc104967378)

[4.1.3 软件订单管理 26](#_Toc104967379)

[4.2 软件标准化管理策略 27](#_Toc104967380)

[4.3 软件商城 32](#_Toc104967381)

[4.3.1 软件仓库 33](#_Toc104967382)

[4.3.2 软件发布策略 34](#_Toc104967383)

[4.3.3 软件升级策略 36](#_Toc104967384)

[4.4 软件分发 37](#_Toc104967385)

[4.4.1 软件分发任务 37](#_Toc104967386)

[4.5 工具管理 41](#_Toc104967387)

[4.5.1 工具仓库 41](#_Toc104967388)

[4.5.2 工具发布策略 42](#_Toc104967389)

[4.5.3 工具箱 42](#_Toc104967390)

[4.6 软件使用时长管理 45](#_Toc104967391)

[第5章 补丁管理 46](#_Toc104967392)

[5.1 微软WSUS策略 47](#_Toc104967393)

[5.2 微软补丁库管理 48](#_Toc104967394)

[5.2.1 微软补丁下载选项 48](#_Toc104967395)

[5.2.2 微软补丁更新策略 49](#_Toc104967396)

[5.2.3 微软补丁卸载策略 52](#_Toc104967397)

[5.2.4 微软补丁库信息 52](#_Toc104967398)

[5.2.5 补丁下载安装信息 53](#_Toc104967399)

[5.2.6 补丁安装详细信息 53](#_Toc104967400)

[5.2.7 补丁安装详细信息 54](#_Toc104967401)

[5.2.8 漏洞修复汇总 54](#_Toc104967402)

[5.2.9 终端漏洞TOP10 54](#_Toc104967403)

[第6章 终端安全管理 55](#_Toc104967404)

[6.1 终端安全策略 55](#_Toc104967405)

[6.1.1 主机进程安全检测策略 55](#_Toc104967406)

[6.1.2 终端标准化策略 57](#_Toc104967407)

[6.1.3 终端流量管理策略 59](#_Toc104967408)

[6.1.4 Windows本地安全策略 61](#_Toc104967409)

[6.1.5 网络资源访问控制策略 63](#_Toc104967410)

[6.1.6 Braise脚本策略 66](#_Toc104967411)

[6.1.7 注册表访问控制策略 66](#_Toc104967412)

[6.1.8 终端系统自检策略 68](#_Toc104967413)

[6.1.9 操作系统账户管理 71](#_Toc104967414)

[6.1.10 网络连接审计与控制策略 72](#_Toc104967415)

[6.1.11 高级终端保护策略 75](#_Toc104967416)

[第7章 数据防泄露 77](#_Toc104967417)

[7.1 敏感数据识别规则 77](#_Toc104967418)

[7.1.1 敏感规则条件库 78](#_Toc104967419)

[7.1.2 文件DNA库 80](#_Toc104967420)

[7.1.3 文档智能聚类 81](#_Toc104967421)

[7.1.4 敏感数据分类定义 84](#_Toc104967422)

[7.1.5 敏感数据级别定义 84](#_Toc104967423)

[7.1.6 敏感规则配置 84](#_Toc104967424)

[7.2 敏感数据发现 85](#_Toc104967425)

[7.2.1 敏感文件审计策略 85](#_Toc104967426)

[7.2.2 敏感数据分布 87](#_Toc104967427)

[7.2.3 敏感文件自检 88](#_Toc104967428)

[7.3 终端数据通道管控 90](#_Toc104967429)

[7.3.1 上网审计策略 90](#_Toc104967430)

[7.3.2 FTP访问控制策略 92](#_Toc104967431)

[7.3.3 非授权外联策略 94](#_Toc104967432)

[7.3.4 硬件设备管理策略 98](#_Toc104967433)

[7.3.5 文件读写操作审计策略 101](#_Toc104967434)

[7.3.6 打印控制策略 103](#_Toc104967435)

[7.3.7 即时通讯审计策略 105](#_Toc104967436)

[7.3.8 邮件审计策略 107](#_Toc104967437)

[7.3.9 移动存储管理 111](#_Toc104967438)

[7.4 水印服务 113](#_Toc104967439)

[7.4.1 有代理水印 113](#_Toc104967440)

[7.4.2 水印追溯 115](#_Toc104967441)

# 前言

## 声明

Copyright © 2003-2019深圳市联软科技股份有限公司（以下简称联软科技）及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

由于产品版本升级或其他原因，本手册内容有可能变更。联软科技留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，联软科技全力在本手册中提供准确的信息，但是不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

## 联系方式

用户支持邮箱：[support@leagsoft.com](mailto:support@leagsoft.com)

技术支持热线电话：400-6288-116

网址：[http://www.leagsoft.com](http://www.leagsoft.com/)

# 产品简介

为应对来自内外部的网络与数据安全威胁，企业或各单位在内部网络中陆续部署数据防泄密、补丁管理、终端安全等各种安全管理系统。这些分散的、不断增多的安全系统加重了管理负担，且因缺乏统一的架构，数据难以集中，系统间缺乏协同，使得安全建设效果欠佳。联软科技认为将网络、终端、应用、信息割裂开来的分别予以治理的方式存在很大局限性。解决信息安全管理问题，必须从顶层设计入手，将终端、应用、信息，乃至包括人员的管理都纳入解决方案中，才能有效的解决问题，为用户提供一体化、全方位的网络与信息安全解决方案。

# 桌面管理

LeagView能够辅助IT管理员对终端桌面的一些运维管理，包括终端允许情况监视、配置变更监视、节能管理、非工作时间开机监视、业务门户维护、公告信息、消息推送等，提高管理员的运维效率。

## 桌面管理策略

### 长期未运行事件

LeagView能发现并记录设备长时间离线事件。

进入【桌面管理|策略配置|长期未运行事件】**。**

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 设备连续未运行天数 | 定义设备连续多少天内未运行，也就是离线的状态，被认为是长期未运行 |
| 状态 | 缺省禁用，启用后开始对全网设备进行监测 |

进入【综合报表|数据分析报表|设备长时间离线报表】，可以查看本策略产生的审计信息、报表，并导出为 Excel文件以分析。

**策略示例：**

需求：IT管理员在对在网设备梳理时，需要找出那些超过1个月未在线的设备，这些设备可能已经不在使用。

配置步骤：

1. 进入【桌面管理|策略配置|长期未运行事件】，设置设备连续30天未运行，并将状态改成启用状态，如图 5‑1



图 5‑1 长期未运行事件配置

1. 到【综合报表|数据分析报表|设备长时间离线报表】，可以查看本策略产生的审计信息、报表，并导出为 Excel文件以分析。

### 配置变更事件

本页面的配置能实现：检测并记录终端的软硬件信息的变更、跟踪配置变更可以帮助管理员控制网络资产，并及时对其产生邮件告警。

进入【桌面管理|策略配置|配置变更事件】**，**点击增加，进入【增加配置变更事件】页：

**硬件变更配置**

单击硬件变更配置，出现硬件变更配置页面。在这个页面中，可以配置哪些硬件的变化会被配置管理系统认为是配置变更。

**软件变更配置**

单击软件变更配置出现软件变更配置页面，这个页面中可以选择软件配置变更的类型。

如果选择【检查指定软件的配置变化,下列软件配置项属性值发生变化时认为发生配置变更】，则必须指定哪些软件发生变化（安装、卸载）时认为是配置变更。

如果选择【检查除指定软件外的软件配置变化】，则同样必须指定哪些软件之外的软件发生变化认为是配置变更。

如果选择【检查所有软件的配置变化】则任何软件变化都认为是配置变更。

如果选择【检查除windows补丁包外的软件配置变化】则除了Windows补丁包的安装与卸载外其它软件的任何变化都认为是配置变更。

如果选择【检查除指定软件外的和除windows补丁包外的软件配置变化】则除了指定软件和Windows补丁包的安装与卸载外其它软件的任何变化都认为是配置变更。

单击增加，出现一行新的软件记录，可以输入软件名称和版本。一般情况下很难直接输入精确的软件名称和版本，此时可以单击从样本设备获取，弹出获取已安装安全助手设备的软件信息的弹出窗口：

在这个页面中首先选择查询条件（可选择条件有“设备IP地址”、“设备名称”、“用户名”、“MAC地址”、“软件名称”），然后输入查询条件后单击<查询>按钮则将符合输入条件的设备上已安装的软件全部显示在页面中。选中查询出来的软件列表中的一个或多个后单击选择按钮则将选中的软件信息（包括软件名称和软件版本）设置到获取已安装安全助手设备的软件信息的弹出窗口。

进入【桌面管理|设备信息|设备配置变更信息】，可以查看本策略产生的审计信息，并导出为 Excel文件以分析。

**策略示例：**

需求：企业资产管理员不允许员工私自更改终端设备的硬件，并且配发的电脑已安装了固定的软件，如果有更改行为及时邮件通知管理员。

配置步骤：

1. 进入【桌面管理|策略配置|配置变更事件】配置策略，在【基本信息】中下拉菜单选择已定义好的预案，如果当前没有可选择的预案，点击配置事件处预案，事件处理预案配置请参考4.4.2事件处理预案；在【硬件变更配置】，全选所有硬件类型；在【软件变更配置】，选择【检查所有软件的变化】，最后下发策略，如所示



图 5‑2 配置变更事件设置

1. 有权限的管理员进入【桌面管理|设备信息|设备配置变更信息】，可以查看本策略产生的审计信息

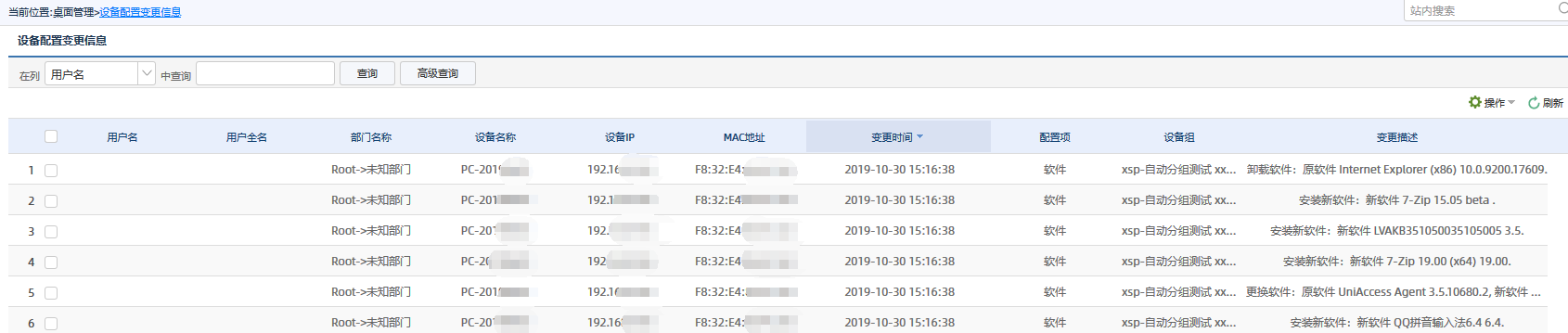


图 5‑3 设备配置变更信息

### 节能管理策略

随着低碳理念的广泛普及，节能环保逐渐成为 IT 管理中必须重视的一环。 LeagView 节能管理重点解决终端用户下班后不关闭计算机导致的电能浪费等问题。具体的做法是当终端计算机在指定时间内没有键盘或鼠标动作时会强制执行指定的动作（睡眠，休眠，关机等），在执行动作前可以设置弹出提示以免误操作；同时提供报表和视图展示各部门各阶段的节能效果供领导参考。

进入【桌面管理|策略配置|节能管理策略】。

管理员可以点击增加策略，对终端设备，配置工作时间、非工作时间的节能管理办法（包括：关机、注销、锁定、重新启动、睡眠、休眠，关闭显示器、锁定并关闭显示器、不作处理）、是否审计、是否提示终端、提示内容以及弹出提示倒计时。

此外，本策略可以有如下配置：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 工作时间 | 先定义工作时间段，以便可以针对工作时间段和非工作时间段做相应的处理 |
| 工作时间节能管理设置 |  |
| 节能处理办法 | 当终端鼠键无操作到达指定时间后，触发相应的操作，如：睡眠、锁定、休眠、关机等 |
| 处理前是否提示 | 当选择处理前提示时，终端将在触发相应操作前进行弹框提示 |
| 弹出提示倒计时 | 当选择处理前提示时，终端将在触发相应操作前进行弹框倒计时 |
| 非工作时间节能管理 |  |
| 节能处理办法 | 当终端鼠键无操作到达指定时间后，触发相应的操作，如：睡眠、锁定、休眠、关机等。。 |
| 处理前是否提示 | 当选择处理前提示时，终端将在触发相应操作前进行弹框提示 |
| 弹出提示倒计时 | 当选择处理前提示时，终端将在触发相应操作前进行弹框倒计时 |
| 其它设置 |  |
| 节能优先级 | 强制执行节能计划：忽略终端用户配置的相关设置，完全按照 “ 节能管理策略 ” 执行。 优先执行终端节能计划：完全遵循终端用户配置的相关设置，忽略 “ 节能管理策略 ”，即 “ 节能管理策略 ” 无效果。智能选择最优节能计划：通过判断 “ 节能管理策略 ” 与终端用户配置，选择时间最短的配置执行；例子：终端配置休眠时间为5分钟，“ 节能管理策略 ” 配置为6分钟，那么以5分钟执行 |
| 节能策略解除 | 配置允许客户端自主解除节能策略，如果勾选，终端助手托盘右键菜单可以选择【解除节能管理策略】，并限定终端最长解除时间，超过该时间自动恢复节能管理策略 |
| 例外设置 | 某些终端需要长时间运行，并不适用节能管理策略，比如这些终端运行某些重要的进程，或者正在升级软件或者打补丁时，可将这些终端按照进程条件进行策略例外 |

进入【桌面管理|信息查询|节能管理信息】，可以查看本策略产生的审计信息，默认按照用户进行统计节能处理结果，点击处理办法的统计数字，可以下钻查询到该用户详细的审计日志。

节能管理审计信息还可以估算节省电能和节省成本，但需先定义关机、休眠、睡眠、关闭显示器的情况节省电功率，以及电费。点击操作，选择【配置默认节省电功率】 ，配置关机、休眠、睡眠、关闭显示器每小时节省的电功率，以及电费。点击保存后，系统自动计算节省电能和节省成本。

【注意】只有节能处理办法为关机、休眠、睡眠、关闭显示器，才可以估算节省电能和节省成本，节能时间使用有效结束时间减去有效开始时间。

进入【综合报表|数据分析报表|节能审计报表】，可以查看本策略产生的报表并导出或打印。

**策略示例：**

需求：IT管理员为了响应公司节能环保的号召，需对员工的办公电脑强制节能处理，员工在工作时间内30分钟内未使用电脑，则将电脑自动进入睡眠状态；非工作时间内，30分钟未使用电脑，则将电脑自动关机。并每月输出节能报表，估算每月可以为公司节省多少电能和成本。

配置步骤：

1. 进入【桌面管理|策略配置|节能管理策略】配置节能管理策略，策略配置详情如图 5‑4所示。

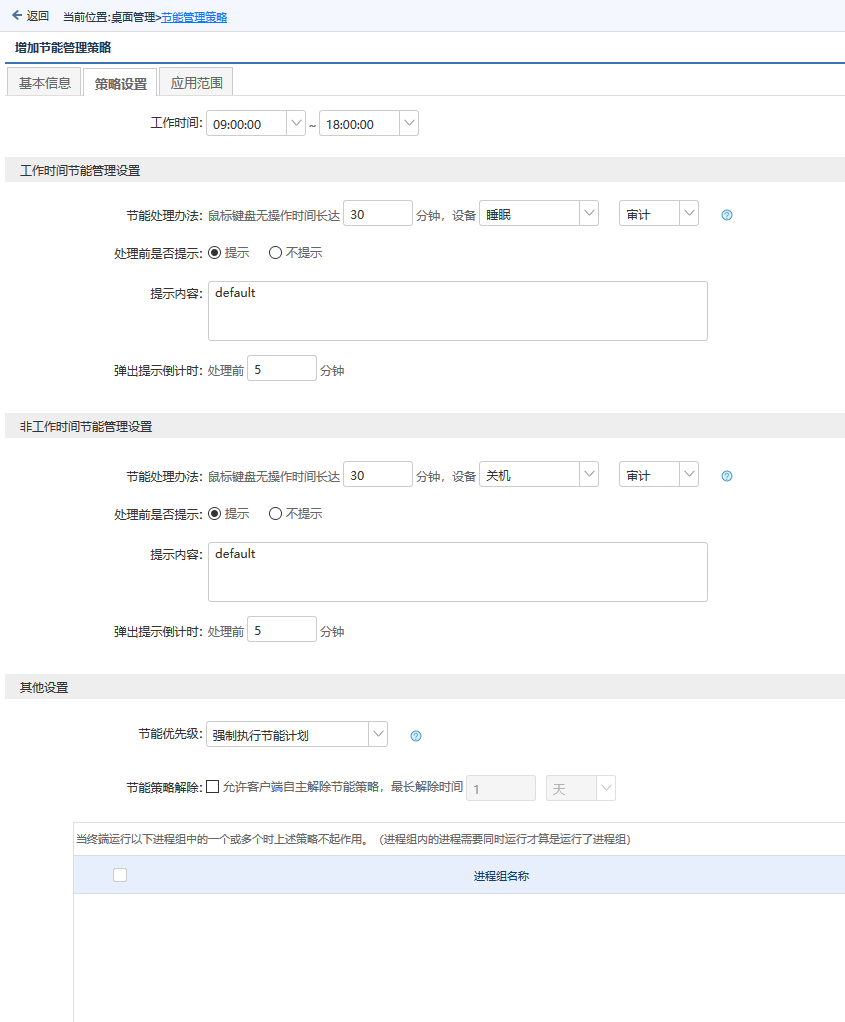


图 5‑4 节能管理策略配置

1. 进入【综合报表|数据分析报表|节能管理审计信息】，点击操作，选择【配置默认节省电功率】，配置节省功率和电价。



图 5‑5 配置默认节省电功率

1. 进入【综合报表|数据分析报表|节能管理审计信息】，即可看到节省电能和节省成本的报表。

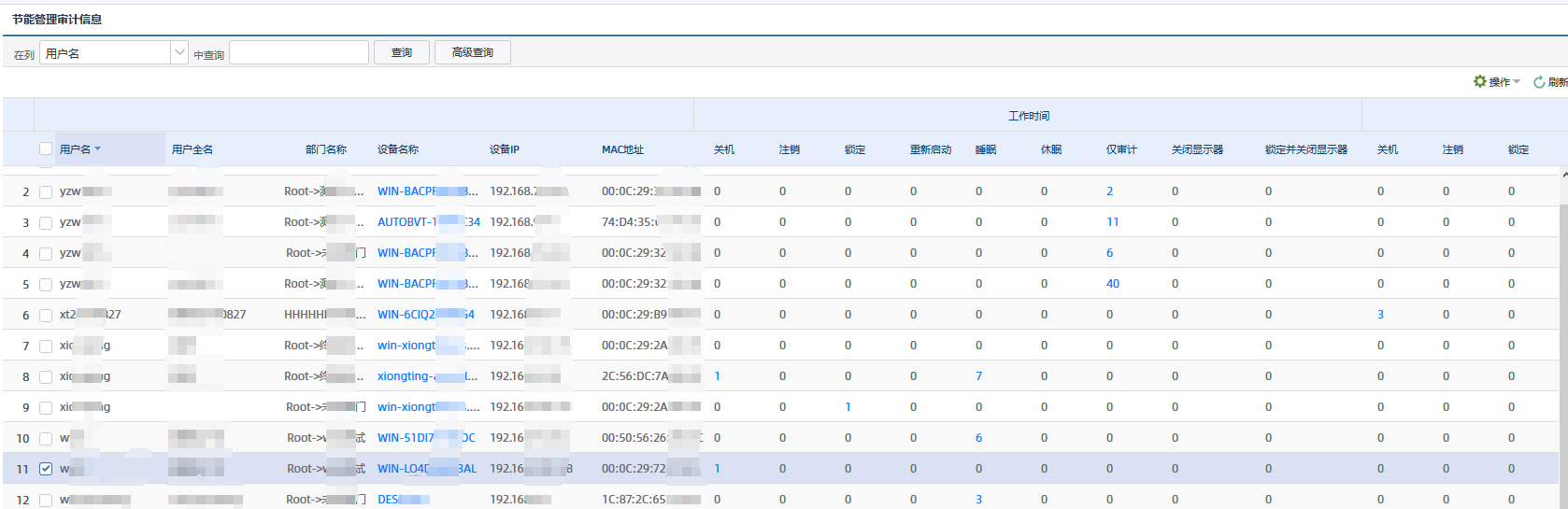


图 5‑6 节能管理审计信息

1. 点击相关的统计数字，可进入查看节省电能和节省成本详情。



图 5‑7 某终端节能详情

### 非工作时间开机事件

进入【桌面管理|策略配置|非工作时间开机事件】**。**

管理员可以在本页面配置企业的非工作时间，以审计终端在非工作时间的开机事件。

点击非工作时间设置，定义非工作时间。点击增加，可以配置审计范围内终端在非工作时间内开机情况的策略。

进入【桌面管理|信息查询|非工作时间开机审计信息】，可以查看本策略产生的审计信息，并导出为 Excel文件以分析。

进入【综合报表|数据分析报表|非工作时段接入报表】，可以查看本策略产生的报表并导出或打印。

策略示例：

需求：监控终端主机在非工作时间的开机情况，分析终端是否存在异常。

配置步骤：

1. 进入【桌面管理|策略配置|非工作时间开机事件】点击，定义非工作时间，如图 5‑8所示：

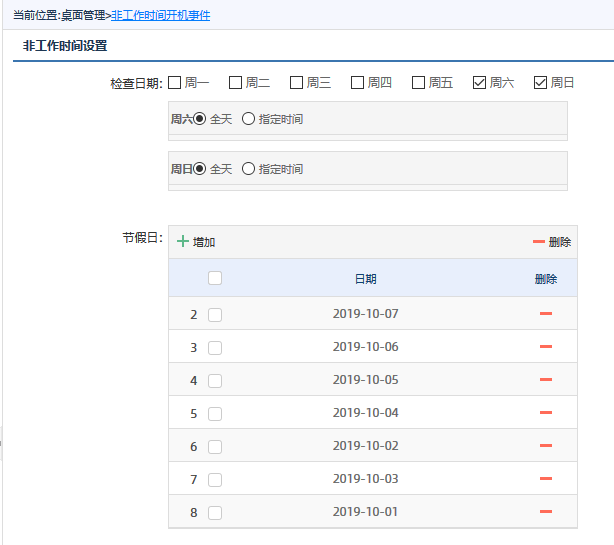


图 5‑8 定义非工作时间

### 业务门户策略

管理员可以根据业务系统URL定义IE浏览器Internet选项的配置，通过策略下发到终端主机，在终端助手主页面上生成业务系统的业务门户导航页面，用户可以点击相应的业务系统名称一键访问业务系统，免去繁琐的IE浏览器配置。

进入【桌面管理|策略配置|业务门户策略】。

点击增加策略或已有策略，进入策略配置页面，进入【策略配置】栏，点击增加，弹出【编辑规则】弹窗。管理员可以配置内容如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 业务系统名称 | 本业务门户的名称，必填 |
| 上传图标 | 该业务门户显示在助手端的图标，如不上传，则使用浏览器的默认图标 |
| URL | 本业务门户的URL，必填 |
| 浏览器类型 | IE和谷歌Chrome之间单选，选择IE后，才会显示下面IE相关的配置，选择谷歌Chrome的话，下面IE所有的配置隐藏，不需要配置。助手会根据策略的配置调用IE或者谷歌Chrome浏览器打开业务系统URL |
| 是否启用IE自动化管理功能 | 选择IE时，存在“是否启用IE自动化设置功能”总开关，以便满足不需要进行设置只是添加业务系统到业务门户的需求，缺省值禁用，禁用状态下，以下配置不生效，置灰 |
| 将业务系统URL添加到兼容性视图 | 让该门户的页面显示兼容于不同浏览器 |
| 管理加载项 | 指IE加载项，比如配置JITVCKEx.Class状态为“已启用状态” |
| IE Internet选项配置 | 请参考IE8、IE11的 Internet选项配置 |

**策略示例：**

需求：企业内有多个业务系统必须使用IE浏览器访问，且要设置IE 的相关配置，但其中有两个业务系统对IE浏览器的设置要求有冲突，员工每次访问这两个业务系统时需要反复修改配置，非常繁琐，希望可以一键设置，甚至不希望自己手动设置IE浏览器。

配置步骤：

1. 管理员进入【桌面管理|策略配置|业务门户策略】配置业务门户策略，点击增加规则，将企业内需要设置IE选项的业务系统添加到策略中，并设置好IE的Internet选项配置，如图 5‑9所示：



图 5‑9 业务门户策略规则

1. 终端用户打开助手页面，选择业务门户TAB，点击业务系统图标即可打开浏览器访问，不需要额外的设置。

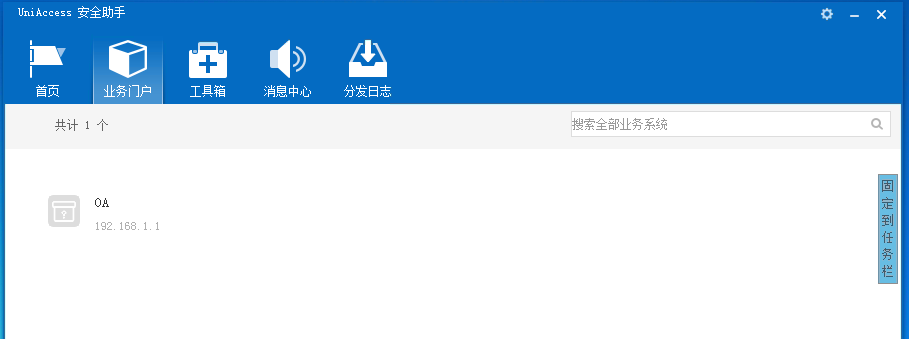


图 5‑10 助手业务门户

1. 如需将业务门户放到助手首页上，进入【桌面管理|助手首页管理|助手首页管理策略】配置助手首页管理策略，在【策略配置】中，选择“公告和业务门户导航模式”，并勾选“显示业务门户导航栏”，如图 5‑11所示

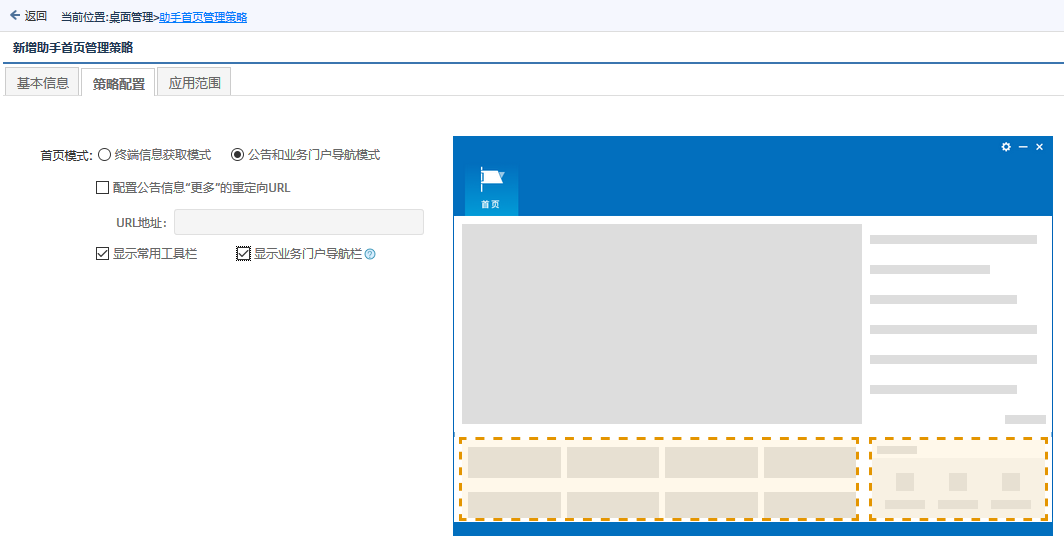


图 5‑11 助手首页管理策略配置

1. 终端用户在助手首页即可看到业务门户的业务系统，如图 5‑12所示：



图 5‑12 助手首页显示业务系统

### 公告信息配置

此公告信息指的是助手上用户认证TAB界面的公告，主要发布准入认证相关的公告。

进入【桌面管理|策略配置|公告信息配置】**。**

管理员可以在本页面配置本域内所有助手端的用户认证页的公告。点击增加，管理员可以编写用户认证页显示的公告并选择发布时间。

终端用户打开助手界面，进入【用户认证】TAB界面时，可以看到管理员发布的公告。

**策略示例：**

需求：管理员需要使用公告信息发布关于准入认证的一些常见问题解答，方便用户完成准入认证。

配置步骤：

1. 进入【桌面管理|策略配置|公告信息配置】，点击增加，新增一条公告信息，如图 5‑13所示

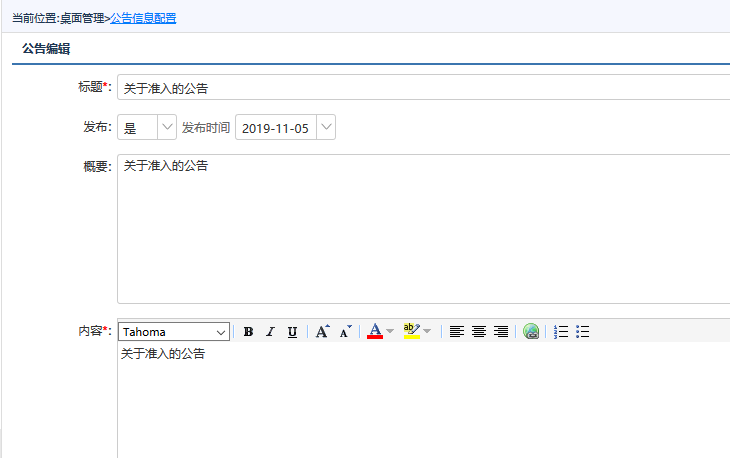


图 5‑13 公告配置

1. 终端用户打开助手认证TAB，即可看到公告信息。

### 消息通知任务

消息通知除了可以推送一些紧急的消息在终端屏幕中间弹窗外，还存在提供信息安全提醒、日常事件通知（例如通知员工参加活动、会议）、内部系统使用小TIPS等非重大或非紧急消息的推送等使用场景，因这些通知比较多，总是在屏幕中间弹窗的话会对用户造成严重干扰，因此消息通知窗口需要可以灵活定义，比如非紧急重要的通知可以在屏幕右下角弹窗。

进入【桌面管理|策略配置|消息通知策略】**。**

定义助手端推送的通知。点击增加任务，管理员可以编写推送给范围内终端的通知，并设置通知时间、频率和消息框属性。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 消息设置 |  |
| 通知框标题 | 必填，弹窗的标题 |
| 通知内容格式 | 纯文本通知：通知内容仅允许填写纯文本；富文本通知：消息内容可以编辑字体、颜色、对齐方式、插入超链接等；HTML文件通知：可以将网页文件保存为XXX.html形式进行上传；HTML-ZIP文件：zip压缩文件包，压缩包根目录内必须包含index.html，其他文件不限路径  备注：所上传的文件均请勿超过8MB；URL通知：输入终端可以访问到的URL |
| 通知内容 | 根据通知内容格式设置，输入对应的内容 |
| 反馈信息 | 无需终端反馈：终端助手消息通知弹窗无法输入反馈内容；终端可选反馈：终端助手消息通知弹窗可以输入反馈内容，也可以不反馈；终端必须反馈：终端助手消息通知弹窗必须输入反馈内容；反馈内容可以在【消息通知审计信息】中查看 |
| 通知时间及频率 |  |
| 通知起始日期 | 立即通知：消息通知任务保存后，立即下发通知任务；定期通知：在指定的日期下发通知，配合通知时间段设置 |
| 通知有效期限 | 定义通知任务在指定的有效期生效 |
| 通知时间段 | 定义通知任务指定的时间段内通生效 |
| 通知频率 | 定义通知任务的频率，避免过度干扰用户或者通知不到位 |
| 消息框属性设置 |  |
| 通知框位置 | 定义通知框在屏幕的位置，重要的消息通知可以设置为屏幕中间，非重要的消息通知可设置为屏幕右下角 |
| 最前端显示 | 使消息通知弹窗在所有窗口最前面，避免被遮挡 |
| 最小化控制 | 是否允许终端用户最小化消息通知框 |
| 手动关闭设置 | 定义用户可手动关闭或者在一段时间后才能关闭 |
| 自动关闭设置 | 定义消息通知框在一段时间后自动关闭 |
| 不允许挪动窗口 | 终端用户不可以挪动消息通知窗口的位置 |
| 弹出窗口百分比 | 设置消息通知窗口占屏幕的大小，按照终端屏幕百分比设置 |

进入【桌面管理|信息查询|消息通知审计信息】，可以查看已下发的消息通知任务，如果有反馈，在此也可以看到终端用户反馈的内容。

**策略示例：**

需求：管理员需要立即发布一条紧急的通知给所有终端用户。

配置步骤：

1. 进入【桌面管理|策略配置|消息通知策略】点击增加任务，在【基本配置】中配置通知内容，如图 5‑14所示：



图 5‑14 消息通知任务配置

1. 终端助手会立即弹出消息通知窗口，如图 5‑15所示

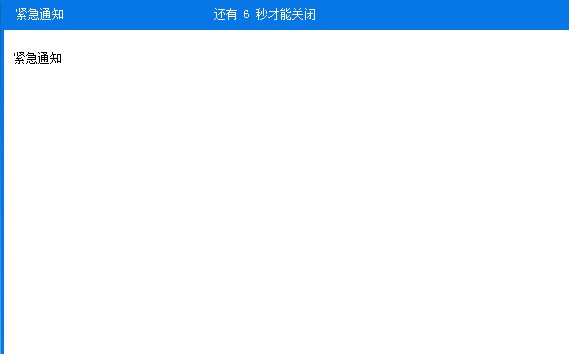


图 5‑15 助手消息通知弹窗

### 终端性能监控策略

终端性能监控策略主要是监控终端主机的CPU、内存、硬盘的使用率，当发现异常时及时上报后台服务器。

登录Web控制台，进入【桌面管理|策略配置|终端性能监控策略】，点击增加策略，新建一条策略。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| CPU占用率 | 定义CPU使用率连续多长时间超过阈值认为异常事件 |
| 内存占用率 | 定义内存使用率连续多长时间超过阈值认为异常事件 |
| 系统盘占用率 | 定义操作系统所在的盘符使用率超过阈值认为异常事件 |
| 硬盘占用率 | 定义硬盘整体使用率超过阈值认为异常事件 |
| 统计周期 | 定义统计的时间间隔 |

**策略示例：**

需求：IT资产管理员希望及时发现那种老旧的、经常卡顿的电脑，以便采购新的电脑进行替换。

配置步骤：

1. 使用终端性能监控策略，实时监控终端的性能使用情况，策略配置如图 5‑16所示：

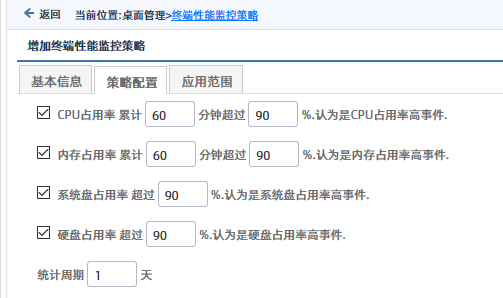


图 5‑16 终端性能监控策略配置

1. 进入【桌面管理|信息查询|终端性能监控信息】，可按照CPU、内存、系统盘、硬盘查看相关的设备。如图 5‑17所示：



图 5‑17 终端性能监控信息

## 远程协助

在大型网络中，特别是跨区域的网络，企业IT部门的管理员在处理终端的故障时，通过远程协助功能可以方便的进行运维，提高运维效率。

在Web控制台，【桌面管理|设备概要信息】，全网设备这里可以快速对终端发起远程协助，选中一条设备信息，点击【远程协助】对选中终端发起远程协助。远程协助前，管理员需要下载远程协助工具。

### 远程协助策略

可以通过远程协助策略规范远程协助的过程，下发远程协助策略后，管理员和终端用户只能按照策略约束的内容进行交互，进入Web控制台【桌面管理|策略配置|远程协助策略】策略主要配置参数如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 允许终端主动请求管理员的远程协助 | 开启此项，助手端显示远程协助tab页，终端用户可以通过助手页面，向在线的管理员申请远程协助请求 |
| 允许终端收到管理员的远程协助请求时弹出确认提示 | 勾选此项，管理员发起远程协助时，必须经过终端用户确认 |
| 允许由提供远程协助的管理员来决定终端是否弹出确认提示 | 勾选后，管理员可以在发起远程协助时，手动选择监控模式或协助模式 |
| 允许终端被远程协助时显示提示信息 | 勾选后终端用户被远程时，显示当前远程协助的管理员信息 |
| 允许管理员控制终端的键盘和鼠标 | 勾选后，管理员可以控制终端的键盘和鼠标，否则无法控制 |
| 允许管理员拷贝终端的文件 | 勾选后，管理员可以从终端拷贝文件，否则无法拷贝，但管理员可以向终端发送文件 |
| 远程中继模式 | 如果远程端与被远程端网络可达，可以选择【无远程中继模式】；如果远程端与被远程端网络不可达，可以在网络中部署中继服务器连接远程端和被远程端，然后选择【指定远程中继ip或域名】；如果网络较复杂，不同的网段需要使用不同的中继，选择【根据终端网段选择对应的中继IP】 |

### 远程协助请求

远程协助策略开启“允许终端主动请求管理员远程协助”后，终端用户可以在助手页面申请远程协助。

终端用户点击助手托盘，打开助手界面，选择【远程协助】TAB，点击申请远程协助，然后选择当前在线的管理员，点击发起申请。如图 5‑18所示：



图 5‑18 申请远程协助

【注意】管理员需在助手端设置在线状态，设置方法如下：

右键助手托盘菜单，选择【管理员状态设置】，管理员助手的登录密码要与管理员密码一致才行。如图 5‑19所示



图 5‑19管理员状态设置

终端用户申请远程协助后，管理员的助手端会自动弹出远程协助申请提醒，如图 5‑20所示：

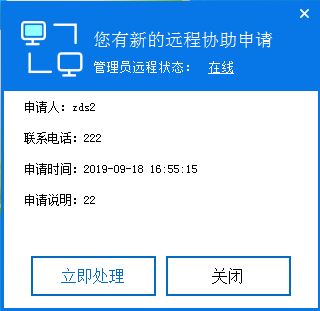


图 5‑20 远程协助申请提醒

点击立即处理进行远程。

如未能及时处理，可以进入Web控制台，【桌面管理|设备信息|远程协助请求】，选择【终端提交待处理请求】TAB页面，选中对应的请求记录，点击协助或拒绝处理。

### 远程协助审计

为了满足合规要求，管理员远程协助终端的过程都会被记录下载，包括远程的设备，发生时间，远程管理IP，文件操作行为等。进入【桌面管理|策略配置|远程协助策略】可以查看所有的审计信息。

# 软件管理

LeagView能够对企业软件进行全生命周期管理，一方面，管理员可以录入软件订单，对用户或者部门进行授权使用，然后通过软件商城发布软件，或使用软件分发强制终端安装，最后可以统计软件的使用时长，从而提高企业软件运维管理的效率，实现企业软件正版化管理。

另一方面，LeagView可以采集已安装软件、软件安装包和绿色软件的信息，并做相应的管控（包括阻止运行、禁止安装、远程删除和卸载），实现对系统内软件安装情况的感知，对违规安装或运行软件行为的管控，对危险软件的卸载，对绿色软件的删除等，从而实现企业软件标准化的管理，保障终端的软件环境合规、安全，免于流氓软件的安装骚扰。软件管理整体思路如**错误!未找到引用源。**所示

## 软件资产与授权管理

软件信息与授权管理页面提供软件信息查询、软件分类、软件信息录入、软件授权管理等功能。

软件授权管理的过程是：先采集终端已安装的软件信息，然后录入商业软件订单，最后根据订单信息进行授权。

### 软件信息与授权管理

进入【软件管理|软件资产与授权管理|软件信息与授权管理】，分别按照【软件】、【绿色软件】、【软件安装包】、【操作系统】四个TAB展示软件信息。

除了可以按照信息列表的列名查询相关的软件信息外，点击每个类型的便签也可以快速筛选需要查看的软件类型。

* 软件分类与标签

收费类型、行业类型、软件类型，既是软件的分类，也是软件的标签。同类型的标签，一个软件只能拥有一个。例如一个软件只能有一个软件类型的标签。点击更多，可以展开标签框，显示全部本模块全部标签。

除了系统内置的软件类型与标签外，管理员可以增加新的类型和标签，点击每个类型后面的进入编辑窗口，此时可以新增或者删除分类。

选择一个或者软件，点击，可以将选中的软件划分收费类型；点击，可以将选中的软件划分行业类型；点击，可以将选中的软件划分软件类型。

* 软件信息录入

点击，进入新增软件配置页面，配置软件名称、软件编号、厂商信息、软件收费类型、行业类型、软件类型等，然后点击增加，或者添加至进程组，关联软件的进程。最后点击保存完成软件新增。

* 授权管理

在软件信息列表中，选中一个或多个软件，点击授权管理，进入软件授权管理页面，此时可以对该软件进行取消授权、通过应用范围授权、通过序列号授权、禁用软件商城授权。

智能授权：不需要关联软件订单；

手工授权：需要关联软件订单。

### 软件安装列表

管理员可以查看所有终端已安装的软件，可按照软件或者设备的视角查看。

进入【软件管理|软件资产与授权管理|软件安装列表】，分别点击【软件安装列表】、【按软件查看】、【按设备查看】可以切换不同的查看视角。

* 导出软件安装报表

在不同的查看列表中，点击导出，可以将列表中的数据导出到Excel文件中。

### 软件订单管理

软件订单是商业软件授权的基础，做软件授权管理时，需先录入商业软件的订单。

进入【软件管理|软件资产与授权管理|软件订单管理】。

管理员可以在本页面查看和管理商业软件的订单，并可以查看当前订单的许可数、安装数、授权数、剩余许可数量等，了解软件授权的总体情况。

* 新增订单

点击新增订单来增加一个新的订单

在订单的填写中，管理员需要编辑如下必填信息：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 软件名称 | 订单中软件的名称，只能从已采购的软件和软件信息库添加 |
| 软件版本 | 选择已被识别的版本号 |
| 收费类型 | 可以根据软件的收费情况，配置收费类型。如无特别需要，可以仅创建一种收费类型“商业软件”，并将所有订单软件均归于这一收费类型 |
| 行业类型 | 可以根据软件的使用领域，配置行业类型。通常可配置为“通用软件”和“xx行业专用软件”，例如Photoshop为设计专用软件，Office为通用软件 |
| 授权类型 | 可以根据企业自身的需要，配置授权类型。如无特别需要，可以仅创建一种授权类型，并将所有订单均归于这一授权类型 |
| 授权子类型 | 可以根据企业自身的需要，配置授权子类型。如无特别需要，可以仅创建一种授权子类型，并将所有订单均归于这一授权子类型 |
| 进程信息 | 关联软件的进程名称 |
| 同类软件信息 | 关联同类软件 |
| 软件采购信息 |  |
| 订单编号 | 软件采购订单编号 |
| License信息 |  |
| 许可数量 | 允许授权的设备数量 |
| 许可类型 | 无序列号：无需关联序列号，直接授权；有序列号：需要录入序列号信息，授权时，需要关联对应的序列号 |
| 序列号信息 | 对于有序列号的许可类型，需要录入所有序列号 |
| 授权机器信息 | 展示已授权的设备，也可以在此直接对设备授权 |

* 查看订单

进入【订单总表】TAB，可以按照订单编号、软件编号、软件名称等查询订单信息。点击订单编号超链接，可以进入订单编辑页面修改订单。

* 导出报表

管理员也可以通过导出【订单总表】模块的信息，达到导出Excel文件，实现简单的正版化报表的效果。

## 软件标准化管理策略

LeagView可以管控终端软件的安装与卸载、设置已安装软件黑白名单、绿色软件管控、配置必须安装的软件，从而实现企业软件的标准化管理。

管理员给终端或者用户下发企业软件标准化管理策略，可以实现企业软件标准化管理，进入【软件管理|软件标准化管理策略|软件安装与卸载】，点击增加策略，进入策略配置页面。

* 软件安装与卸载管控

进入【软件管理|软件标准化管理策略】，点击增加策略，进入【软件安装与卸载】配置页面。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 软件安装包信息采集 | 分为“全盘扫描”和“运行时采集”，勾选“全盘扫描”在下发策略时进行全盘扫描采集软件安装包信息；勾选“运行时采集”则在运行 |
| 软件卸载管理 | 勾选“审计”将审计所有软件卸载行为；勾选“禁止”将禁止所有软件卸载行为 |
| 软件安装管理 | 勾选“审计全部”，可以审计所有软件的安装行为；勾选“禁止”可以禁止所有软件的安装；如需要允许已安装软件的自动升级，但禁止其他软件的安装，可以同时勾选“禁止”和“允许软件自动升级”；如需要限定部分可安装或不可安装的软件，可以同时勾选“禁止”和“软件安装黑白名单”，并在下方添加黑白名单信息；如需仅对黑白名单软件的安装行为进行审计，可以取消勾选“审计全部”并勾选“仅审计黑白名单软件安装” |

* 配置已安装软件黑白名单
  + - 进入【软件管理|软件标准化管理策略】点击增加策略，进入【已安装软件黑白名单】配置页面。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 黑白名单模式选择 | 选择黑名单，终端如果安装了黑名单中的软件，则执行违规处理；选择白名单，终端如果安装了不在白名单中的软件，则执行违规处理 |
| 违规处理 | 选择“审计”则对所有违规行为进行审计；选择“禁止运行”，则禁止违规软件运行；选择“自动卸载”，则自动卸载违规软件 |
| 终端提示信息 | 选择【不弹出提示信息】当发生违规行为后助手不弹窗提示；选择【弹出自定义提示信息】，在右方输入自定义提示内容，当发生违规行为后助手弹窗提示自定义的提示内容；选择【弹出缺省提示信息】当发生违规行为后助手弹窗提示系统内置的内容；选择【弹出本策略全局提示信息】当发生违规行为后助手弹窗提示本策略【基本信息】中客户端全局提示信息的内容； |

【注意】软件黑白名单审计和自动卸载当新策略下发后立即执行一次，以后每隔5小时执行一次，或者安全助手重启后开始执行。

* 绿色软件管控

进入【软件管理|软件标准化管理策略】点击增加策略，进入【绿色软件】配置页面。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 绿色软件信息 | 分为“全盘扫描”和“运行时采集”，选择“全盘扫描”在下发策略时进行全盘扫描采集绿色软件安装包信息；选择“运行时采集”则在运行绿色软件安装包时采集软件安装包信息 |
| 绿色软件运行 | 勾选“审计全部”，可以审计所有软件的安装行为；勾选“禁止”可以禁止所有软件的安装；如需要限定部分可安装或不可安装的软件，可以同时勾选“禁止”和“绿色软件安装黑白名单”，并在下方添加黑白名单信息；如需仅对黑白名单软件的安装行为进行审计，可以取消勾选“审计全部”并勾选“仅审计黑白名单绿色软件” |
| 终端提示信息 | 选择【不弹出提示信息】当发生违规行为后助手不弹窗提示；选择【弹出自定义提示信息】，在右方输入自定义提示内容，当发生违规行为后助手弹窗提示自定义的提示内容；选择【弹出缺省提示信息】当发生违规行为后助手弹窗提示系统内置的内容；选择【弹出本策略全局提示信息】当发生违规行为后助手弹窗提示本策略【基本信息】中客户端全局提示信息的内容； |

* 设置必须安装软件

进入【软件管理|软件标准化管理策略】，点击增加策略，进入【必须安装软件】配置页面。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 增加软件组 | 软件组内的软件之间为或关系，只要安装一个即认为符合软件组的要求；软件组之间为与关系，如有未安装的则视作违规并执行违规处理 |
| 违规处理 | 勾选择“审计”可以对所有未安装必须安装软件的用户或设备信息进行记录；勾选择“自动安装”则对未安装必须安装软件的终端执行软件自动安装 |
| 终端提示信息 | 选择【不弹出提示信息】当发生违规行为后助手不弹窗提示；选择【弹出自定义提示信息】，在右方输入自定义提示内容，当发生违规行为后助手弹窗提示自定义的提示内容；选择【弹出缺省提示信息】当发生违规行为后助手弹窗提示系统内置的内容；选择【弹出本策略全局提示信息】当发生违规行为后助手弹窗提示本策略【基本信息】中客户端全局提示信息的内容； |

【注意】：

1、当勾选自动安装后，每组软件中从软件仓库添加的软件才会自动安装，从软件组中自动选择符合要求的软件进行安装，安装成功后停止安装；自定义的软件无法安装，当软件组中全部为自定义软件时，请手动修复。

2、必须安装软件当新策略下发后立即执行一次检查，以后每隔5小时执行一次，或者安全助手重启后开始执行。

进入【软件管理|软件标准化审计信息】可以查看本策略产生的审计信息，并导出为Excel的文件以分析。

策略示例1

需求：企业内部根据IT部门管理规定，为了规范企业内容的软件，禁止私自安装软件，只允许特定的渠道下载安装软件。

配置步骤：

1. 配置软件标准化管理策略，进入【软件安装与卸载】配置页面中，配置如图 6‑1所示：

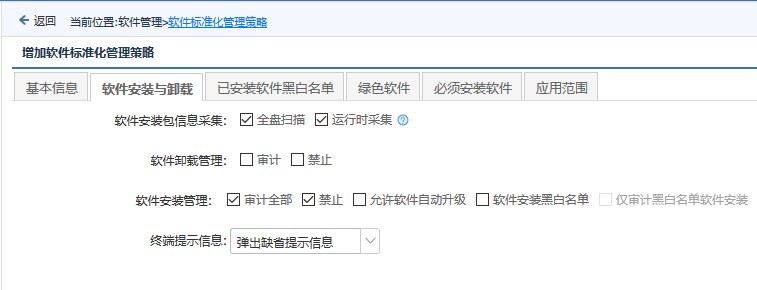


图 6‑1 软件标准化管理策略-安装与卸载

1. 再配置软件发布策略，将允许安装的软件发布给用终端用户，终端用户只能通过软件商城下载安装软件，在资源管理器双击运行无法安装，如所示

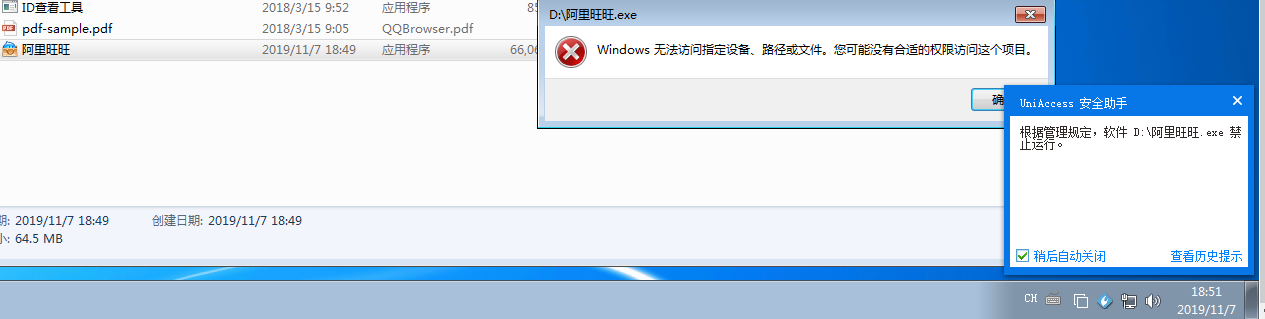


图 6‑2 禁止安装软件

**策略示例2**

需求：企业未购买Microsoft Office软件，为避免受到软件厂商的指控，需要及时发现和自动卸载该软件。

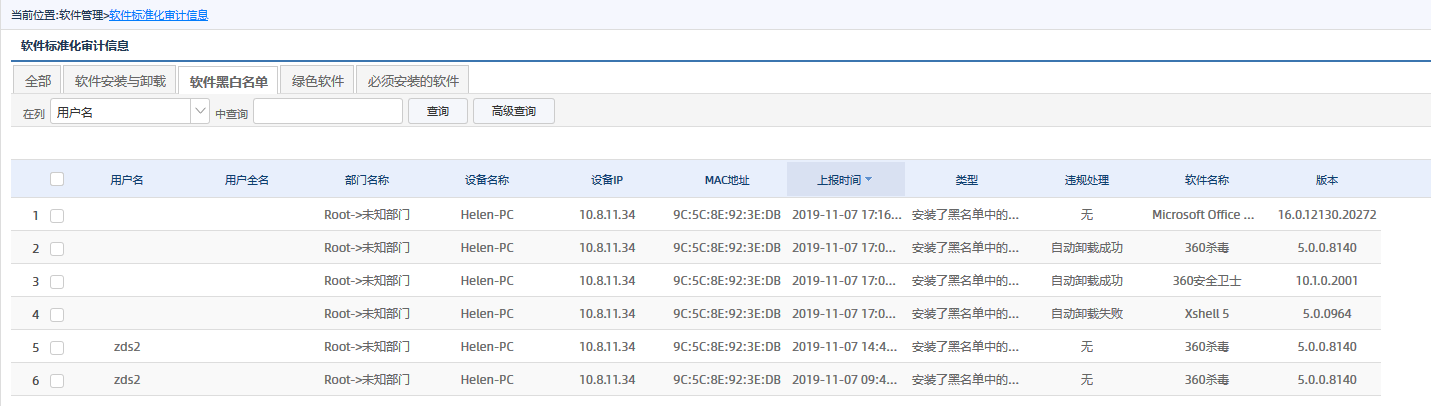
配置步骤：

1. 配置软件标准化管理策略，进入【已安装软件黑白名单】配置页面中，选择【以下为黑名单软件，如果安装了黑名单中的软件，则执行违规处理】，点击增加，将Microsoft Office相关的软件添加到列表中（软件名称要与Windows控制面板中已安装的软件名称一致，可以从采集到的软件信息库直接添加）；违规处理：勾选【审计】和【自动卸载】，配置如图 6‑3所示：



图 6‑3 软件管理策略-软件黑名单

1. 进入【应用范围】配置页面，添加策略应用范围将策略下发到指定的终端和用户
2. 违规软件被处理后，进入【软件管理|软件标准化审计信息】可以查看被处理结果的审计信息



## 软件商城

管理员可以将软件发布至软件商城以供终端用户下载，也可以通过软件分发策略，将软件安装包推送给终端强制安装，或推送命令以达到统一执行命令的效果，如远程批量卸载软件等，从而实现企业软件运营管理。

配合软件标准化管理策略，可以使软件分发和软件商城成为终端获取软件的唯一途径，类似于IOS里的App Store.

### 软件仓库

软件仓库是软件商城的软件安装包后台库，管理员发布软件前，需要上传软件安装包和软件信息到软件仓库中。

进入【软件管理|软件商城|软件仓库】**。**此页面可以看到已经上传的软件信息，点击增加，为软件仓库添加一款新的软件。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 软件基本信息 |  |
| 上传软件 | 将软件安装包从本地上传至服务器，点击获取软件信息，系统将自动获取软件安装包里的软件名称、软件版本、厂商信息等 |
| 上传图标 | 上传96\*96像素的图标，如果不符合，将会强制转换大小，该图标会在软件商城显示，如果未上传，会使用默认的图标 |
| 软件名称 | 软件安装后显示的名称，【注意】此处的名称要与软件安装后操作系统显示的名称一致，否则影响软件商城中卸载软件的功能 |
| 软件版本 | 软件版本号 |
| 厂商信息 | 软件厂商名称 |
| 管理员评级 | 管理员为该软件进行评级，方便用户参考 |
| 内存要求 | 填写软件内存要求信息 |
| 软件类别 | 为软件分类，以便在软件商城分类展示 |
| 置顶时长 | 将软件在软件商城置顶显示时长 |
| 安装命令 | 填写软件安装时执行的一些命令，可以不填写，不填写表示不加任何参数直接安装 |
| 卸载命令 | 填写软件卸载时执行的一些命令，可以不填写，不填写表示不加任何参数直接卸载 |
| 适用平台 | 勾选软件适用的操作系统平台，在非适用平台内的操作系统不可安装该软件 |
| 允许安装包另存 | 配置是否允许用户保存软件商城下载的安装包 |
| 禁止软件卸载 | 勾选禁止后，助手端软件商城不提供本软件的卸载功能 |
| 使用一下账户运行工具 | 某些软件需要系统管理员的权限才可以正常安装使用，在此可以配置安装软件商时使用的账户类型 |
| 更新日志 | 填写新版本的更新信息 |
| 安装检测条件 | 当满足安装表达式时，进行安装，一般不需要配置 |
| 安装成功检测条件 | 当满足表达式时表示安装成功，助手会根据软件名称自动检查，但如果无法自动检查，可以配置一下安装成功条件，以便助手正确识别软件是否已成功安装 |

软件仓库中的软件可以通过6.3.2软件发布策略被发布至软件商城。

### 软件发布策略

管理员可以在后台定期发布和更新软件商城的软件。

进入【软件管理|软件商城|软件发布策略】**。**

进入【软件发布】配置页面，点击，管理员可以将软件从6.3.1软件仓库发布至软件商城；点击，将管理员本地的软件发布至软件商城，以供特定用户或设备下载安装。管理员也可以配置终端安装软件后，安装包的处理方式、软件发布后助手是否弹窗提醒、终端的本地软件是否允许卸载。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 下载安装包处理方式 | 选择助手从软件仓库下载安装包后的处理方式 |
| 启用本地软件管理 | 勾选启用后，软件商城会显示本地已安装软件TAB |
| 软件管理禁止卸载 | 勾选后，软件商城中的本地软件管理不提供卸载功能，用户需要到操作系统自带的控制面板中卸载 |
| 上传配置文件 | 软件相关的配置文件，需咨询软件厂商提供 |
| 消息通知 | 勾选后，当管理员发布新的软件时，助手弹窗通知用户前往软件商城下载安装 |
| 软件列表 | 添加需要发布的软件，有两种方式，一种是点击增加，上传新的软件安装包，另一种是点击选择要发布的软件，从软件仓库中选择已有的软件 |

**策略示例：**

需求：企业原本使用FTP服务器存放常用的办公软件，用户可以登录FTP进行下载安装，目前企业内部已使用上千款软件，管理员维护起来很困难，用户很难在FTP上找到适合自己使用的软件，而且同类型的软件有多款，也不清楚哪些比较受欢迎，哪些软件有问题，管理希望有个统一的软件门户，用户可以轻松找到其需要的软件，已经对软件做一些评价，以便管理员可以淘汰掉一些口碑不好的软件。

配置步骤：

1. 将原FTP所有的软件安装包例如LeagView软件仓库中并做分类，并使用软件发布策略，按照用户部门，分发不同类型的软件。用户不需要再登录FTP，只需要打开助手的软件商城，即可看到适合自己的软件并下载安装，用户对使用软件后作出评价，以供管理员参考。

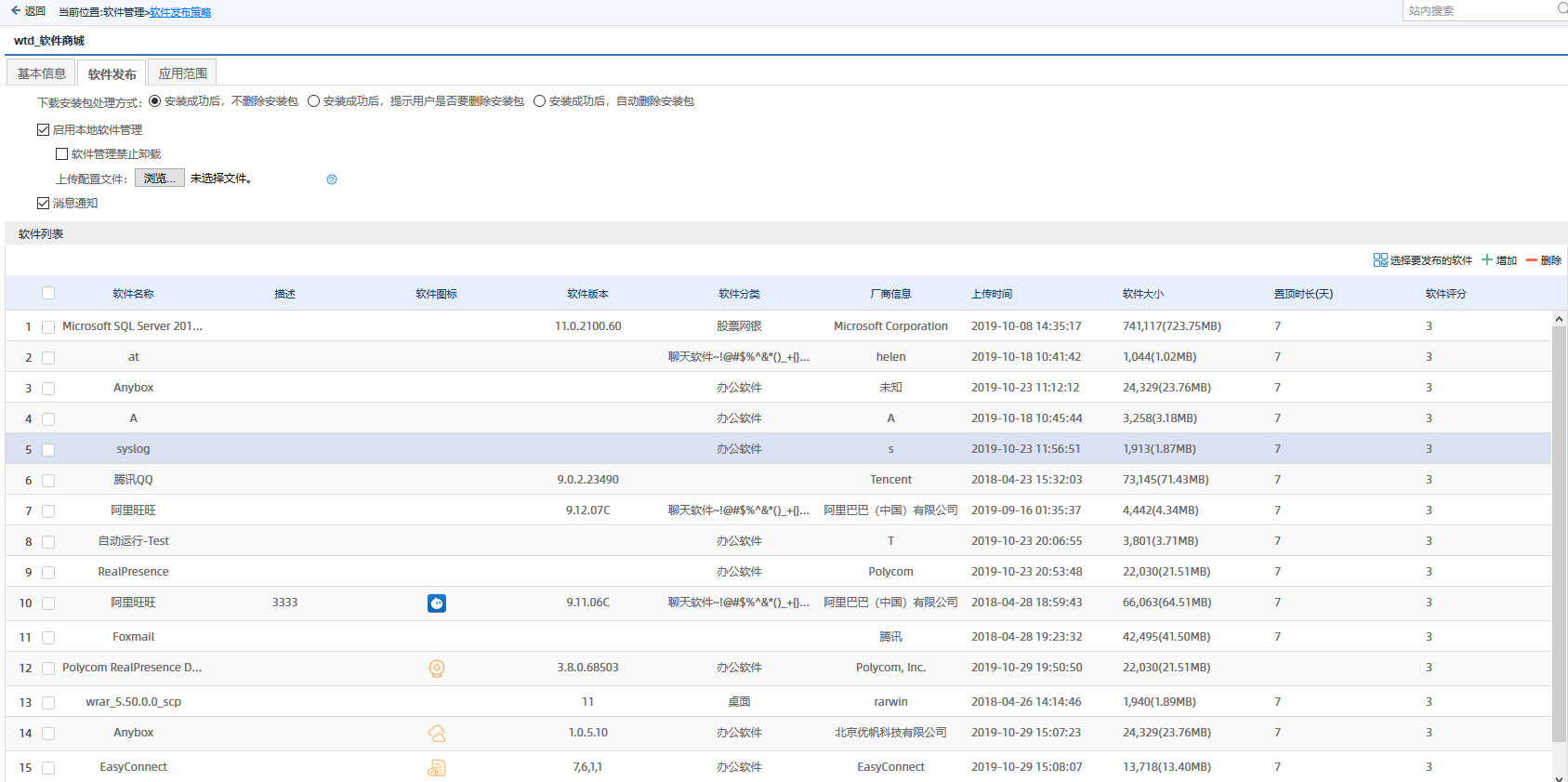


图 6‑4 软件发布策略配置

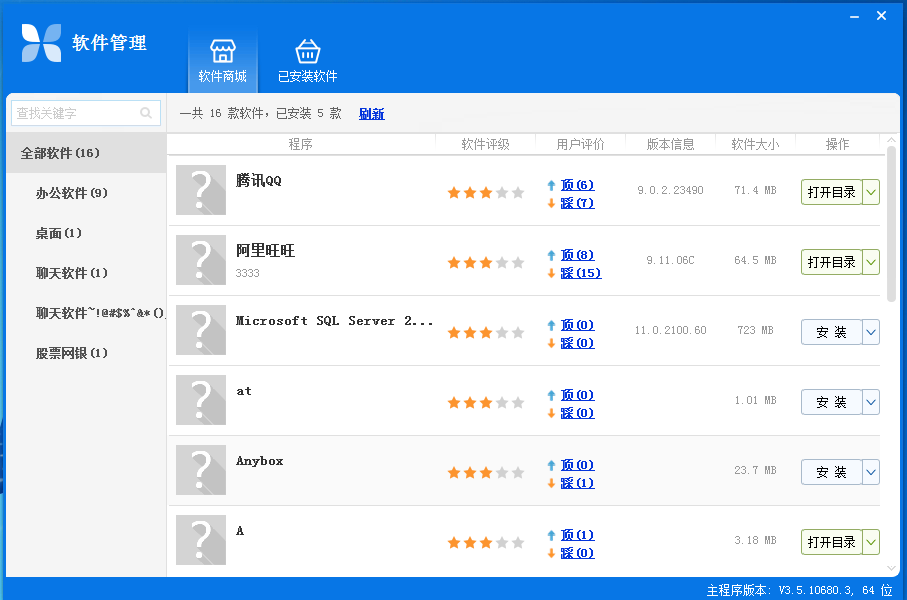


图 6‑5 助手软件商城

### 软件升级策略

LeagView支持当特定用户或终端被检测到装有旧版本的软件时，在软件商城中显示该软件的新版本以供其更新。

进入【软件管理|软件商城|软件升级】**。**进入策略配置，新增一条升级规则

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 软件基本信息 |  |
| 软件升级信息 | 点击选择要升级的软件，选择该软件的新版本或者升级包，下方会自动显示该软件名称与软件版本信息 |
| 软件升级条件 | 下列软件列表作为升级条件，满足条件时，助手软件商城显示升级按钮，一般选择需要升级的软件的旧版本，当然也可以选择其它软件 |
| 从样本中获取 | 从终端已安装的软件信息中选择 |
| 增加 | 手动填写软件信息 |
| 删除 | 删除选中的软件信息 |

【注意】配置本策略之前，需要管理员先发布软件的最新版本到软件商城，参见6.3.2软件发布策略，配置升级策略后，如果终端符合升级条件，用户在软件商城看到的新版本的软件后面显示的是升级按钮。

**策略示例：**

需求：软件商城的某款软件A已有新版本，并希望用户可以通过软件商城进行升级。

配置步骤：

1. 将软件A的新版本发布到软件商城，并将软件A的旧版本取消发布（或者保留就版本）
2. 配置软件升级策略，使该软件在软件商城显示可升级，如图 6‑6所示



图 6‑6 软件升级策略配置

## 软件分发

LeagView支持将软件安装包、脚本、文件等分发到终端上，为了适应多种多样的网络环境和使用需求，软件分发可以灵活配置分发的客户端环境、分发时间、执行时间、执行方式、分发条件、安装检测条件，并且对于大文件的分发，考虑到带宽消耗的问题，可以使用下载中继系统解决，节省文件下载过程中消耗过多的带宽，从而提高企业软件运维效率。

配合软件标准化管理策略，可以使软件分发和软件商城成为终端获取软件的唯一途径，类似于IOS里的App Store

### 软件分发任务

进入【软件管理|软件分发|软件分发任务】。

管理员可以上传软件，分发给特定终端并令其安装；或选择软件，令特定终端卸载。通过软件分发，管理员可以集中地为指定范围内的设备安装各种软件，这些软件可以是标准的Setup安装包、msi安装包，也可以是管理员自己定义的安装脚本，或exe、bat、com格式的可执行文件。

软件分发功能要求目标终端必须安装了安全助手，才能分发成功。

LeagView软件分发功能使用步骤如下：

（1）设置软件分发需要的中继设备（可选，参见12.7.9中继设备管理）；

（2）配置软件分发任务；

（3）查看软件分发任务执行结果。

管理员可以配置该策略的如下参数：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 分发环境 | 客户端的系统环境。选择指定的客户端系统作为分发环境时，策略只会应用到所选系统的终端 |
| 分发时间 | 定义该该策略中的软件何时分发。可以选择全部时间段均可分发，也可以选择只在指定时间段内分发 |
| 分发文件 | 定义该策略执行的动作：安装或卸载。若安装，则管理员需要上传该软件的安装包；若卸载，则管理员需要填写该软件的软件名，管理员也可以从系统已收集的软件信息中选择软件。本渠道内的卸载是非静默的 |
| 执行时间 | 定义软件下载的时间和软件安装/卸载的时间，并配置是否在下载、安装/卸载时，助手端右下角弹出提醒 |
| 执行方式 | 定义该软件在下载后自动安装还是手动安装，以及安装权限和执行的命令。管理员可以通过执行命令的配置实现卸载终端软件的效果 |
| 下载配置 | 定义下载的等待时间、每日重试次数和下载持续周期，实现助手端的错峰下载和下载失败后重新下载。本模块的配置可以减小对网络和终端的影响，如需减轻对服务器的影响，请配置中继，参见12.7.9中继设备管理 |
| 软件分发条件 | 管理员可以定义：当终端安装有如下软件时，方可向其执行本策略 |
| 终端检测条件 | 管理员可以定义：当助手端满足安装检测条件的表达式时，进行安装；当助手端满足安装成功检测条件的表达式，表示安装成功。通常情况下无需配置 |

进入【桌面管理|软件管理|软件分发执行信息】**，**管理员可以查看该策略的执行情况，在此页面可以实时查看分发任务的执行情况，包括分发完成率和异常率等。

**策略示例：**

需求：企业内部要求员工办公电脑必须安装杀毒软件，但仍有许多人未安装，需要强制统一安装。为了避免分发软件安装包时过多占用带宽，或者在员工办公期间安装软件影响办公，需要在空闲时段才下载和安装，例如中午午休的时段。

配置步骤：

1. 配置软件分发任务，下载时段和安装时段都在中午的时段，如图 6‑7所示：



图 6‑7 软件分发任务配置

1. 查看软件分发执行信息，查看分发任务的按成率和异常率，对于异常的终端进行及时处理。如图 6‑8所示：



图 6‑8 软件分发执行信息

## 工具管理

LeagView支持提供工具以供助手端反复多次地快速使用。助手端可以通过工具以实现文档相似度比较、文档聚类、重要文档备份迁移、粉碎文件、安全U盘浏览等效果，提高员工的工作效率。

### 工具仓库

工具仓库负责存储工具箱所需的程序包。

进入【软件管理|工具箱|工具仓库】。

系统已经内置常见的文件删除、垃圾清理安全U盘等工具，管理员可以在本模块上传工具。

【注意】该页面除了展示工具的基本信息外，还会统计工具的下载总数和使用总数，这两个数值按照使用时间统计，在查询栏配置工具使用时间即可查看在该时间范围内工具的下载总数和使用总数。

点击增加，添加新的工具。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 上传工具 | 管理员可以对32位、64位系统分别上传同一工具的不同版本，也可以上传通用版本的工具。上传工具后，管理员需要点击获取工具信息，输入工具名称和工具版本方可上传该工具 |
| 上传图标 | 上传工具的图标，该图标会在助手端的工具箱显示，如果不上传将使用默认图标 |
| 工具名称 | 工具的名称，在工具箱内也会显示该名称 |
| 工具类别 | 配置工具的分类，以便在助手端的工具箱可以按照分类显示 |
| 工具版本 | 填写工具的版本号，以便后续升级维护 |
| 描述 | 对工具简明扼要的描述 |
| 工具使用要求 | 可以指定工具在初次使用和每次使用前后执行相关的脚本，支持bat、vbs、Braise脚本 |
| 适用平台 | 勾选工具适用的操作系统平台 |
| 执行命令 | 运行工具时执行相关的命令 |
| 使用以下账号运行工具 | 为工具运行指定账户权限，有些特殊的工具需要系统的权限，可以指定SYSTEM账户 |

在工具仓库查询页面，选中某一个工具，点击按钮，进入工具升级配置页面，对原工具信息进行编辑，替换或删除原工具程序包，上传新版本的工具程序包。

### 工具发布策略

工具发布后，才会在相应的终端助手界面上显示工具TAB，终端用户才可以使用工具。

进入【软件管理|工具箱|工具发布策略】。在工具列表中配置需要发布的工具，有两种方法添加工具，一是点击选择需要发布的工具，从工具仓库中选择已经配置好的工具，而是点击增加，新增加一个工具，增加工具的方法步骤参考6.5.1工具仓库。

管理员可以配置一个或多个工具仓库里的工具，将其发布至助手的工具箱以供助手端使用。

### 工具箱

将工具发布策略下发到对应的终端后，在助手端即可显示工具箱TAB，如下图所示：



工具箱界面左侧是全部工具的分类，上方显示工具统计信息，并提供搜索工具功能。中间展示工具的图标和名称，以及工具的描述。点击右上角的下载设置，配置工具下载的保存路径。

图标表示工具未下载，点击后会自动下载，然后显示工具相应的图标。

系统内置工具介绍：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 文件特征采集 | 提取文档中权重最大的前N个关键词的集合作为文件特征，用于文件聚类,并将提取结果上传到系统后台服务器 |
| 文件删除 | 类似文件粉碎工具，可以使用该工具删除一些顽固的病毒木马文件，或者彻底删除一些机密文件，使其无法恢复 |
| 文件DNA采集 | 提取文档中所有的关键词通过Hash映射出DNA的值，用于比较两个文件内如的相似度，并将提取结果上传到系统后台服务器 |
| 系统优化 | 对系统痕迹进行清理，优化运行效率 |
| 文档迁移 | 对重要文档进行备份、迁移 |
| 大文件查找 | 查找硬盘中占用空间较多的大文件 |
| 截图工具 | 用于截图 |
| 安全U盘 | 安全U盘浏览器，配合安全U盘控制策略使用 |
| 垃圾清理 | 扫描系统垃圾并清理 |

进入【软件管理|工具箱|工具使用审计信息】。管理员可以在本页面查看和导出助手采集的终端用户使用工具的审计信息。

## 软件使用时长管理

软件使用时长管理主要通过统计时间阈值，提示终端用户，比如提示员工专心办公，切勿娱乐过久。另外，通过分析软件使用时长统计数据报表，可以为了解哪些软件使用率最高，为商业软件采购提供依据。

配置软件使用时长监控列表

进入【软件管理|软件使用时长管理|软件使用时长管理策略】 ，在【策略配置】页面可以配置软件使用时长管理策略，如策略全局配置、编辑软件使用时长管理列表等。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 策略全局配置 |  |
| 统计时间间隔 | 多久统计一次，如：10分钟，30分钟 |
| 上报时间间隔 | 多长时间汇报一次统计记录。如：30分钟，1个小时 |
| 编辑软件使用时长管理列表 |  |
| 类型 | 上网浏览：统计终端用户浏览网页的时长；应用程序：统计终端用户使用软件的时长 |
| 网站列表 | 当类型为上网浏览时，需要配置监控的网站库列表 |
| 进程组 | 当类型为应用程序时，需要配置进程组，进程组中“Office”和“即时聊天工具”属于内置进程组，其中：即时聊天工具主要包含QQ、TIM、微信WeChat、腾讯通RTX，Office主要包含Word、Excel、PPT、Adobe阅读器、福昕阅读器、WPS |
| 提示阈值 | 定义持续多久提示终端用户 |
| 提示内容 | 填写提示终端用户市的提示内容,如请专心办公，切勿娱乐过久 |

进入【软件管理|软件使用时长管理|软件使用时长审计信息】查看相应审计信息，支持查询、高级查询、导出等。

进入【综合报表｜数据分析报表 | 软件使用时长统计报表】查看分析报表，支持查询、统计、多种形式展示、导出、打印等。

**策略示例：**

需求：为了提高员工工作效率，HR部门需要收集和分析员工使用办公软件的时长以及上网娱乐的时长。

配置步骤：

1. 配置软件时长管理策略，添加一条类型为应用程序的监测规则，用于统计常用办公软件时长，再添加一条类型为上网浏览的规则，用于监测员工上网娱乐时长，如图 6‑9所示

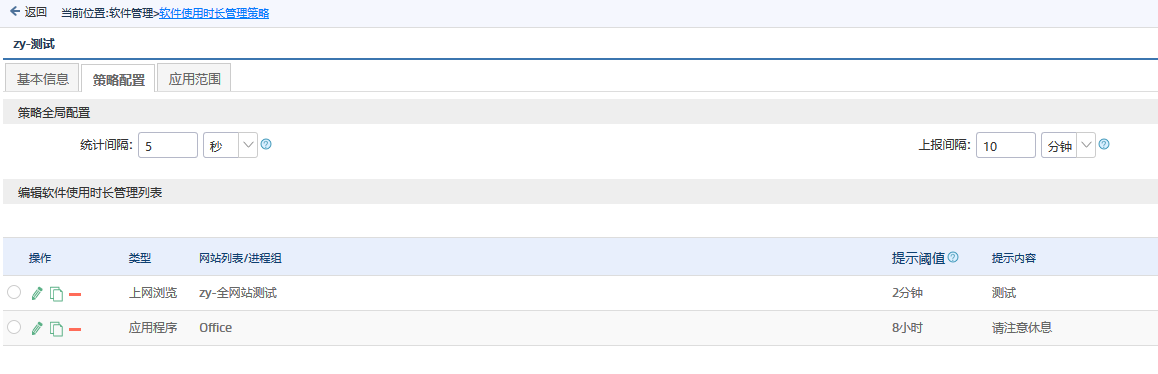


图 6‑9 软件使用时长策略配置

1. 进入【综合报表｜数据分析报表 | 软件使用时长统计报表】查看分析报表并导出。

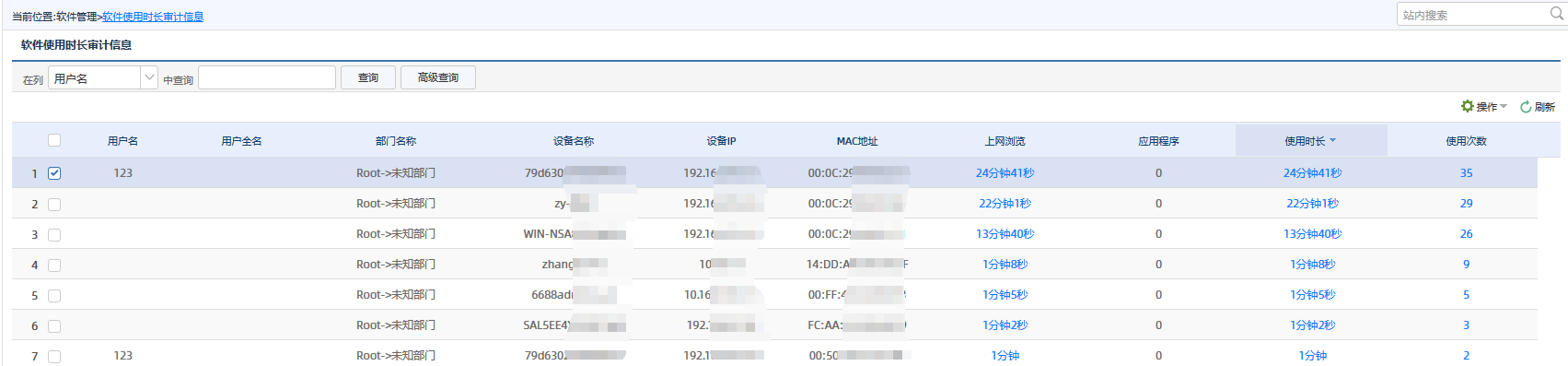
图 6‑10

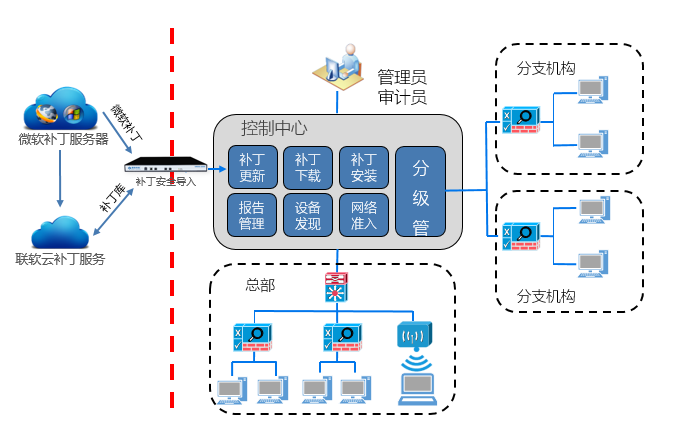
图 6‑10 软件使用时长审计报表

# 补丁管理

在IT维护中保证所有 Windows 终端总是及时打上最新的补丁是一个艰巨的任务，IT管理员为此耗费了大量精力，而效果很难达到预期，为此联软提供了微软补丁云服务，简称“云补丁”。云补丁是联软对用户提供的一个高附加值IT服务，用户通过LeagView的补丁管理模块使用这个服务，简单、高效、自动的确保所有被管理的 Windows 终端总是及时打上最新的补丁，全过程完全不需干预。

LeagView补丁模块可以从微软的WSUS服务器下载补丁，也可以从联软云补丁服务器下载补丁。LeagView能够实现快速、准确、可用的微软补丁检查，并根据终端电脑的补丁检查结果与管理员定制的补丁分发策略下发补丁或卸载补丁，支持分级管理，实现全网漏洞与补丁的全面管理，及时为终端打上最新的补丁，避免终端主机遭受恶意的攻击。

联软的补丁管理解决方案如下图所示：



## 微软WSUS策略

LeagView能和WSUS服务器集成，通过为各个客户端设置WSUS自动更新策略，使客户端通过WSUS服务器自动更新微软补丁包。

在【补丁管理|微软WSUS策略|微软WSUS策略】中配置补丁包从微软网站下载策略。策略配置项说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| WSUS服务器IP地址/域名 | 填写WSUS服务器IP地址或者域名，如果LeagView服务器能够访问互联网，可以使用互联网的WSUS服务器，如微软的服务器；如果不能访问互联网，需在内网部署的WSUS服务器 |
| 补丁更新策略配置 | 按WSUS管理策略更新补丁：选择此方式时，系统将按照WSUS的策略以及本策略中配置的客户端执行方式进行补丁更新，客户端补丁包安装方式仅支持Windows7及以下版本，因新版本的Windows补丁相关注册表配置已去掉；按补丁管理平台策略更新补丁：选择此方式时，将按照LeagView的补丁管理平台策略进行更新 |
| 启用补丁管理平台统计终端补丁安装情况 | 勾选后，助手将终端的补丁安装信息上报到管理平台，统计安装情况 |

## 微软补丁库管理

LeagView补丁模块通过连接联软云补丁服务器，下载经过联软人工验证的补丁后，通过补丁管理平台的微软补丁更新策略，将补丁一键更新到对应的终端上，并生成漏洞修复报表。

【注意】在使用联软云补丁服务时，需确保助手客户化选项中已勾选“微软补丁云服务”。

### 微软补丁下载选项

微软补丁下载选项，即是后台补丁模块从云补丁下载情况及下载的代理服务代理配置。

进入WEB控制台选择【补丁管理|微软补丁库管理|微软补丁下载选项】，管理员可以在页面上半部分进行服务器配置，在下半部分查看服务器的补丁更新信息。配置信息如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 启用代理服务器 | 默认情况下后台服务器会直接访问联软云补丁服务器，当后台服务器无法直接访问联软云补丁服务器时，可以设置代理服务器进行代理转发 |
| 补丁文件确认 | 勾选系统自动确认后，新下载的补丁，其补丁的确认安装状态会被修改成“系统自动确认”。勾选等待管理员手工确认，新下载的补丁，其确认状态为“管理员未确认”。该选项用于和补丁策略中的“补丁文件需要确认”的选项联动。 |

点击立即更新，LeagView后台服务器会自动连接联软云补丁服务器去下载补丁库信息。下载成功后，会在下方显示最新的补丁库信息。

### 微软补丁更新策略

LeagView后台支持微软补丁的分发，使助手终端即时更新客户端漏洞，保证终端的安全；微软补丁更新策略的配置。

进入WEB控制台选择【补丁管理|微软补丁库管理|微软补丁更新策略】，点击增加策略，管理员可以选择对范围内终端配置不同的更新策略，包括安装模式、下载时间、更新范围、更新来源等。策略配置参数说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 安装模式 | 自动下载，自动安装：到了有效的下载时段，安全助手自动去下载后台的补丁，并自动安装已经下载好的补丁；自动下载，手动安装：到了有效的下载时段，安全助手自动去下载后台的补丁，终端用户在安全助手的“补丁扫描”界面点击“立即修复”按钮后安全助手开始安装补丁；手动下载，手动安装：：终端用户在安全助手的“补丁扫描”界面点击“立即修复”按钮后安全助手开始下载所需的文件并进行安装 |
| Service Pack 安装策略 | 当勾选相应的操作系统名称时，表示要求该系统升级到最新的 SP。例如：勾选了 win8，那么当 win8 发布了它的 SP1 的时候，安全助手  会自动将 win8 系统升级到 SP1，同样的，再自动升级到 SP2，SP3 等。如果不勾选，则表示维持当前 SP，并在此 SP 基础上进行常规的补丁更新，建议不要选择安装最新的操作系统 SP，一般 SP 都是几百 兆，下载和安装都很耗时，而且安装过程中容易出问题 |
| 扫描轮询时间 | 安全助手自动检测补丁安装情况周期 |
| 更新范围 | 更新范围可以指定大于特定补丁级别和补丁发布的天数的补丁，也可以指定为某几个特定的补丁 |
| 更新来源 | 指定终端下载所需要的补丁文件的来源，可以从Microsoft补丁公有云下载，也可以从LeagView补丁私有云下载，或者其它指定的WSUS服务器，如果选择了多个补丁下载源，这些下载源的选择是有先后顺序的。排在前面的先选用，如果下载成功，则忽略后面的下载源，如果下载失败，则继续选用下一个下载源 |
| 指定安装参数 | 为特殊的补丁使用指定的安装参数，一般情况下不需要配置 |
| 补丁文件需要确认 | 当配置补丁文件需要确认时，后台只会向安全助手发布“确认安装状态”为“系统自动确认”和“管理员手工确认”的补丁，对于“管理员未确认”的补丁，安全助手不会安装也不会显示漏洞，管理员可以在【补丁管理|微软补丁库信息】页面将修改补丁文件的确认状态。如果配置补丁文件不需要确认，则无论补丁状态是不是已经确认，都直接安装 |
| 安装失败重试次数 | 并不是每次安装补丁都能一次性安装成功，在此可以配置重试次数 |
| 启动蓝屏修复 | 当出现安装补丁所导致蓝屏时，本选项可还原对应的安装，修复蓝屏。注意：本选项要在安装之前下发 |

补丁文件下载，尤其是大的文件下载时，需要消耗较多的带宽资源，，可以通过配置中继进行分流下载，点击中继配置超链接，配置下载中继服务器。

进入WEB控制台选择【补丁管理|微软补丁库管理|补丁安装详细信息】。管理员能以列表形式查看或导出具体到终端的补丁安装信息。

进入WEB控制台选择【补丁管理|微软补丁库管理|补丁下载安装信息】。管理员可以根据组织架构，查看、导出或打印补丁的安装情况。

**策略示例：**

需求：内网Windows终端需要及时打上最新的补丁并自动下载安装。

配置步骤：

1. 确保LeagView后台服务器能够访问联软云补丁服务器
2. 配置微软补丁更新策略，选择自动下载，自动安装，按照指定级别更新，重要更新以上级别如图 7‑1所示：



图 7‑1 补丁更新策略配置

1. 将策略下发到内网所有Windows的终端上
2. 进入WEB控制台选择【补丁管理|微软补丁库管理|补丁下载安装信息】。管理员可以根据组织架构，查看、导出或打印补丁的安装情况，如图 7‑2所示：

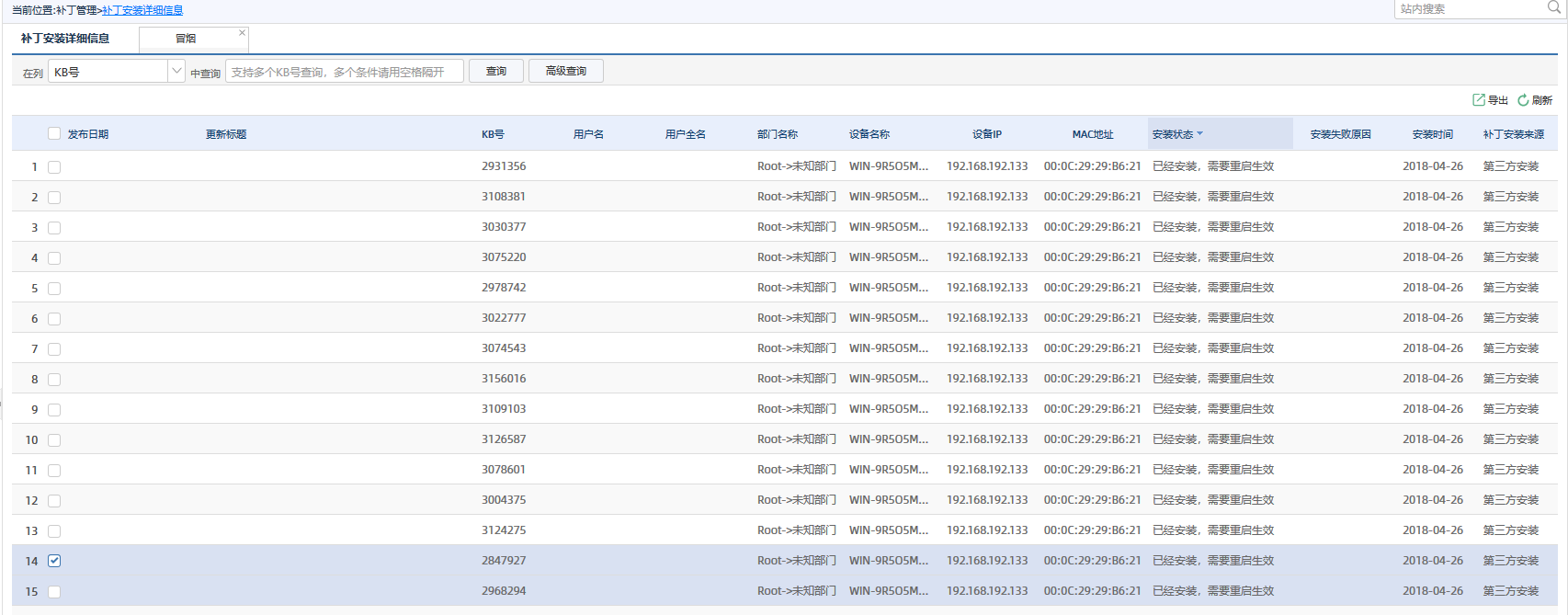


图 7‑2 补丁下载安装信息

### 微软补丁卸载策略

LeagView后台支持微软补丁的卸载，使助手终端即时卸载补丁。

进入WEB控制台选择【补丁管理|微软补丁库管理|微软补丁卸载策略】，点击增加策略，管理员可以配置对范围内终端卸载补丁的策略。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 卸载配置 | 按条件卸载更新：根据补丁安装时间段、补丁等级进行卸载；指定需要卸载的更新：从补丁库中选择需要卸载的补丁 |
| 有效卸载时段 | 在指定的时间段内才会执行卸载操作，比如指定非工作时间段内卸载，避免影响终端用户正常办公 |

进入WEB控制台选择【补丁管理|微软补丁库管理|微软补丁卸载信息】。本页面统计了助手终端补丁卸载情况。管理员可以将这些信息导出为Excel。

### 微软补丁库信息

补丁下载完成后，管理员对补丁信息进行维护，需要进入后台补丁信息管理界面。

进入WEB控制台后选择【补丁管理|微软补丁库管理|微软补丁库信息】。

在补丁库信息页面，列出了所有已下载的补丁，点击补丁的名称（即更新标题），可以查看该补丁的详情。

补丁的统计信息说明如下：

|  |  |
| --- | --- |
| 列名 | 说明 |
| 总计 | 统计某补丁需要安装的设备数 |
| 已安装并生效 | 统计某补丁已安装并生效的设备数，且该补丁正常使用 |
| 已安装未重启 | 统计某补丁已安装未重启的设备数，该补丁需设备重启后生效 |
| 未安装 | 统计某补丁未安装、安装失败、安装失败继续尝试安装、安装失败不再尝试安装的设备数 |

选中一个或者多个补丁，点击操作，管理员可以对补丁信息作出如下操作：

|  |  |
| --- | --- |
| 操作 | 说明 |
| 忽略 | 选择需要忽略的补丁，进行“忽略”操作，完成对指定补丁的忽略。在进行补丁分发策略时，忽略的补丁不要求安装 |
| 取消忽略 | 如需要对已忽略的补丁重新启动安装要求，则选择“取消忽略”操作 |
| 安装确认 | 在进行补丁分发策略过程中，如果需要安装确认，则需要进行进行“安装确认”操作，完成对指定补丁的安装确认补丁才会被允许安装 |
| 取消确认 | 如果确认安装的补丁需要取消确认功能，则选择“取消确认”操作 |
| 定制补丁更新策略 | 为该补丁配置专门的更新策略 |
| 增加 | 手动增加一个新的补丁到补丁库中 |
| 导入补丁包 | 将离线的补丁包文件导入到系统中 |

### 补丁下载安装信息

下发微软补丁分发策略后，助手会上传终端设备最新的补丁安装信息，在此页面按照部门统计补丁下载安装情况。

进入WEB控制台选择【补丁管理|微软补丁库管理|补丁下载安装信息】。

管理员可以根据组织架构，查看补丁的安装情况。

### 补丁安装详细信息

下发微软补丁分发策略后，助手会上传终端设备最新的补丁安装信息，在此页面以补丁的维度统计补丁安装情况。

进入WEB控制台选择【补丁管理|微软补丁库管理|补丁安装详细信息】。

根据补丁查看补丁的安装情况。

### 补丁安装详细信息

后台服务器连接到联软云补丁后，可以定期接收到云补丁的发布公告。

进入WEB控制台选择【补丁管理|微软补丁库管理|微软补丁安全通告】。

可以查看每一期的联软补丁公告，查看每期发布的补丁详情。

### 漏洞修复汇总

进入WEB控制台选择【补丁管理|微软补丁库管理|漏洞修复汇总】。

管理员可以查看并导出漏洞修复汇总，以部门、补丁级别和补丁来源为维度统计漏洞修复信息，包括需要安装补丁的设备数、已经安装且补丁生效的设备数和补丁未生效的设备数。

|  |  |
| --- | --- |
| 列名 | 说明 |
| 漏洞数 | 统计该部门所有设备需要安装的补丁数 |
| 已修复 | 统计该部门所有设备已安装的补丁数，已安装包括：已安装且生效和已安装需重启生效 |
| 未修复 | 统计该部门所有设备未安装的补丁数，未安装包括：安装失败继续尝试安装、安装失败不再尝试安装的补丁 |

### 终端漏洞TOP10

进入WEB控制台选择【补丁管理|微软补丁库管理|终端漏洞TOP10】。

管理员可以在本页面查看、导出和打印终端漏洞未修复数量情况（终端漏洞TOP10、统计助手终端设备的补丁情况报表），也可以通过点击已安装和需安装数字链接，查看某个终端设备的补丁安装明细和未安装的补丁明细信息。

# 终端安全管理

LeagView支持通过WEB控制台统一设置安全策略， LeagView后台将安全策略分发给安全助手，由安全助手依据策略内容对终端进行安全检查、安全控制、安全审计，实现对终端的集中管控。

## 终端安全策略

### 主机进程安全检测策略

LeagView支持对终端运行的进程进行管控。在LeagView系统中通过自定义设置进程的访问控制列表，构建进程的黑白名单，对进程的运行进行控制。LeagView对进程的管控支持两种方式：允许、禁止进程的运行和监控指定进程的运行状态。从而监视和控制主机的恶意进程，保障关键进程的正常运行。

进入【终端安全|安全策略设置|主机进程安全检测策略】页面中列出了系统中已经配置好的主机进程安全检测策略，单击指定主机进程安全策略名称的超链接可以修改已经配置好的主机进程安全检测策略，点击增加策略按钮，可以配置一个新的主机进程安全检测策略。策略配置参数如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 进程管理 | 进程管理可以控制终端主机进程的运行状态 |
| 增加 | 新增一条进程控制规则 |
| 删除 | 删除一条进程控制规则 |
| 上移/下移 | 进程控制规则列表从上到下依次匹配，当匹配上某一条规则后则不会继续往下匹配，因此需要设置每条规则的顺序，通过上移/下移调整规则的顺序 |
| 个人申请运行程序 | 终端用户可以申请某些被禁用的进程，管理员可以通过申请允许的进程列表中的进行添加到规则中，如允许用户申请的某个进行运行 |
| 进程监视 | 进程监视主要用于发现关键进程运行情况，保障关键进程正常运行 |
| 进程运行要求 | 以下进程必须全部运行：以下的进程列表中的所有进程都需要运行，否则不符合运行要求，执行相应的动作；以下进程至少运行一个：以下进程列表中的进程只要有一个即可，如果都未运行，则不符合运行要求，执行相应动作 |
| 发现进程未运行时 | 当主机上的进程不符合运行要求时，执行相应的动作，审计：审计进程的运行情况；终端弹窗提示：管理员可以自定义提示信息，提示终端用户进程不符合运行要求 |

进入【终端安全|信息查询|进程控制审计信息】、【终端安全|信息查询|进程监视审计信息】查看相应审计信息，支持查询、高级查询、导出等。

**策略示例：**

需求：要求终端主机必须安装瑞星杀毒软件，如果没有安装的主机需要及时发现和通知终端用户。

配置步骤：

1. 配置主机进程安全检测策略，在进程监视中，将瑞星杀毒软件的进程名称添加到列表中，勾选发现进行未运行时审计和终端弹窗提示。如图 8‑1所示：

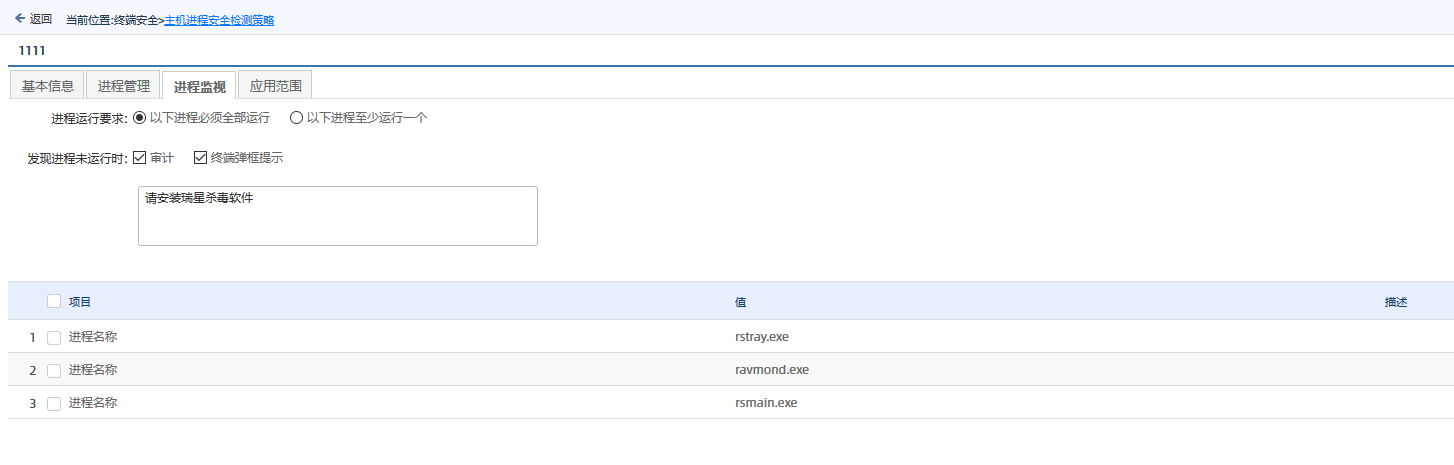


图 8‑1 进程监视策略配置

1. 将策略下发到所有终端；
2. 进入【终端安全|信息查询|进程监视审计信息】查看相应审计信息，如图 8‑2所示：



图 8‑2 进程监视审计信息

### 终端标准化策略

终端标准化是指通过模板机对全网终端文件、软件等进行标准管控，以达到规范化管理的效果。一般情况下，只有对终端软件标准化要求非常严格，不在意系统不能打补丁，不在意软件不能升级，非常在意软件的规范化标准化，非常在意病毒和木马防御，并且执行力较强的客户才建议使用本策略。

在使用终端标准化策略前，需要先配置模板机，进入【终端安全|信息查询|终端标准化模版机管理】，点击TAB右上角“下载模版机信息采集工具”，根据提示完成模版机信息采集。此页面还提供对模板机的查询、查看、删除等操作。

进入【终端安全|安全策略设置|终端标准化策略】，增加新策略，策略配置说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 请选择模板机 | 选择已有的模板机，以此模板机作为标准，检测其它终端的违规情况 |
| 违规 | 分别检测终端主机的exe、dll、sys、软件与模板机对照，不在模板机列表中的属于违规。最严格的的标准化程度是同时勾选exe、dll、sys，即终端上运行的任何 exe， exe 加载的任何 dll，任何驱动文件，只要不在模板机的列表中，一律算违规。这个配置导致的后果是：所有的 exe，dll，sys 文件都不能升级，任何新增加的exe/dll/sys 都不能运行。当然了，病毒也就没任何机会了；如果有些软件必须要经常自我更新安装目录下的 exe 和 dll，那么可以额外勾上“不在模板列表里面的软件属于违规”，这就意味着这些软件所在的目录自然成为了白名单，那么目录下的所有 exe/dll/sys 都可以运行，即使他们有更新，有变化。勾上后带来一个漏洞，就是终端用户任意 exe/dll/sys 拷贝到软件所在目录即可自动合规。这个功能弱化了安全性，增加了便利性。适用于某些特殊软件需要定期的更新自身的 exe 和 dll |
| 违规执行动作 | 禁止：禁止违规文件或软件运行；审计：审计违规的文件或软件 |
| 目录白名单 | 手工配置的这些目录都是白名单，那么目录下的所有exe/dll/sys都自动是白名单，并且可以任意拷贝exe文件到这个目录下后成为白名单文件。勾上后带来一个漏洞，就是终端用户可以任意拷贝exe文件到该目录下。这个功能弱化了安全性，增加了便利性。目录名称支持\*号匹配，也支持类似%xxxx%风格，比如 "%SystemDrive%\test\abc" 表示系统盘下的test\abc，一般情况下是"c:\test\abc"，由助手自动翻译。 |

进入【终端安全|信息查询|终端标准化审计信息】查看相应审计信息，支持查询、高级查询、导出等。

**策略示例：**

需求：企业内部采购了一批特殊的终端主机，由财务部门专门使用，这些终端主机出厂的时候已经安装了财务专用的软件，为了最大程度的保障这些终端的安全性，需要对这些终端做严格的标准化控制。

配置步骤：

1. 使用模板机信息采集工具在这批特殊的终端其中一台上采集相关信息并上传到后台服务器，使其成为模板机；
2. 采集完后，进入【终端安全|信息查询|终端标准化模版机管理】，选择刚采集的模板机，点击查看，查看已采集到的文件和软件信息，进一步确认信息是否准确，如图 8‑3所示：

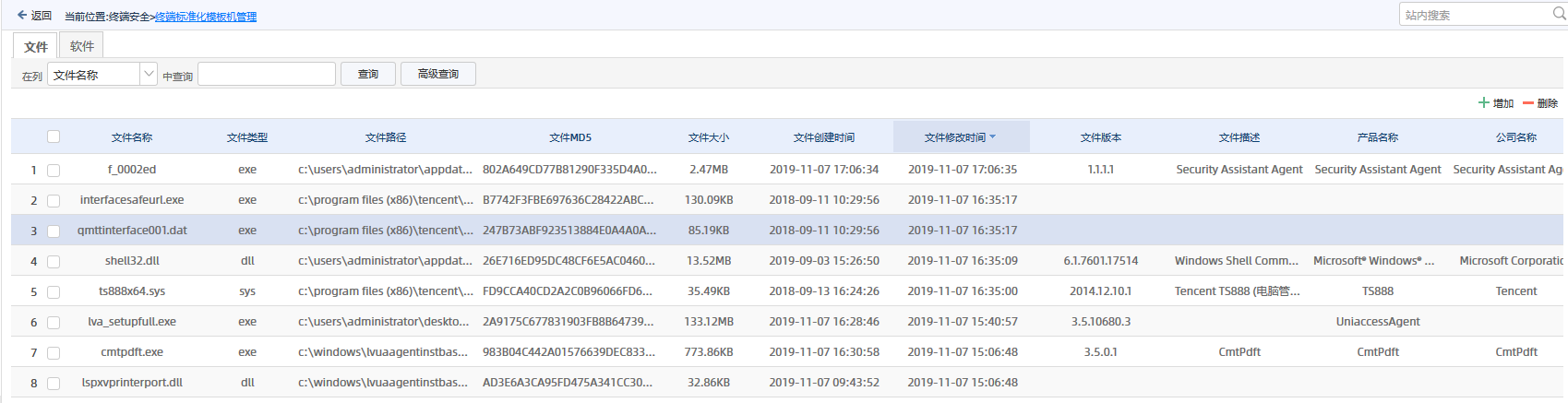


图 8‑3 模板机采集信息查看

1. 配置终端标准化策略，选择之前配置好的模板机，违规情况勾选所有，违规执行动作勾选禁止和审计，将策略下发到这批特殊的终端上，如图 8‑4所示：



图 8‑4 终端标准化策略配置

1. 如果有业务软件需要升级，或者要引入新的软件，那么管理员必须先在模板机中安装，然后再次运行采集工具 LVTplHostInfo.exe，这样就得到最新的白名单。助手会自动刷新白名单，刷新后终端就可以进行软件升级或安装了。简单来讲：模板机软件变化时，再运行一次LVTplHostInfo.exe 即可，其他事情系统会自动做。

### 终端流量管理策略

LeagView支持对已安装助手的终端的流量进行管理和分析，检测终端异常的流量和对终端流量的控制，避免对网络带宽资源造成浪费。

进入【终端安全|安全策略设置|终端流量管理】，增加新策略。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 网络异常检测 | 终端系统会由于受恶意程序的破坏，可能伴随随着网络流量也会产生异常。通过流量异常检测，及时发现可能遭受恶意程序破坏的终端 |
| 终端流量统计 | 及时发现对网络带宽占用最大的终端，便于查找网络拥塞的故障点 |
| 终端流量控制 | 可用来对一些下载软件进行限速管控，避免由于终端下载占用大量网络带宽而导致网络拥塞，对业务的正常运行产生影响 |

进入【终端安全｜信息查询 | 网络异常审计信息】、【终端安全｜信息查询 |终端流量统计】、【终端安全｜信息查询 |终端流量控制】查看相应审计信息，支持查询、高级查询、导出等。

进入【综合报表｜数据分析报表 | 网络异常审计报表】、【综合报表｜数据分析报表 | 终端流量统计】查看分析报表，支持查询、统计、多种形式展示、导出、打印等。

**策略示例：**

企业内网络总是很卡，怀疑某些终端主机中了病毒，占用了大量的网络带宽资源，需要找到这些异常的终端。

解决方案：

1. 配置终端流量管理策略，配置网络异常检测，流量统计：每秒钟不能大于1000KB，同时最多与20个主机建立TCP连接，在统计时段1分钟内，连续2个统计值超过设定值时认为异常；配置终端流量统计，统计15分钟内的终端流量平均值，统计终端所有网络流量，如图 8‑5图 8‑6所示：



图 8‑5 网络异常检测配置



图 8‑6 终端流量统计配置

1. 分别进入【终端安全｜信息查询 | 网络异常审计信息】、【终端安全｜信息查询 |终端流量统计】，查询分析这些占用网络带宽的终端，如图 8‑7图 8‑8所示：

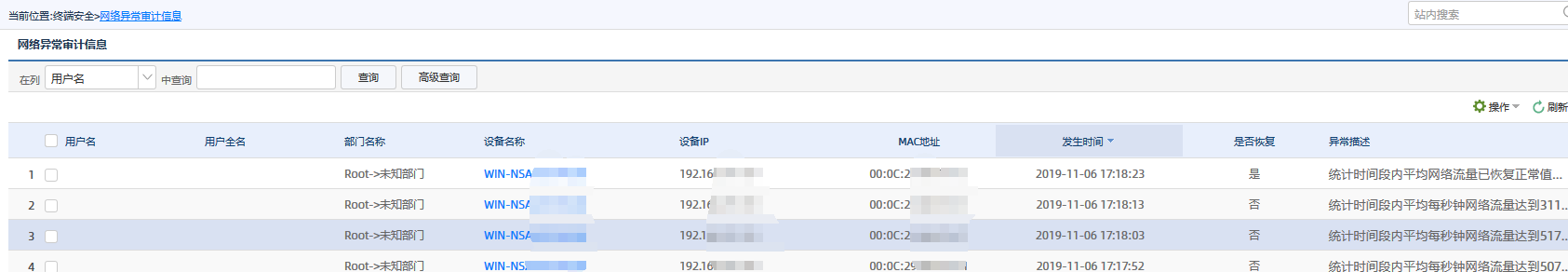


图 8‑7 网络异常审计信息

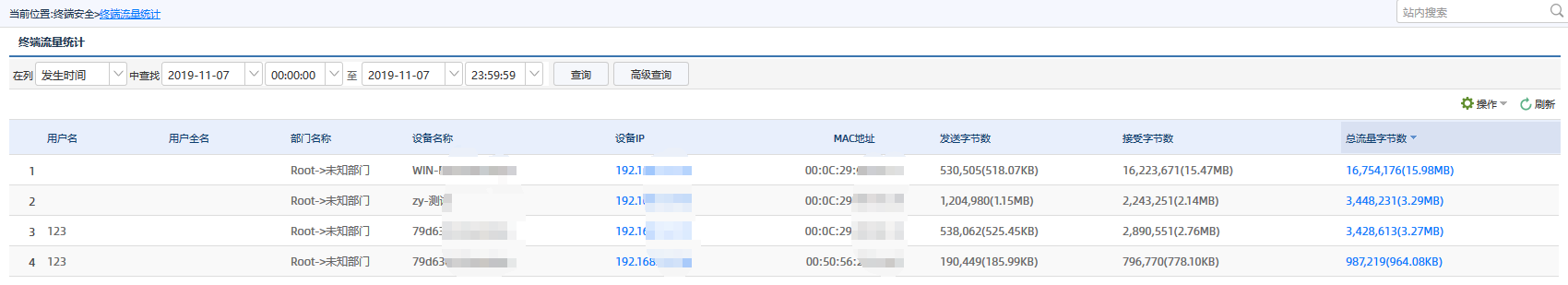


图 8‑8 终端流量统计

### Windows本地安全策略

通过在每个终端上设置Windows的本地安全策略，可以对终端操作系统的系统功能进行一些安全控制，包括：有安全隐患的不必要使用功能的禁用，系统服务的禁用，注册表的管控等。LeagView支持将一些常见的Windows本地安全策略的管理项，通过在WEB控制台制定统一的安全策略的方式，分发到终端执行，实现对终端windows本地安全策略设置的自动、集中管理。

进入【终端安全|安全策略设置|Windows本地安全策略】这个页面中列出了系统中已经配置好的Windows本地安全策略，单击指定Windows本地安全策略名称的超链接可以修改已经配置好的Windows本地安全策略点击增加策略按钮，可以配置一个新的Windows本地安全策略。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 系统 |  |
| 使用注册表编辑器 | 设置在当前设备上是否允许使用注册表编辑器，禁止使用则用户无法启动注册表编辑器 |
| 使用.reg注册表文件 | 设置在当前设备上是否允许使用注册表文件方式导入注册表信息，禁止使用则无法将注册表文件导入到注册表中 |
| 远程修改注册表 | 设置在当前设备是否允许其他用户远程修改当前设备的注册表功能，禁止使用则其他用户无法通过远程方式修改当前设备的注册表功能 |
| 添加打印机 | 设置在当前设备上是否允许添加打印机功能，禁止使用则无法为当前设备添加打印机 |
| 控制面板"添加或删除程序" | 设置在当前设备上是否允许使用控制面板中的“添加删除成”功能，禁止使用则无法打开控制面板中的“添加删除程序”菜单 |
| 设置网络属性 | 置在当前设备上是否允许使用网络属性功能，禁止使用则无法打开网络属性页面 |
| 保留打印的文档 | 支持对打印机设置中“保留打印的文档”选项进行禁用。禁用后，该设备控制下打印机打印的文档都不会被保存 |
| 增加的注册表项 | 修改当前设备的注册表项，可根据用户定义增加、修改注册表内容，其中“撤销动作”项是指当策略被禁用或删除时当前设备对此注册表项的处理方式，如：“直接删除该键”是将此注册表项删除，“修改键值为”是将此注册表项的键值修改为指定的键值 |
| 本地服务 |  |
| 服务名称 | Windows本地服务的名称 |
| 服务显示名 | Windows本地服务的显示名称 |
| 服务依赖 | Windows本地服务的依赖关系 |
| 描述 | Windows本地服务的描述信息 |
| 启动类型 | 用户设置当前Windows本地服务的启动类型。除“自动”“手动”“禁用”外，还支持配置为“自动并立即启用”、“禁用并立即停用”，可以达到策略内容立即生效的效果 |

**策略示例：**

需求：企业内部终端都使用静态IP地址，但有些终端用户经常私自修改IP，造成IP地址冲突，需要进行终端用户修改IP

配置步骤：

1. 配置Windows本地安全策略，设置网络属性，选择“禁止”，将策略下发至终端，此时终端用户无法通过设置网络属性修改IP地址，如图 8‑9所示：

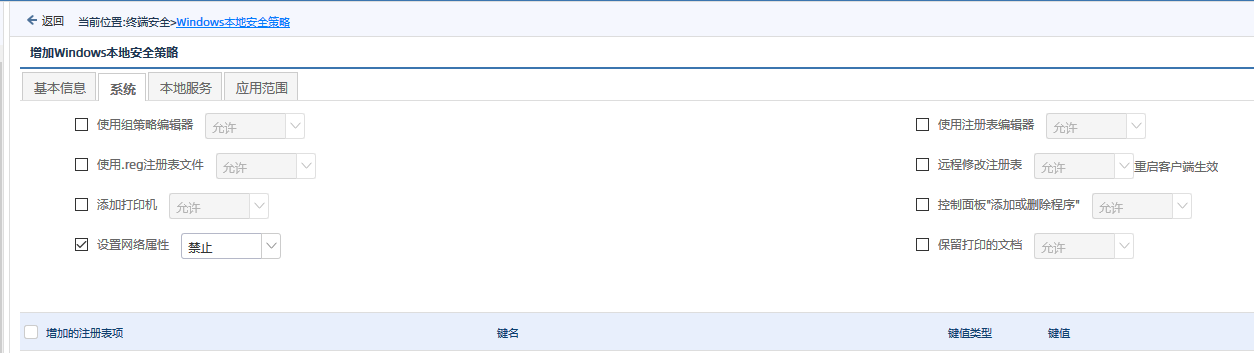


图 8‑9 Windows本地安全策略设置-禁止修改IP

### 网络资源访问控制策略

网络资源访问控制策略，对安装安全助手的终端在远程访问网络资源或自己的网络资源被远程端访问的控制，俗称“个人防火墙” ；主要限制终端用户的对外访问，特别对一些恶意站点的访问，同时也能保护终端自身的一些不安全应用或服务被他人访问和利用，从而加强终端的安全性。

进入【终端安全|安全策略设置|网络资源访问控制策略】。

增加新策略页面有四个TAB页：【基本参数】、【访问控制】、【其它】和【应用范围】，单击它们则分别切换到不同的TAB页面。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 访问控制 | 访问控制列表由多条规则组成，每条规则指定一个或一类进程在访问指定网络资源时应该受到的控制，规则列表是有先后顺序的，从第一条开始匹配进程和动作，如果都匹配上，就执行该条规则设置的控制，例如禁止。如果都不匹配，不做任何控制 |
| 进程特征项 | 当选择"进程名称"，"进程文件CRC校验值"，"软件名称"，"目录名称"，"已签名进程"时，其值不可以为空 |
| 进程特征值 | 支持\*号匹配，例如，如果配置"是进程"，"进程文件属性:公司名称"，"\*Microsoft\*"，表示所有微软公司的进程都匹配这个规则中的进程条件。如果配置"非进程"，"进程文件属性:公司名称"，"\*Microsoft\*"，表示除了微软公司的进程外其他任何进程都匹配 这个规则中的进程条件。为了防止进程伪装，可以指定"进程文件CRC校验值"，用16进制，例如"abcdef12"，不分大小写 |
| 方向 | 网络访问的方向，进站或者出站，即下载或上传 |
| 协议 | 网络访问传输层协议类型，TCP或UDP |
| IP/MAC/域名 | IP范围格式示范： 192.168.1.1 192.168.1.\*(1网段) 192.168.\*(168网段) \*(表示所有) 192.168.1.1-192.168.2.20  上述是基础格式，也可以用逗号分隔放在一起，如： 192.168.1.1,192.168.1.2,192.168.2.\*,192.168.4.1-192.168.4.10 |
| 端口范围 | 如果出栈，表示对方的端口范围，如果是进栈，表示自己开的端口范围，格式如下： 0(表示所有) 100 100-200  上述是基础格式,也可以用逗号分隔放在一起，如： 100,101,200-400 |
| 审计 | 审计网络访问详情，每次访问都审计 |
| 仅审计一次 | 审计网络访问详情，为了避免产生过多审计记录，每次相同的访问仅审计一次 |
| 阻止 | 阻断符合条件的网络访问 |
| 阻止时弹出提示 | 阻断符合条件的网络访问，且助手弹窗提示 |
| 仅弹出一次提示 | 阻断符合条件的网络访问，且助手弹窗提示，为了避免干扰用户，仅弹窗一次 |
| 其它 |  |
| 禁止与同网段中未安装安全助手的机器通讯 | 勾选后，助手工作如下：  1.设置默认合法的IP地址：所有网卡的网关IP、DHCP服务器IP、DNS服务器IP、LeagView后台服务器IP。 2.其余要通讯的IP地址，先获取该IP地址对应MAC地址，如果是第一次通讯，则用MAC地址到后台去查询，并将后台返回的结果保存到缓存。如果后台认为是合法的MAC地址，则放行，否则拒绝。 3.后台判断MAC地址是否合法：安全助手提交一个Mac地址，代理通讯查询内存（数据库）看这个Mac地址对应的设备有没有安装安全助手，安全助手在不在线。如果安装了且助手在线，则返回MAC地址合法，否则非法。 |
| 设置网卡远程唤醒 | 如果要远程开机或远程唤醒睡眠的电脑，需要先手工在电脑的BIOS设置里面开启远程唤醒功能，然后启用本选项去自动设置网卡的属性使得网卡支持远程唤醒。当然，不使用本选项，而是手工在电脑上设置也可以 |

【注意】默认仅支持应用层的管控，不支持内核层的端口管控（445、3389等端口），如需支持内核层端口都支持，需增加扩展配置：use\_kfw=1，但存在与流量中转软件、vpn软件等冲突的可能（表现为策略不生效，或者导致策略生效对方不生效）。

进入【终端安全|信息查询|网络资源访问控制审计信息】查看相应审计信息，支持查询、高级查询、导出等。

**策略示例：**

需求：禁止所有终端访问baidu.com

配置步骤：配置网络资源访问控制策略，进程特征项选择进程名称，特征值使用\*匹配所有，域名填写baidu.com（可使用\*baidu\*包含baidu的域名），端口范围为0，勾选“阻止”，将策略下发至终端，如图 8‑10所示：



图 8‑10 网络资源访问控制策略配置

### Braise脚本策略

用户环境复杂多变，各种需求不停变换，原来的通过修改软件功能块来满足客户的需求已经不能及时快速的满足客户需求，现在用户可通过编写Braise脚本来达到指定的目的。

Braise 是联软全新设计和开发的程序设计语言，它的语法基于有广泛用户群的C++和Java，也参考了Lua，Ruby等流行的脚本语言。

进入【终端安全|安全策略设置|Braise脚本策略】，增加新策略页面。配置说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 上传braise脚本 | 将脚本文件上传到系统后台 |
| 运行方式 | 根据终端的实际环境选择对应的运行方式 |
| 运行账号 | 某些脚本需要使用特殊的账号权限，可以在此赋予脚本相应的账号权限 |
| 上传运行结果 | 将脚本的运行结果以审计信息的形式上传到LeagView后台，“返回码”指脚本的return 语句的返回值；“错误描述”指当脚本有语法或运行期错误时脚本解析器的报错信息；“输出信息”是指通过函数io.out 或io.outln 输出的文本 |

进入【终端安全|信息查询|Braise脚本策略执行结果】、【终端安全|信息查询|Braise运行时信息】查看相应审计信息和Braise脚本的运行结果，支持查询、高级查询、导出等。

### 注册表访问控制策略

注册表是 Windows 独有的技术，操作系统的大部分配置放在注册表中，这也给恶意程序提供了方便。通过修改某些特定的注册表项，可以改变系统的行为，种木马。因此，我们需要对注册表进行全面的监控：既可以防止系统被木马病毒篡改，也可以防止终端用户对重要注册表项的误操作。如果审计所有终端的注册表读写操作，在后台还可以利用大数据技术进行多维度分析，防范风险。

进入**【终端安全|安全策略设置|注册表访问控制策略】，**页面中列出了系统中已经配置好的注册表访问控制策略，单击指定注册表访问控制策略名称的超链接可以修改已经配置好的注册表访问控制策略，点击增加策略按钮，可以配置一个新的注册表访问控制策略。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 编辑注册表访问控制列表 | 访问控制列表包含一条或多条控制规则，按照从上到下的顺序匹配 |
| 增加访问控制规则 |  |
| 进程 | 当选择“进程名称”，“进程文件CRC校验值”，“软件名称”，“目录名称”，“已签名进程”时，其值不可以为空。支持\*号匹配。例如，如果配置“指定进程”，“进程文件属性:公司名称”，“\*Microsoft\*”，表示所有微软公司的进程都匹配这个规则中的进程条件。如果配置“非指定进程”，“进程文件属性:公司名称”，“\*Microsoft\*”，表示除了微软公司的进程外其他任何进程都匹配这个规则中的进程条件。为了防止进程伪装，可以指定“进程文件CRC校验值”，用16进制，例如“abcdef12”，不分大小写。CRC值是不支持\*号匹配的。策略在配置时，应该遵循最小化配置原则。进程特征，动作，源设备及目标设备应明确。否则策略下发后可能对终端性能及功能造成影响 |
| 注册表操作 | 选择注册表的操作的控制类型 |
| 路径 | 注册表路径指通过注册表编辑器的“复制项名称”得到的字符串，不能为空，支持\*号匹配 |
| 键 | 填写注册表键的名称，支持\*号匹配，不填写表示仅关注和匹配注册表路径，忽略本字段及其值 |
| 值 | 注册表键对应的值，只有注册表操作类型为“修改”的时候，值的配置才有效 |
| 控制 | 审计：审计上面已勾选注册表操作；阻止：阻止上面已勾选的注册表操作 |

进入【终端安全|信息查询|注册表访问审计信息】查看相应审计信息，支持查询、高级查询、导出等。

**策略示例：**

需求：审计所有注册表删除、修改、创建、重命名的行为。

配置步骤：

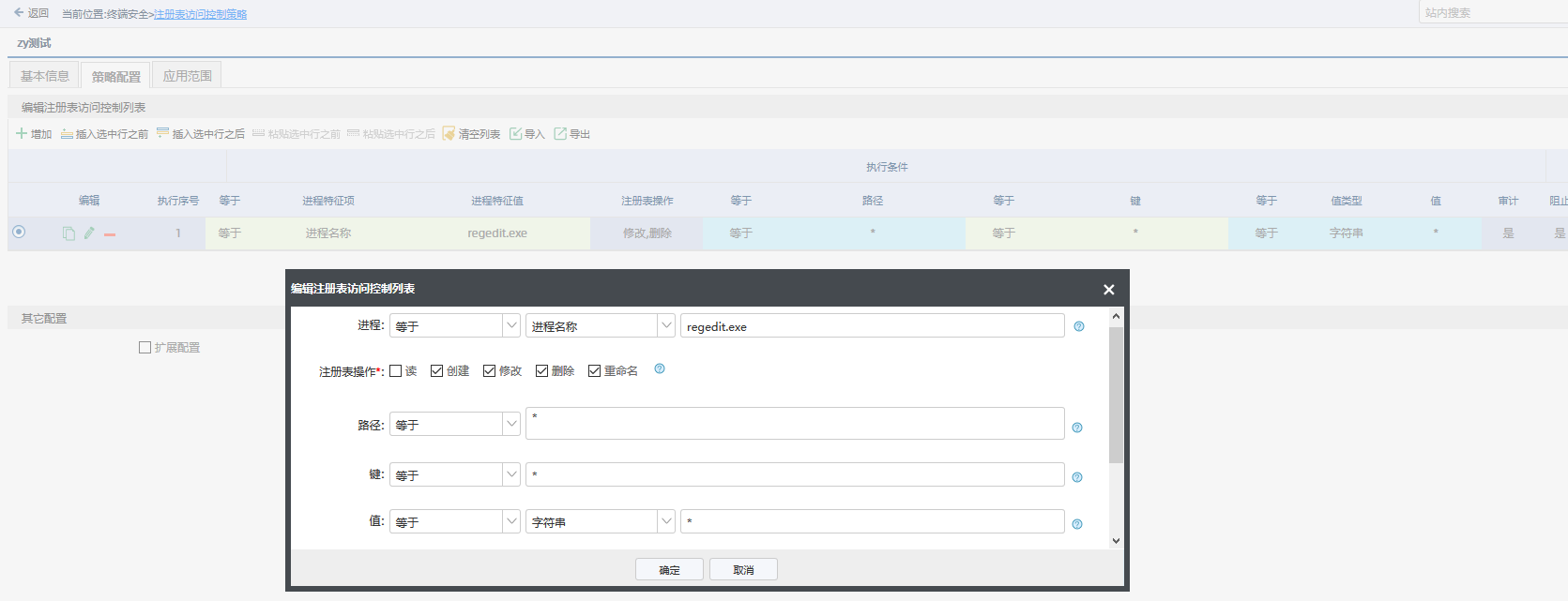
1. 进入**【终端安全|安全策略设置|注册表访问控制策略】，**点击增加策略按钮，可以配置一个新的注册表访问控制策略，配置如图 8‑11所示：

图 8‑11 注册表访问控制策略配置

1. 进入【终端安全|信息查询|注册表访问审计信息】查看相应审计信息，如图 8‑12所示：

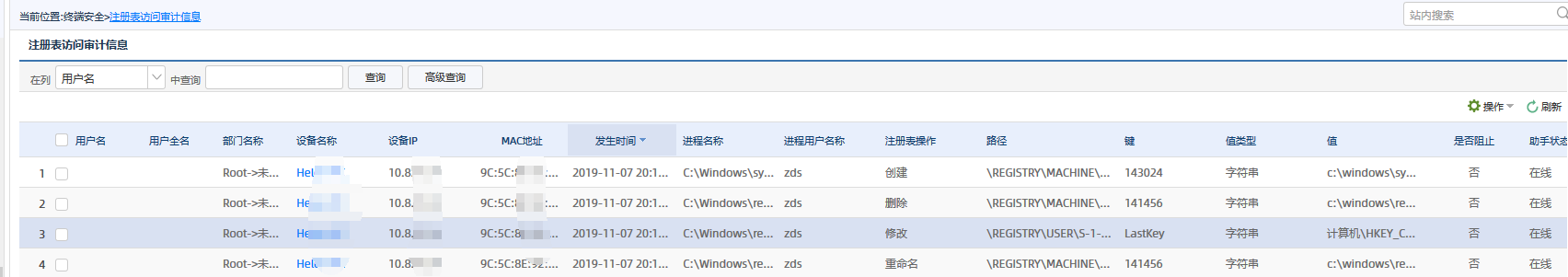


图 8‑12 注册表访问审计信息

### 终端系统自检策略

通过设置终端系统自检策略，安全助手可以实现对终端操作系统的账户、口令，可疑文件、注册表信息，可写共享，系统补丁更新情况等常见终端安全漏洞进行持续的、周期性的检查，时刻发现漏洞并及时通知。

进入【终端安全|安全策略设置|终端系统自检策略】，增加新策略页面有九个TAB页：【基本信息】、【终端配置检查】、【终端环境检查】、【终端安全检查】、【终端软件黑白名单】、【终端必须安装的软件】、【自定义检查】、【自检计划】和【应用范围】，分别切换到不同的TAB页面进行参数配置。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 终端配置检查 | 配置终端系统自检策略的终端配置检查策略，如设备注册检查、软件版本检查、磁盘剩余空间检查、IE代理检查等 |
| 终端环境检查 | 配置终端系统自检策略的终端环境检查策略，如DNS检查、DHCP检查、加域信息检查、网络连接检查等 |
| 终端安全检查 | 配置终端系统自检策略的终端安全检查策略，如终端安全策略、软件安全检查、补丁安装检查、防病毒软件检查等 |
| 终端软件黑白名单 | 配置终端系统自检策略的终端软件黑白名单策略，如白名单设置、黑名单设置等 |
| 终端必须安装的软件 | 配置终端系统自检策略的终端必须安装的软件策略，如必须安装的软件等。管理员可以从软件仓库添加软件至系统自检策略中，若终端在系统自检时检测到未安装该软件，支持一键修复安装 |
| 自定义检查 | 配置终端系统自检策略的自定义检查策略，如自定义检查设置等 |
| 自检计划 | 配置终端系统自检策略的自检计划策略，如是否允许终端用户自主检查、定期检查设置、定期检查时间计划等 |

进入【综合报表｜数据分析报表 | 系统自检漏洞报表】查看分析报表，支持查询、统计、多种形式展示、导出、打印等。例如，管理员可以根据漏洞描述查询，查看某特定漏洞的情况并导出为Excel。

**策略示例：**

需求：企业内部网络为了规范终端的网络环境配置，要求终端只能配置指定的DNS服务器192.168.1.1，且必须要加入域leagsoft.com，管理员需要每天收集和统计不合规的终端情况。

配置步骤：

1. 配置终端系统自检策略，在终端环境检查中，勾选“要求必须连接合法的DNS服务器”，再勾选“终端只能配置策略中指定的DNS服务器”，点击添加，输入合法DNS服务器IP地址192.168.1.1；勾选“加域信息检查”，再勾选“要求必须加入指定合法域”，点击添加，输入合法域leagsoft.com；如图 8‑14所示：



图 8‑14 终端系统自检策略配置

1. 在自检计划中，勾选“定期检查终端系统情况，检查后上传审计信息与系统检查报告”，检查周期选择“每天检查”，检查时间输入09:35。如图 8‑15所示

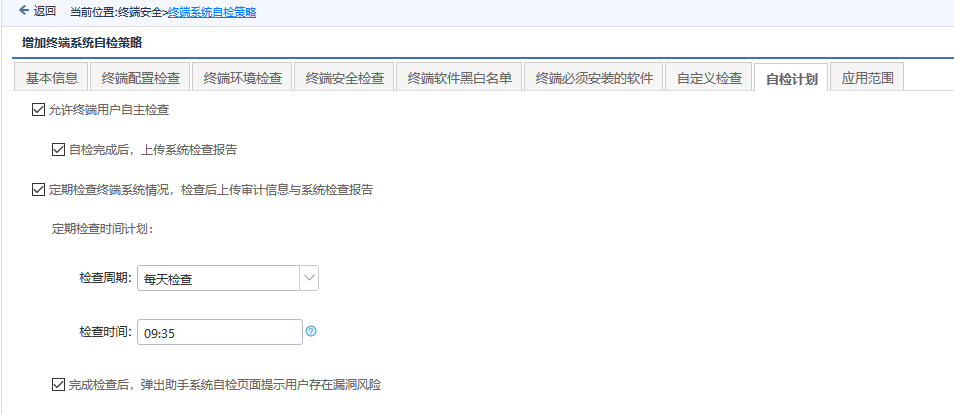


图 8‑15 终端系统自检策略配置

1. 每天09:35后，管理员进入【综合报表｜数据分析报表 | 系统自检漏洞报表】查看分析报表。

### 操作系统账户管理

许多企业环境中对Windows账户有严格的管理要求，特别是在域的环境中，一般不允许终端用户使用Windows本地管理员的权限，但有时候终端用户临时需要本地管理员权限，比如安装一些特殊的软件，或者其它一些需要管理员权限的操作，使用后却没有被及时回收权限，或者终端用户通过其它特殊的手段使用本地管理员权限的账户，此时会造成管理上的漏洞。

操作系统账户管理策略功能包含账户/账户组配置变更审计、系统登录变更审计、账户组成员监控。

管理员可以通过配置策略对终端操作系统账户/账户组配置变更的行为、操作系统账户的登录/注销的行为进行审计，对账户组的违规成员进行监控及审计。

进入【终端安全|安全策略设置|操作系统账户管理策略】，增加新策略。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 账户/账户组配置变更审计 | 新增账户、新增账户组、删除账户、删除账户组、修改账户密码、禁用账户、启用账户、修改账户所属组。如果勾选了新增账户，那么应用此策略的终端有新增账户的行为时，进行审计 |
| 系统登录审计 | 登录、注销。如果勾选了登录，那么应用此策略的终端有登录账户的行为时，进行审计 |
| 组成员监控 | 增加和删除列表，列表字段为：账户组（账户组名称）、合规成员（账户组所属成员的账户名）。如果添加admin账户组里的A、B、C用户为合规成员，那么应用此策略的终端在admin账户组里除了A、B、C以外的用户都为违规，对违规用户进行监控审计 |

进入【终端安全|信息查询|操作系统账户管理审计信息】查看审计信息，本页面支持查询、高级查询、删除、导出等。

**策略示例：**

需求：企业网络中的终端都要求加入域，终端用户只能使用域账户登录，不允许终端用户使用具有administrators组权限的本地账户，终端主机上的本地账户仅保留administrator这个本地账号供管理员调试使用，但管理员发现，终端用户通过其它特殊方法私自创建了本地账号，管理员需要找到这些存在除了administrator外本地账号的违规终端并进行相应的处理。

配置步骤：

1. 配置操作系统账户管理策略，勾选审计账户/账户组配置变更，以便管理员追溯这些变更行为；
2. 账户组成员监控中，增加账户组administrators进行监控，合规成员配置administrator；

如图 8‑16所示：

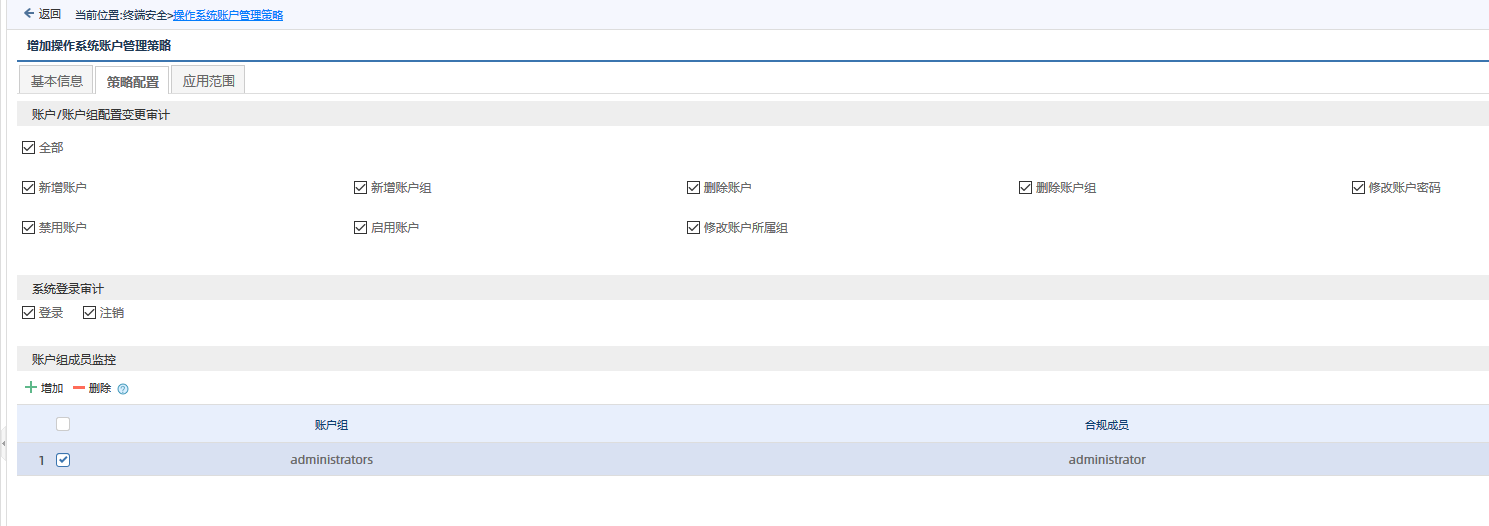


图 8‑16 操作系统账户管理策略配置

1. 进入【终端安全|信息查询|操作系统账户管理审计信息】查看审计信息，通过高级查询筛选“存在违规账户”的审计记录，即可找到所有存在违规行为的终端。如图 8‑17所示：

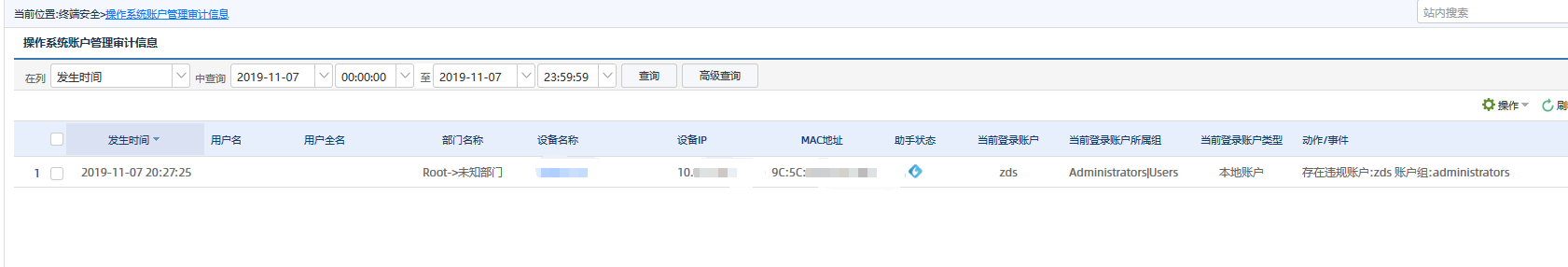


图 8‑17 操作系统账户审计信息

### 网络连接审计与控制策略

终端可以通过网络连接审计与控制策略实时探测网络连接情况，对违规行为作出提示和审计。

进入【终端安全|安全策略设置|网络连接审计与控制策略】，增加新策略。策略中可以配置多条检测规则，从上往下的顺序匹配，检测规则配置说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 检测目标 | 终端能连接互联网：助手会内置固定的一定数量的互联网网站或通用DNS服务器地址，只要这些公网地址能ping通，即触发策略；终端能连接外网：这里外网的定义是，只要不在能连接LeagView后台的内网中，都算外网，比如，两机使用网线直连，挪到另外一个局域网或网段中，当然，也包括互联网；终端能连接指定地址：在下边的编辑框中指定地址，多个地址用分号隔开，可以是域名，也可以是IP，比如，”www.baidu.com;8.8.8.8”, 地址不能有http之类开头，后面也不能有目录，例如，不能写成“ http://www.baidu.com/abc”。也不能加上端口号；终端的安全助手离线：助手所在的主机无法连接LeagView后台服务器 |
| 检测方式 | Ping方式检测：助手使用ICMP协议尝试连接目标；tcp方式检测：助手使用tcp协议尝试连接目标；HTTP方式检测：助手使用HTTP协议尝试连接目标 |
| 检测轮询周期 | 助手会在轮询周期内重复检测 |
| 处理手段 | 无：仅检测，不进行处理；禁用所有网卡，直到管理员解锁：触发后，助手立即禁用所有网卡，此时，助手本身也无法通信。重启电脑也无法恢复。终端用户不能强行启用网卡。解锁的唯一办法是从管理员处获取管理员密码或者认证随机码，从而卸载助手或者进入特权模式；阻止网络流量，直到触发条件解除：触发后，助手没有禁用网卡，而是使用助手内置的防火墙阻止了IP流量，此时，助手本身作为例外进程不受影响，仍然可以和后台通信，如果触发条件消失了（例如断开ADSL拨号，或者拔出联通3G网卡），限制自动解除；阻止网络流量，直到管理员解除：在“永恒之蓝”事件后，希望避免内网终端在员工私自连接互联网，以此来降低黑客攻击的风险，检测终端可以访问互联网后，立即断开其外网连接，仅允许终端与Leagview后台通信，且必须管理员介入才能解除。策略生效阻断网络时生成mark文件，mark文件不会因终端恢复合规而清除，只能靠管理员介入修改策略或助手来完成清除动作，发现终端存在mark文件时，不管终端是否合规，都会进行网络阻断动作 |
| 审计 | 否：仅控制，助手不上传审计数据；是（立即断网，恢复后上传）：触发后，立即断网，恢复网络后上传审计数据；是（先试图上传，再断网）：触发后，如果助手在线，会先试图上传审计数据，之后，不管上传是否成功，立即断网。因为助手判断是否在线不是实时的， 而且由于使用TCP协议上传，所有存在一定程度的风险，试图上传时可能网络刚好断开，或者其他原因导致超时，这样事件触发后10秒甚至更长时间才开始断网。如果断网前上传失败，则恢复网络后再上传审计数据 |

进入【终端安全|信息查询|网络连接控制审计信息】查看相应审计信息，支持查询、高级查询、导出等。

**策略示例：**

需求：企业内某部门的终端不允许任何形式连接互联网，如果连接了互联网立即断网。

配置步骤：

1. 配置网络连接审计与控制策略，增加一条控制规则，检测目标选择终端能连接互联网，检测方式ping，检测轮询周期120秒（不宜过长也不宜过短），处理手段：阻止网络流量，直到触发条件解除。配置完成后将策略下发到该部门下的终端。如图 8‑18所示：

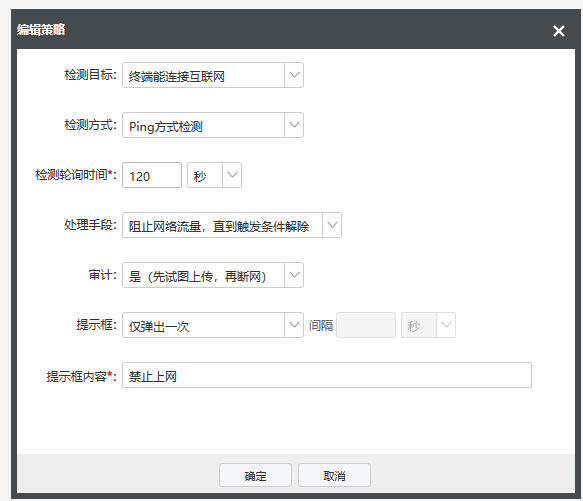


图 8‑18 网络连接审计与控制策略配置

1. 进入【终端安全|信息查询|网络连接控制审计信息】查看相应审计信息，如图 8‑19所示：

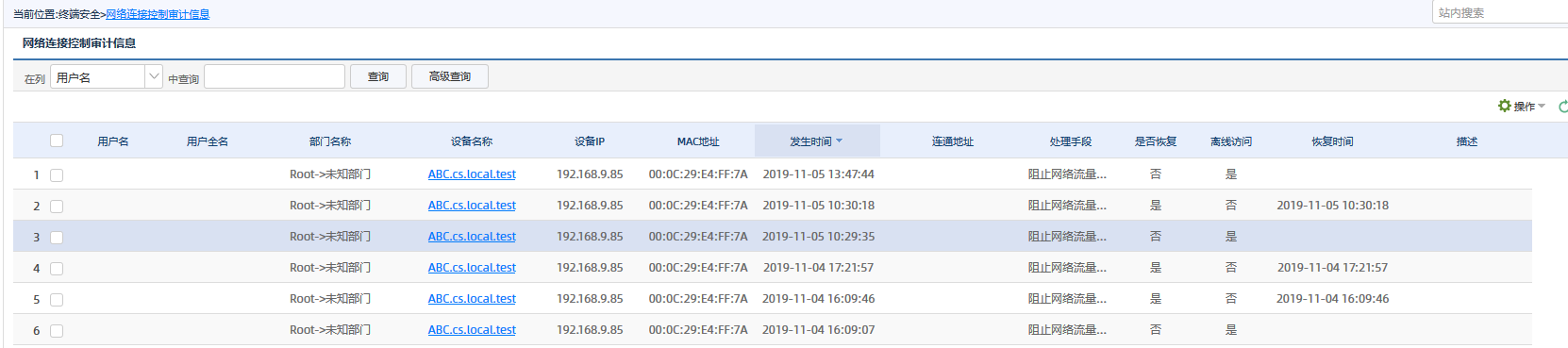


图 8‑19 网络连接审计与控制信息

### 高级终端保护策略

高级终端保护策略可以全量收集终端的行为数据，通过后台的大数据引擎和人工智能算法，以全局视角来分析和展示终端的各种外来和内部威胁。

进入【终端安全|安全策略设置|高级终端保护策略】，增加新策略，策略说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 启用客户端进程行为采集和上传功能 | 勾选后开启采集终端所有的进程行为 |
| 启用客户端网络行为采集和上传功能 | 勾选后采集终端所有网络行为，包括网络流量统计、网络访问、网络协议等 |
| 访问威胁情报中设定的黑名单IP时弹出提示 | 勾选后，下方填写提示内容；需结合联软网络智能防御系统UniNID的网络威胁情报 |
| 阻止访问威胁情报中设定的黑名单IP | 勾选后，可阻止终端访问威胁情报的黑IP；需结合联软网络智能防御系统UniNID的网络威胁情报 |
| 访问威胁情报中设定的黑名单域名时弹出提示 | 勾选后，下方填写提示内容；需结合联软网络智能防御系统UniNID的网络威胁情报 |
| 阻止访问威胁情报设定的黑名单域名 | 选后，可阻止终端访问威胁情报的黑域名；需结合联软网络智能防御系统UniNID的网络威胁情报 |
| 启用客户端文件行为采集和上传功能 | 采集终端上所有EXE/DLL文件的签名/公司名称/描述/文件路径/内存占用/MD5/创建时间/大小等信息；采集终端上所有文档的文件名称、文件原有格式（如后缀名是exe，实际是doc）、所在路径等信息 |
| 启用客户端注册表行为采集和上传功能 | 勾选后开启采集终端所有的注册表变更行为 |
| 启用客户端操作系统日志采集和上传功能 | 勾选后开启采集Windows终端原有的操作系统日志 |
| 启用客户端用户登录行为采集和上传功能 | 勾选后开启采集终端已存在的账户名称、账户全名、所属用户组、账户类型、最近登录时间以及当前登录账户 |
| 采集终端系统账号变更并上传 | 勾选后开启采集终端所有系统账户配置变更行为 |
| 采集终端系统服务和驱动及其变更并上传 | 勾选后开启采集终端所有系统服务和驱动变更行为 |
| 采集终端系统启动项及其变更并上传 | 勾选后开启采集终端系统启动项及其变行为 |
| 采集客户端PE文件(exe/dll/sys)基本信息及其变更并上传 | 勾选后开启采集客户端PE文件(exe/dll/sys)基本信息及其变更行为 |

高级终端保护策略在管理页面上没有审计信息页面，其采集的数据经过后台分析后，输出到数据分析模块。

进入【数据分析|风险汇总】、【数据分析|风用户风险TOP10】、【数据分析|用户行为全景】可查看分析结果。

# 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 |

### 文件DNA库

联软科技的文档DNA技术可对文档进行分词、主题分析，然后通过机器学习算法进行特征降维去噪，生成DNA字符串，通过比对DNA字符串，可得到对应文档内容的相似度。

在DLP数据识别中，可以使用文档DNA对比目标文件与敏感数据的样本文件的内容相似度，当达到一定的相似度阈值我们可以认为目标文件属于敏感文件。

传统的关键字、正则等识别方法，需要定义清楚关键字等相关规则后才能识别敏感文件，这样肯定会存在误报和漏报，文档DNA技术只需使用工具自动提取DNA，即可将两个文档进行文档相似度匹配，不再依赖于固有的规则，可有效提高识别的准确性。

在Web控制台选择菜单【全局信息|敏感数据基础设置|文件DNA库】在此页面可以看到使用文件DNA采集工具上报上来的样本文件信息，这些文件DNA信息可供敏感规则条件引用。

* 文件DNA采集

工具箱中内置了文件DNA采集工具，前往【软件管理|工具箱|工具箱】即可下载该工具，或者将该工具发布到助手工具箱上，在助手的工具箱中打开该工具，如图 9‑1



图 9‑1 文件DNA采集工具

点击添加文件，选择需要采集的样本文件，采集完成后，点击开始上传，即可将采集结果上传到后台服务器，前提是被采集的终端可以与LeagView后台服务器通讯。

### 文档智能聚类

文件自动聚类是一种典型的无指导机器学习方法，用机器学习算法将不同文档分别映射到特征向量空间中，以实现将未分类文档集合自动分成若干类文档的目的。利用中文分词等技术，将不同文档分别映射到特征向量空间中，提取的特征向量尽可能突出文章的中心思想，根据向量的密集分布程度，将文档聚集成某些特定类别。在特征空间中，同类文档往往集聚在同一个空间区域中，从而实现将未分类文档集合自动分成若干类文档。

在DLP数据识别中，使用文档智能聚类将样本文件分类后形成分类库后，当对文件进行敏感扫描时，提取文件内容的特征，匹配已有的分类库，可识别出该文件属于那种类型的数据。

智能聚类的分类结果的准确性取决于样本文件的质量，需要每种类型的文件内容高度相似，例如都是相同模板的会议纪要，相同模板的征信报告等，且样本文件数量越多，分类的结果越准确。

* 文件特征采集

工具箱中内置了文件特征采集工具，前往【软件管理|工具箱|工具箱】即可下载该工具，或者将该工具发布到助手工具箱上，在助手的工具箱中打开该工具，如图 9‑2



图 9‑2 文件特征采集工具

点击添加文件，选择需要采集的样本文件，采集完成后，点击开始上传，即可将采集结果上传到后台服务器，前提是被采集的终端可以与LeagView后台服务器通讯。

* 智能聚类

在Web控制台选择菜单【全局信息|敏感数据基础设置|文档智能聚类】在此页面选择【所有文件】TAB，可以看到所有文件特征采集工具上传的文件信息，包括已分类和未分类的。点击，开始对未分类的文件进行聚类。聚类页面如图 9‑3

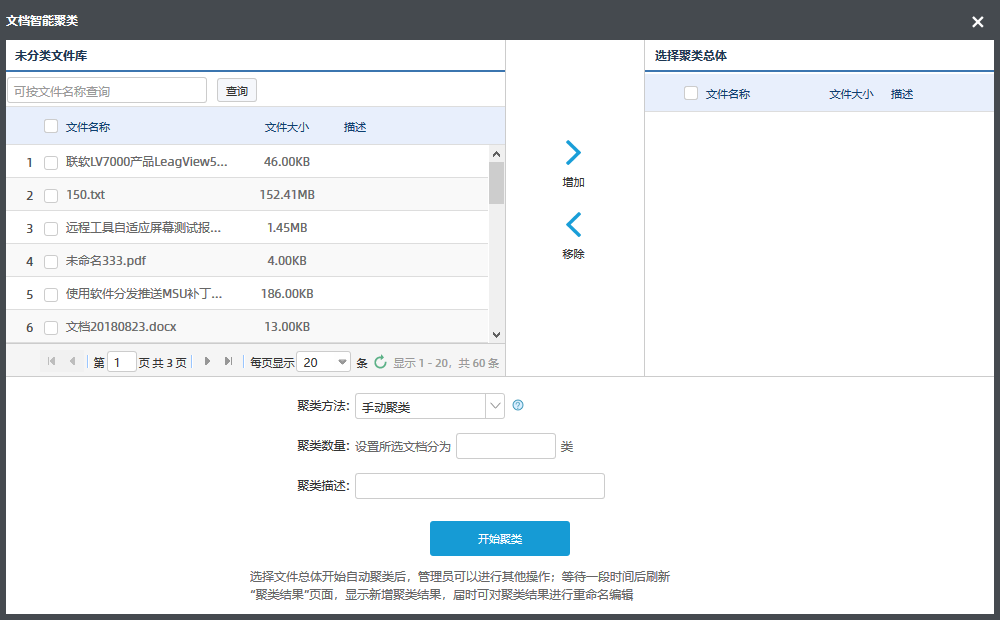


图 9‑3 文档智能聚类

左边显示未分类的文件列表，选择一个或者多个文件，点击增加，将这些文件移到选择聚类主体中。

根据样本文件的情况，选择相应的聚类方法。

手动聚类：适用于对样本文件比较熟悉的情况，明确知道样本文件中有几类数据，然后设置分类数。

自动聚类：使用于样本文件中数据类型较多的情况，不明确有多少类型，样本数量越多，分类效果越好。

聚类完成后，进入【聚类事件】页面，查看刚才的聚类情况，该页面统计本次聚类的的文件个数，聚类后的分类数。点击聚类主体数，可以查看参与聚类的文件，点击分类数，跳转到【聚类结果】，查看本次的聚类结果，点击每个分类的聚类样本数，可以看到该分类下都有哪些文件。

系统会自动给聚类结果的分类进行命名，如分类0、分类1等，这些分类名称没有实际意义，聚类完成后，需要人工更改分类的名称。

【注意】已被分类的文件，无法再次聚类，需在聚类结果中删除该分类后，该分类下的文件才可以再次进行聚类。

### 敏感数据分类定义

敏感数据分类定义主要用于敏感规则引用，配置敏感规则之前需先定义好敏感数据分类。

Web控制台选择菜单【全局信息|敏感数据基础设置|敏感数据分类定义】进入敏感数据分类定义页面，页面左侧是已定义好的分类，点击上方的图标增加一级分类。选中某个一级分类，点击图标增加子分类，点击保存将配置信息保存到数据库。

【注意】该分类的定义与智能聚类的分类无关，这是人为的给敏感数据做个分类的标签，而智能聚类的分类是根据文件内容做的分类。

### 敏感数据级别定义

敏感数据级别定义主要用于敏感规则引用，配置敏感规则之前需先定义好敏感数据级别。

Web控制台选择菜单【全局信息|敏感数据基础设置|敏感数据级别定义】进入敏感数据级别定义页面，点击增加创建新的级别，点击保存将配置信息保存到数据库。

【注意】敏感级别有高低之分，在敏感数据级别定义列表中，敏感级别大小由上到下排列，越往上的级别越大，通过上移/下移按钮调整顺序来调整级别的高低。

### 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 |

## 敏感数据发现

### 敏感文件审计策略

管理员通过下发敏感文件审计策略，主动探测终端上的敏感文件，掌握敏感数据的分布情况。

在Web控制台选择菜单【数据防泄露|终端数据通道管控策略|敏感文件审计策略】进入策略配置页面，新增一条策略，策略配置说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 关键字信息 | 选择已配置好的敏感规则模板，如果选择了多个敏感规则模板，这些敏感规则模板的匹配是有先后顺序的。排在前面的先匹配，如果匹配成功，则忽略后面的模板，如果匹配失败，则继续匹配下一个模板 |
| 搜索本地磁盘 | 指定搜索本地磁盘的范围 |
| 搜索安全虚拟磁盘 | 指定搜索安全虚拟磁盘范围 |
| 检索时机和控制 | 指定敏感扫描时段和间隔，注意该时段应包含在策略生效时段范围内，否则无法触发扫描 |
| 选项 | 上传审计记录：将扫描结果上传到后台服务器；实时检查：当有新的文件数时立即触发扫描，当本地磁盘检查任务和安全虚拟磁盘检查任务都处于空闲状态时，实时检查才生效。实时检查不会剪切或拷贝敏感文件到安全虚拟磁盘 |
| 检索时高级控制 | 敏感文件扫描可能会占用终端较多资源，为了不影响终端主机正常使用，可以限制CPU和内存使用率的上限值，当超过该值时停止扫描，但会最终影响扫描的速度；为了平衡性能和扫描速度，可以利用终端空闲的时段进行扫描 |
| 防泄露动作 | 敏感扫描与安全虚拟磁盘联动，助手自动将敏感文件拷贝或剪切到安全虚拟磁盘中，以便敏感数据得到全面的保护 |
| 文件服务器配置 | 可将发现到的敏感文件上传到后台服务器集中存储 |

进入【数据防泄露|信息查询|敏感文件审计信息】查看敏感扫描结果，该页面统计每个用户终端数行的敏感文件总数，以及按照敏感等级进行统计，点击相应的统计数字，可以查看敏感文件信息。选择某个敏感文件，点击，可以查看该文件命中敏感规则模板详细情况。

**策略示例：**

需求：扫描发现终端上的敏感文件分布情况。

配置步骤：

1. 在Web控制台选择菜单【数据防泄露|终端数据通道管控策略|敏感文件审计策略】进入策略配置页面，新增一条策略，策略配置如图 9‑4所示：



图 9‑4 敏感文件审计策略配置

1. 进入【数据防泄露|信息查询|敏感文件审计信息】查看敏感扫描结果，如图 9‑5所示：

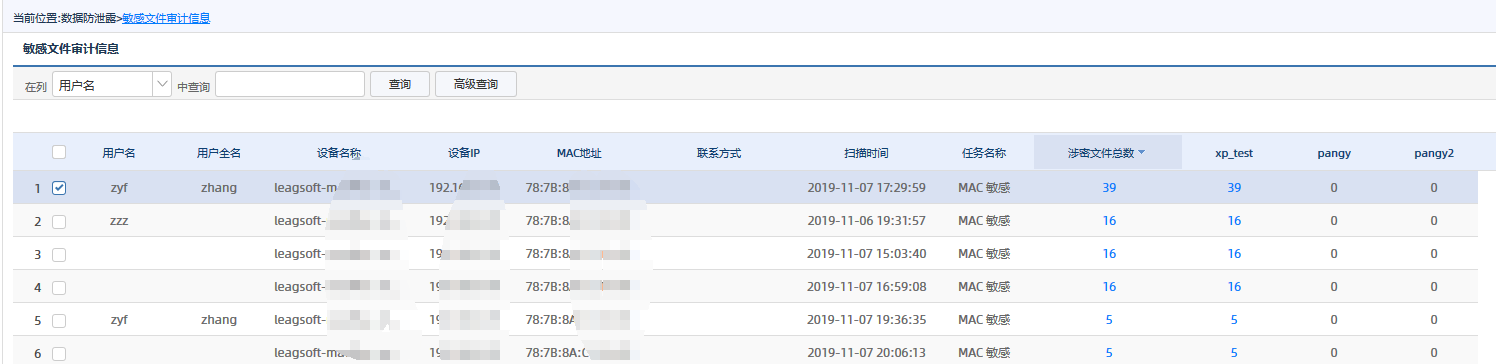


图 9‑5 敏感文件审计信息

### 敏感数据分布

通过敏感文件审计策略对敏感数据进行发现后，LeagView提供可视化界面展示敏感数据的分布，帮助管理员了解各部门终端存储敏感文件的情况。

进入【数据分析|数据分析|敏感数据分布】查看敏感数据分布情况。

该页面首先按照时间和部门筛选需要展示的数据范围，数据展示组件介绍如下：

|  |  |
| --- | --- |
| 组件 | 说明 |
| 按照敏感数据等级统计 | 第一个仪表盘统计全网发现到的敏感文件总数，后面一次展示各个敏感等级的文件总数 |
| 敏感数据变化趋势 | 按照时间轴展示敏感文件数量的趋势 |
| 敏感数据在各个部门分布情况 | 按照部门展示敏感数据所占百分比 |
| 按照文件数查看敏感数据分布 | 左侧饼图展示每个敏感等级所在百分比，右侧条形图展示每个部门敏感文件数 |
| 按文件大小查看敏感数据分布 | 以文件大小的维度展示各个等级、各个部门的敏感数据分布情况 |
| 敏感数据用户分布情况 | 以用户的维度分别展示文件数、文件大小、命中次数，统计前10名用户 |

### 敏感文件自检

LeagView除了可以统一扫描发现敏感文件外，还提供了敏感文件自查工具，让终端用户自查终端上的文件，发现敏感文件后并做相应的处理，以满足合规的要求，也避免自己造成敏感数据泄露。

敏感文件自检工具集成到了安全助手上，终端用户在助手托盘右键菜单中，选择【敏感文件自检工具】，即可允许自检工具。

【注意】需要在助手客户化的时候，勾选“右键托盘菜单“敏感文件自检工具...”，终端用户才能在助手上打开运行此工具。

工具的界面如下图 9‑6



图 9‑6 敏感文件自检工具

敏感文件自检工具使用流程如下：

1、在【主要】选项卡选择敏感检查模板，下拉勾选需要的检查模板，可以同时选择一个或者多个模板。

快速扫描：扫描文件时，按照敏感检查模板从前到后的顺序进行检查，匹配上其中一个模板就结束扫描。

完整扫描：扫描文件时，所有的敏感检查模板都需要进行检查，扫描结果可能会匹配多个模板。

文件名：配置需要扫描的文件名称的关键字后，只扫描文件名包含关键字的文件。

包含文本：配置需要扫描的文件内容包含的关键字后，只扫描内容包含关键字的文件。可以配置多个关键字，每个关键字之间用空格隔开，例如“秘密 机密”。

【注意】：如果既配置了敏感检查模板，又配置了“文件名”和“包含文本”关键字，则会先按照关键字筛选出特定的文件，再进行敏感检查模板匹配，提高敏感检查效率。

2、可以在【文件大小】、【修改时间】、【文件类型】对扫描的对象进一步筛选，如果不配置将按照默认值进行扫描。

3、配置扫描路径，全盘扫描或自定义路径扫描，自定义路径如果配置多条路径会自动过滤掉重复的路径。

4、点击“开始”按钮开始扫描任务，可以暂停任务或继续任务，右下角的【摘要】实时统计扫描结果。

5、支持增量扫描，已扫描过的文件下次将不会再次扫描，除非文件被修改过。

6、扫描结束后在文件列表处选择文件右键菜单可以执行打开、打开文件位置、标记非敏感、和删除操作。对某个文件标记非敏感后，下次将不会再扫描该文件，除非文件被修改过。在【已标记文件】菜单可以看到被标记过的文件。

7、每次扫描任务结束或者停止，都会自动生成历史记录，在【历史记录】菜单可以查看所有的扫描历史记录，打开某个历史记录可以看到完整的扫描结果。

## 终端数据通道管控

LeagView支持通过WEB控制台统一设置终端数据通道管控策略，LeagView后台在安全助手连通时将终端数据通道管控策略下发给安全助手，由安全助手依据LeagView后台配置的策略内容对终端数据通道进行管控，实现对终端数据通道日常使用的灵活控制和审计，以及进一步实现对终端数据通道的集中式管理的需求。

### 上网审计策略

上网审计策略，通过建立URL访问控制列表，来实现对终端的WEB浏览进行控制。

进入【终端安全|安全策略设置|上网审计策略】，单击增加策略按钮，可以配置一个新的上网审计策略。在【策略配置】页面可以配置上网审计策略的上网审计控制规则，用户自定义提示，上传时的配置。其中策略配置说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 编辑上网审计控制规则 | 上网控制规则列表包含一条或多条控制规则，按照从上到下的顺序匹配 |
| 增加 | 点击增加按钮，可以自定义增加上网控制规则；执行条件：满足进程、网站分类敏感规则模板条件，才执行后面的动作；执行动作：当满足前面的执行条件后，再执行相应的审计、阻断等动作 |
| 编辑网站列表 | 系统已经内置了常见的网站分类库，如果需要控制的网站不在库中，可以增加新的网站分类库，例如增加一个所有网站的库，前缀选择http(s)://，网址用\*代替，表示所有 |
| 自定义提示功能 | 点击禁止时弹出提示的前面的正方形框框，会弹出一个文本框，您可以在里面填写您想在禁止操作时弹出的提示信息；同理还有：审计URL时弹出提示、审计上传文字时弹出提示、审计上传文件时弹出提示 |
| 上传配置功能 | 选择是否审计记录保存在本地，不上传到后台与选择合适的文件服务器配置 |
| 其他 | 是否允许通过代理上网，只有使用代理服务器上网时才有效 |

【注意】：默认的情况下，上网审计策略仅支持仅支持ie和http方式的域名、全路径审计，部分文本和文件的上传，其他浏览器不支持，如需支持其它浏览器，需增加扩展配置：use\_kfw=1。

进入【终端安全|信息查询|上网审计信息】查看相应审计信息（包括明细查看和根据设备统计查看两种模式），支持查询、高级查询、导出等。

进入【综合报表｜数据分析报表 | 上网审计报表】查看分析报表，支持查询、统计、多种形式展示、导出、打印等。

**策略示例：**

需求：禁止用户通过上网浏览网页的方式外发敏感文件。

配置步骤：

1. 配置上网审计策略，添加上网审计控制规则，且增加扩展配置：use\_kfw=1如图 9‑7所示：

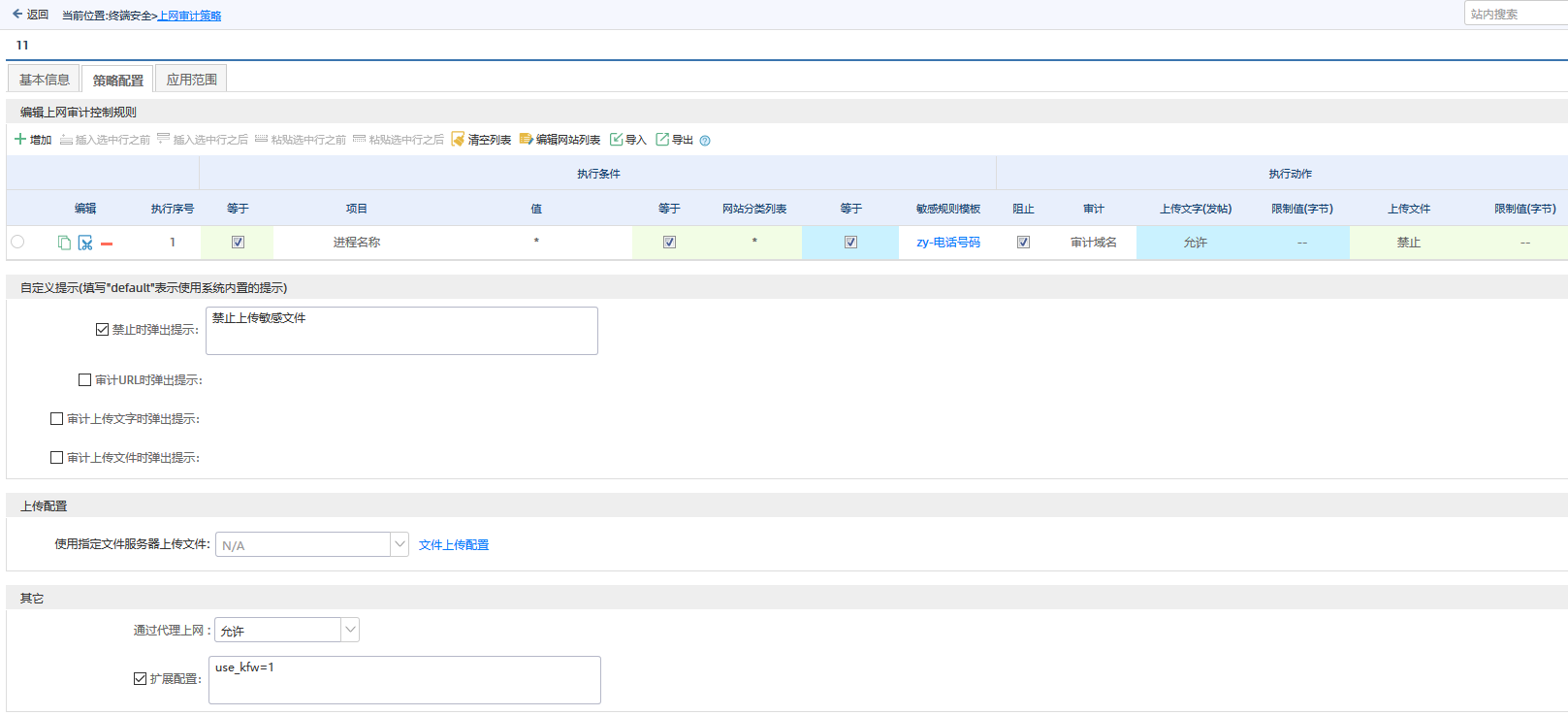


图 9‑7 上网审计策略设置

1. 进入【终端安全|信息查询|上网审计信息】查看相应审计信息，如图 9‑8所示：

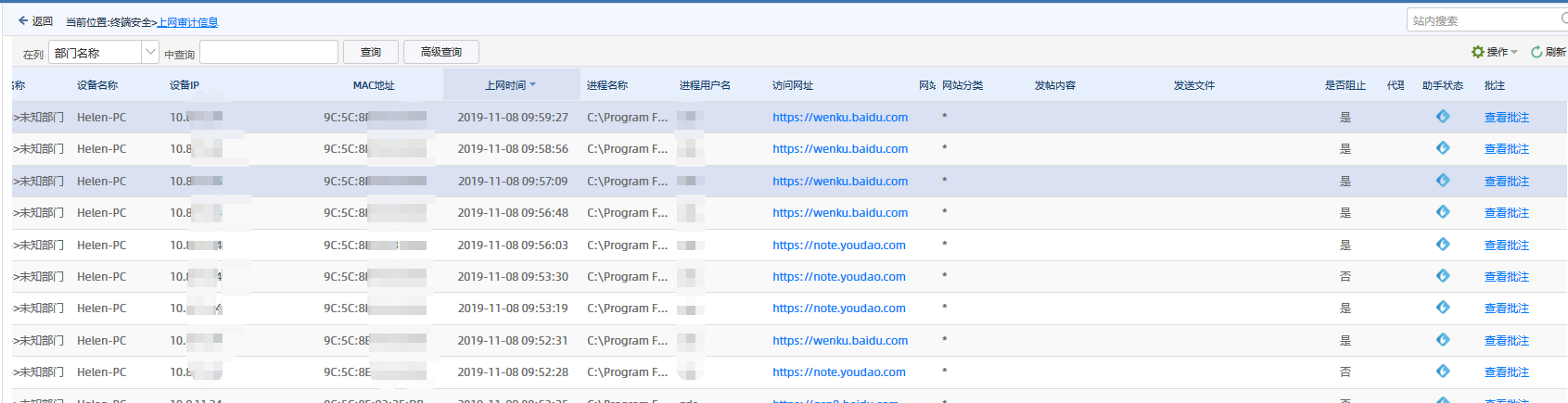


图 9‑8 上网审计审计信息

### FTP访问控制策略

FTP访问控制策略，通过建立FTP访问控制规则，可以持续性、周期性管控FTP访问控制否权限、操作等。

进入WEB控制台选择**【终端安全|安全策略设置|FTP访问控制策略】，**这个页面中列出了系统中已经配置好的FTP访问控制策略，点击指定FTP访问控制策略名称的超链接可以修改已经配置好的FTP访问控制策略，点击增加策略按钮，可以配置一个新的FTP访问控制策略，点击增加规则，配置说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 进程 | 需要控制的FTP客户端进程 |
| IP/域名 | FTP服务器的IP或者域名 |
| 端口范围 | FTP服务器的端口 |
| FTP操作 | 勾选需要控制的FTP操作，敏感规则只匹配上传操作，其余均不匹配。其他命令不支持阻止动作 |
| 本地文件路径 | 如果FTP操作为“上传”时，需指定本地路径 |
| 远程路径 | 如果FTP操作为“上传”时，需指定远程路径 |
| 敏感规则模板 | 如果FTP操作为“上传”时，可以配置敏感规则模板进行敏感检查 |
| 动作 | 当匹配上述条件时，执行相应的管控动作 |
| 文件服务器配置 | 如果上诉动作勾选了“异步上传”则需要指定上传审计附件的服务器 |

在【策略配置】页面可以配置FTP访问控制策略的访问控制规则。如进程、IP/域名、端口范围、FTP操作、本地文件路径、远程文件路径、敏感规则模板等。

进入【终端安全|信息查询|FTP访问控制信息】查看相应审计信息，支持查询、高级查询、导出等。

**策略示例：**

需求：禁止用户将敏感文件上传到FTP服务器。

配置步骤：

1. 进入WEB控制台选择**【终端安全|安全策略设置|FTP访问控制策略】，**点击增加策略按钮，可以配置一个新的FTP访问控制策略，配置如图 9‑9所示：



图 9‑9 FTP访问控制策略配置

1. 进入【终端安全|信息查询|FTP访问控制信息】查看相应审计信息，如图 9‑10所示：

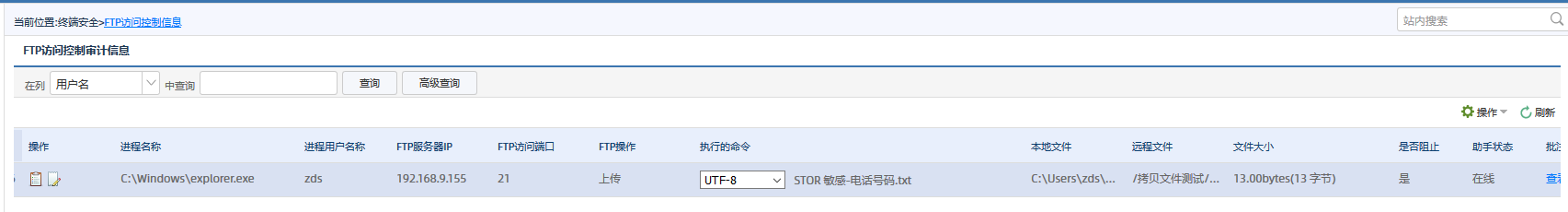


图 9‑10 FTP访问控制审计信息

### 非授权外联策略

通过设置非授权外连策略，安全助手可以实现对终端常见的数据通道如“红外、蓝牙、软驱、串行接口、并行接口、1394接口、PCMCIA接口、外联internet设备、自建Wi-Fi热点、无线以太网卡、智能设备连接、光驱等”进行灵活的、严格的、有效的管控，实时发现违规操作进行通知并阻止或审计。除此之外，通过设置非授权外连策略还可以灵活的配置策略周期性的检测终端其它行为如“互联网是否连通、新接入的外设、是否同时使用两个以上网络端口（只对TCP通信起作用）、执行未注册U盘上的应用程序、执行已注册U盘上的应用程序、其它设备连接情况”，以及对USB大容量存储设备的管控。从而从技术角度上提供了保证终端数据的安全性和可靠性的方法，结合高效的管理制度，可实现对终端数据及数据通道的控制效率和管理质量。

进入【数据防泄露|终端数据通道管控策略|非授权外连策略】，点击增加策略按钮，进入【非授权外连】页面。

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 红外 | 定义使用红外方式传输数据允许还是禁止 |
| 蓝牙 | 定义使用蓝牙方式传输数据允许还是禁止 |
| 软驱 | 定义使用软驱是允许还是禁止 |
| 串行接口 | 定义使用串行接口是允许还是禁止 |
| 并行接口 | 定义使用并行接口是允许还是禁止 |
| 1394接口 | 定义使用1394接口是允许还是禁 |
| PCMCIA接口 | 定义使用PCMCIA接口是允许还是禁止 |
| 外联Internet设备 | 定义能够访问互联网Internet设备方式允许还是审计、禁止、审计并禁止 |
| 自建WIFI热点 | 定义使用WIFI热点方式允许还是审计、禁止、禁用并审计 |
| 上报检测到的新接入外设 | 检查终端所有接入的设备，如果检查到有新设备，则会产生事件，可以在非授权外连信息中查到 |
| USB大容量存储设备 | 定义使用USB大容量存储设备管控方式，当禁用并审计USB大容量存储设备，同一被禁用U盘只有第一次在终端上插入时，才会生成审计记录及产生告警事件。  配置未注册设备只读需要重启终端设备 |
| 无线以太网卡 | 定义无线网卡的管控方式 |
| 智能设备连接 | 定义对智能设备的管控方式，智能设备指智能手机等设备 |
| 同时使用两个以上网络端口 | 允许：不做任何限制，此时"例外网卡"配置不生效。审计：如果有多个网卡，将会把所有网卡的名称上报到后台。禁用TCP通信：将所有网卡的TCP通信禁用，直到系统只有一个网卡生效为止。禁用TCP通信并审计网卡：禁用TCP通信并审计网卡。禁用非助手与后台通信的网卡：检查到有多个网卡可以通信，禁用非助手与后台通信的网卡。禁用非助手与后台通信的网卡并审计网卡：检查到有多个网卡可以通信，禁用非助手与后台通信的网卡并审计网卡 |
| 执行未注册U盘上的应用程序 | 定义未注册U盘上的可执行程序的管控方式，未注册U盘即普通的U盘，未使用LeagView的U盘注册工具进行注册的U盘，禁止U盘上可执行程序运行，可以有效防止U盘传播病毒 |
| 执行已注册U盘上的应用程序 | 定义已注册U盘上的可执行程序的管控方式，已注册U盘即已使用LeagView的U盘注册工具进行注册的U盘，禁止U盘上可执行程序运行，可以有效防止U盘传播病毒 |
| 光驱 | 定义光驱的管控方式，光驱禁用策略针对的是终端接入的所有的光驱，一旦光驱禁用策略生效，所有的光驱将不能正常工作。但是在某种场景下，客户不希望某一些特殊的光驱被禁用掉。例如银行常用的USBKey。对此，可采用例外处理。可采用光驱驱动的友好显示名称来做例外的参数。获取途径：右键光驱对应的盘符，选择属性，在弹出的对话框中选择硬件，选中光驱对应的驱动显示名，点击属性，在弹出的对话款中选择详细信息->属性->友好名称，即可得到；  例外格式：fname=xxx 支持\*匹配，不区分大小写。如fname=USB Token EasyPlay USB Device, 亦可：fname=\*EasyPlay USB Device 当配置了上传服务器时，例外不可用，同时配置了例外和上传服务器则以上传服务器为主。 |

进入【数据防泄露|信息查询|非授权外连信息】可以查看本策略产生的审计信息，并导出为Excel的文件以分析。

**策略示例：**

需求：禁止终端用户将敏感文件刻录到光驱进行外发

配置步骤：

1. 配置非授权外联策略禁用所有光驱的刻录，此时仅允许使用联软提供的专门刻录工具进行刻录和审计，如图 9‑11所示：



图 9‑11 非授权外联策略配置

1. 配置文件读写操作审计策略，添加一条控制规则，进程名称填写ltb.exe，动作：复制剪切，源文件和目标文件选择所有设备类型并使用\*匹配所有路径和所有文件名，敏感规则模板选择已经配置好的模板进行敏感扫描，控制动作勾选“禁止”“审计”“上传”，如图 9‑12所示：

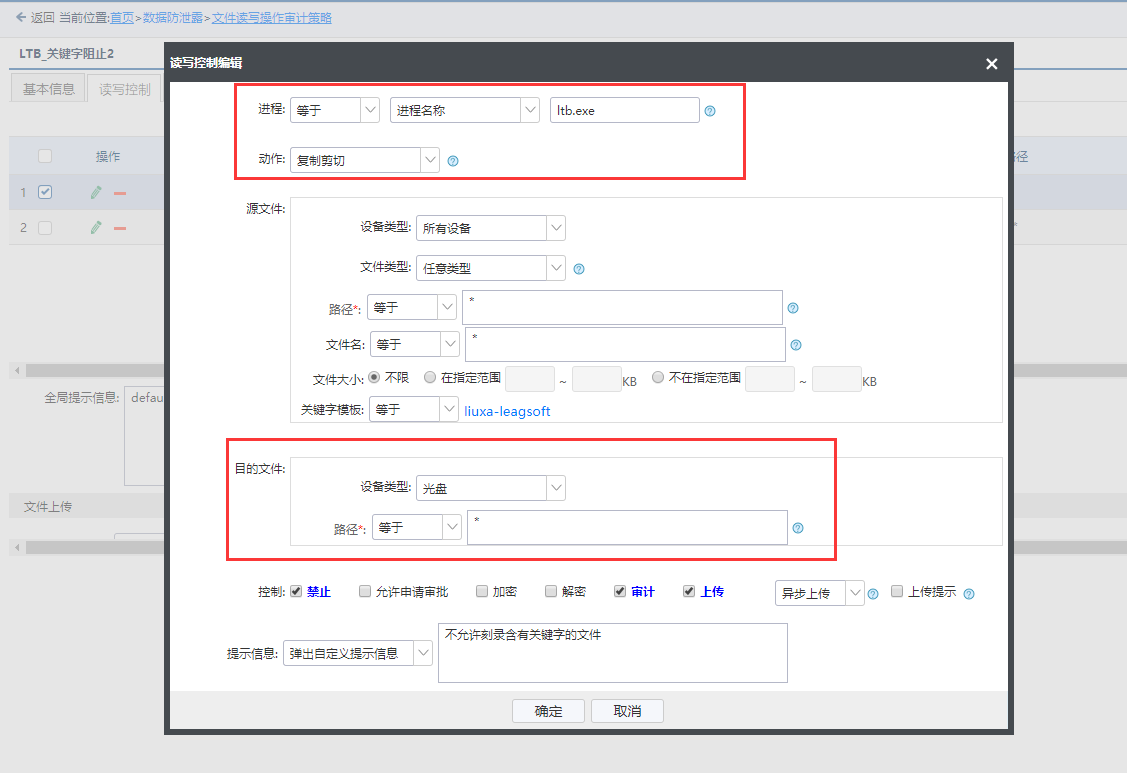


图 9‑12 文件操作读写控制策略-光盘刻录审计配置

1. 通过上述策略配置后，终端用户只能使用联软提供的专门刻录工具进行文件刻录，当刻录的文件包含敏感信息时将会被阻止

### 硬件设备管理策略

LeagView支持根据设备属性管控外设，以实现对具体型号的外设进行精准管控的效果。管理员可以从后台实时获取终端接入外设的硬件属性并一键添加至管控策略。大幅提升了管理效率。

本策略能管控计算机【设备管理器】中所有支持“禁用”的外设。对于系统不提供“禁用”功能的设备，本策略不支持管控。如要确认哪些设备可能被禁用，建议通过在终端操作系统的【设备管理器】中查看外设是否存在“禁用”选项。

硬件设备管理策略可以通过设备属性的类Guid、类描述、设备实例路径、显示名称、设备描述、设备服务名对设备进行匹配，这些信息可以在终端主机操作系统上，【设备管理】配置页面中，选择某一个设备，右键菜单，选择属性，选择详细信息TAB查询设备属性信息，如下图 9‑13 设备属性信息

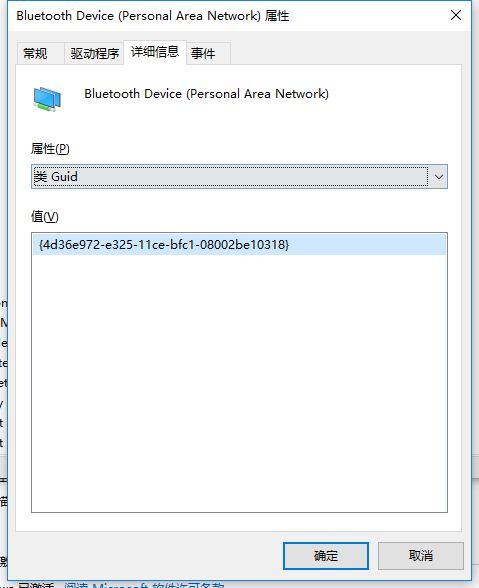


图 9‑13 设备属性信息

在策略配置中，配置一条ACL，使得符合本条ACL所有非空配置项的外设才能被匹配并执行对应动作。设备属性支持 \* 匹配。匹配后，本外设不会在之后的ACL里被匹配。本策略会根据执行序号从小到大的顺序应用ACL。

如果已经产生审计信息，需要进行策略的后续维护（将误禁用的外设加白），则建议在【非授权外连 | 信息查询 | 硬件设备审计信息】中，选择要加白的外设的审计信息（选择一个或多个均可）添加至已有策略中，效果即为所选外设会成为该策略执行序列最高的ACL，默认控制方式为允许，不会弹出提示信息。

【注意】若用户希望通过白名单管控外设，建议先查看外设列表中，是否有可以根据属性特征合并的设备：例如，若要确保系统的正常运行，可以配置多条ACL：类描述分别为**System、Monitor、LegacyDriver、，其他项均略过，控制为允许的ACL。**

**策略示例：**

需求：管理员希望通过黑名单管控外设，例如禁用USB但不影响鼠标、键盘、打印机等设备的使用

配置步骤：

配置硬件设备管理策略，添加以下ACL规则：

1. 设备描述：\*keyboard\*，允许；
2. 设备描述：\*mouse\*，允许；
3. 类描述：USB，禁止并审计；

如图 9‑14所示：



图 9‑14 硬件设备管理策略配置

这样能够确保：USB键盘鼠标不会因为USB被禁用而被禁用。

在【非授权外连 | 信息查询 | 硬件设备审计信息】中查看被禁止的设备的审计信息，如图 9‑15所示：

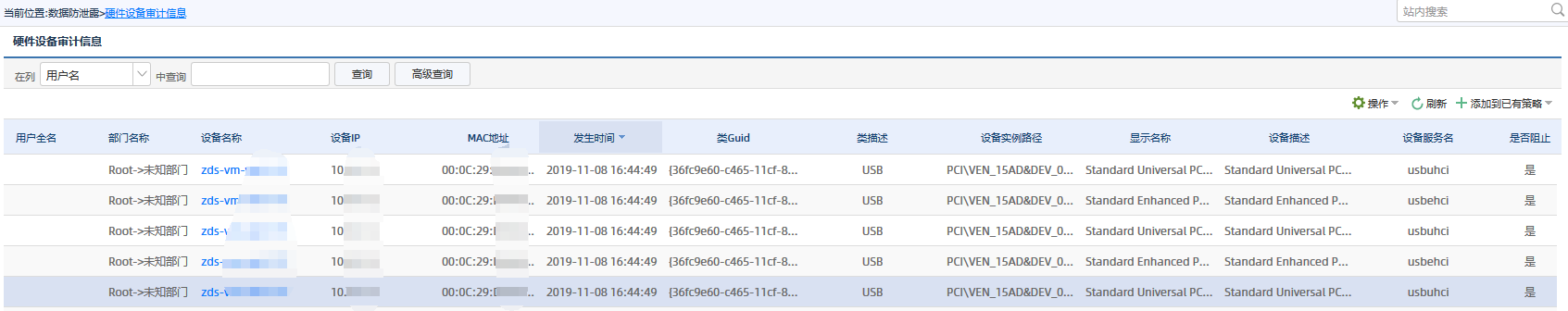


图 9‑15 硬件设备管理审计信息

### 文件读写操作审计策略

通过设置文件读写操作审计策略，终端安全助手收到策略后可以实现对终端上的“本地硬盘、未注册U盘、已注册U盘、加密U盘、网络共享、所有U盘、光盘、软盘”等常见存储介质进行文件读写操作的管理，包括：“允许、禁用、审计、上传”等管控手段，并集合高效的ACL控制方式可灵活的对各种文件读写操作行为进行管理和控制，适用于多种多样的文件流转场景进行控制。

进入【数据防泄露|终端数据通道管控策略|文件读写操作审计策略】，点击增加策略，进入【读写控制】页面，点击增加，弹出【读写控制编辑】窗口，其中的各个配置项说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 进程 | 填写与这条规则匹配的进程条件。当选择“进程名称”，“进程文件CRC校验值”，“软件名称”，“目录名称”，“已签名进程”时，其值不可以为空。支持\*号匹配 |
| 动作 | 选择要管控的终端动作。对光盘的管控动作只支持“读”审计;光盘“写”、“复制剪切”等操作实际属于“刻录”，关于“刻录”操作，需要使用“非授权外联”策略中的“光驱”选项进行管控 |
| 文件 | 选择、输入文件的所在设备类型（例如本机硬盘、未注册U盘、网络共享等）、路径、文件名、文件大小和匹配的敏感规则模板 |
| 控制 | 对终端文件操作的管控 |
| 提示信息 | 终端被控制读写操作时弹出的提示信息 |

进入【数据防泄露|信息查询|文件读写操作审计信息】可以查看本策略产生的审计信息，并导出为Excel的文件以分析。

**策略示例：**

需求：禁止终端用户拷贝敏感文件到U盘

配置步骤：

1. 配置文件读写操作审计策略，添加一条控制规则，进程名称填写\*匹配所有进程，动作：复制剪切，源文件选择所有设备类型并使用\*匹配所有路径和所有文件名，目标文件选择“所有U盘”，敏感规则模板选择已经配置好的模板进行敏感扫描，控制动作勾选“禁止”“审计”“上传”，如所示：

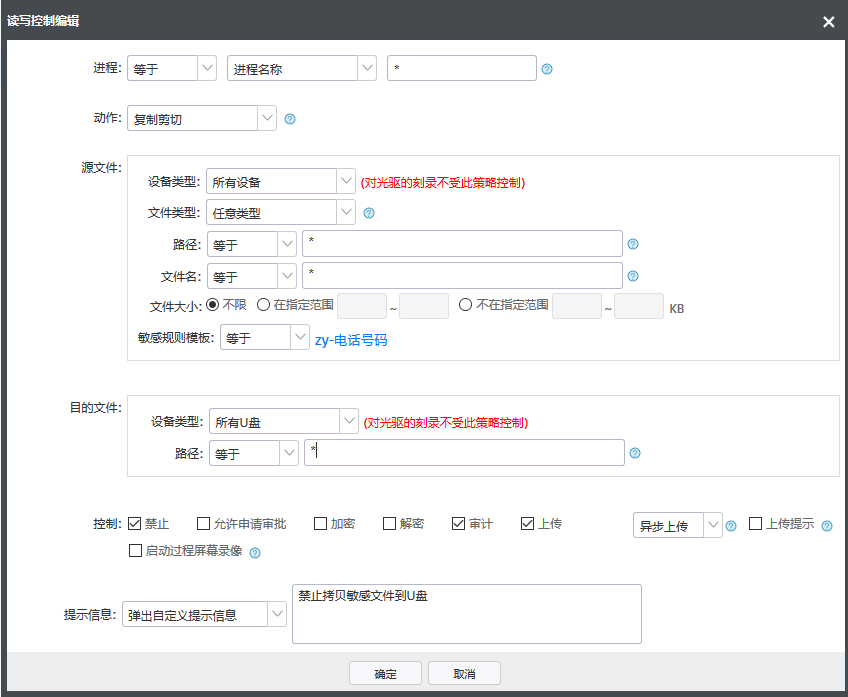


图 9‑16 文件操作读写审计策略配置

1. 将策略下发到终端，当终端用户拷贝文件到U盘时触发敏感检查，敏感文件将被阻止拷贝，非敏感文件可以正常拷贝到U盘。
2. 进入【数据防泄露|信息查询|文件读写操作审计信息】可以查看本策略产生的审计信息，如图 9‑17所示：



图 9‑17 文件操作读写审计信息

### 打印控制策略

通过设置打印控制策略，终端安全助手收到策略后可以实现对终端通过打印机进行文件打印操作的控制、审计和上传打印文件到指定网络共享位置。可以有效降低通过文件打印导致数据泄漏的风险，大大提高对打印机使用的管理和控制力度。

此策略可单独使用，可配合业务数据防泄漏策略使用，可配合审批方案和业务数据防泄漏策略使用。打印监控策略配合业务数据防泄漏策略一起使用，控制其业务系统的打印及打印水印方式和非/受控盘数据的打印及打印水印的方式。

在WEB控制台页面中选择【数据防泄露|终端数据通道管控策略|打印控制策略】，点击增加策略，进入【策略设置】页面，点击增加，弹出【编辑】窗口。管理员可以在这里根据打印机、进程、数据源和敏感规则模板匹配文件，并选择对打印行为的管控方式。

其中的各个配置项说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 打印机 | 可以指定一个或多个特定的打印机型号。名称支持\*号匹配  例如填写“\*HP\*”表示匹配所有的包含HP的打印机型号 |
| 进程 | 调用打印机的进程，指定一个或者多个进程，名称支持\*匹配 |
| 数据源 | 选择打印数据的来源，分三大类，业务系统、安全虚拟磁盘、其它（如C盘或者非业务系统） |
| 内容匹配模板 | 选择已经定义的敏感规则模板 |
| 执行动作 | 选择符合策略条件时执行的动作，并且可以添加水印方案 |

进入【数据防泄露|终端数据通道管控策略|打印控制审计信息】可以查看本策略产生的审计信息，并导出为Excel的文件以分析。

**策略示例：**

需求：禁止打印包含敏感信息的文档。

配置步骤：

配置打印控制策略，添加一条控制规则，打印机选择所有打印机，进程使用通配符\*匹配所有进程，数据源选择“所有”，内容匹配模板选择已配置好的敏感规则模板，用于敏感信息检查，执行动作“禁止并审计”。如图 9‑18所示：

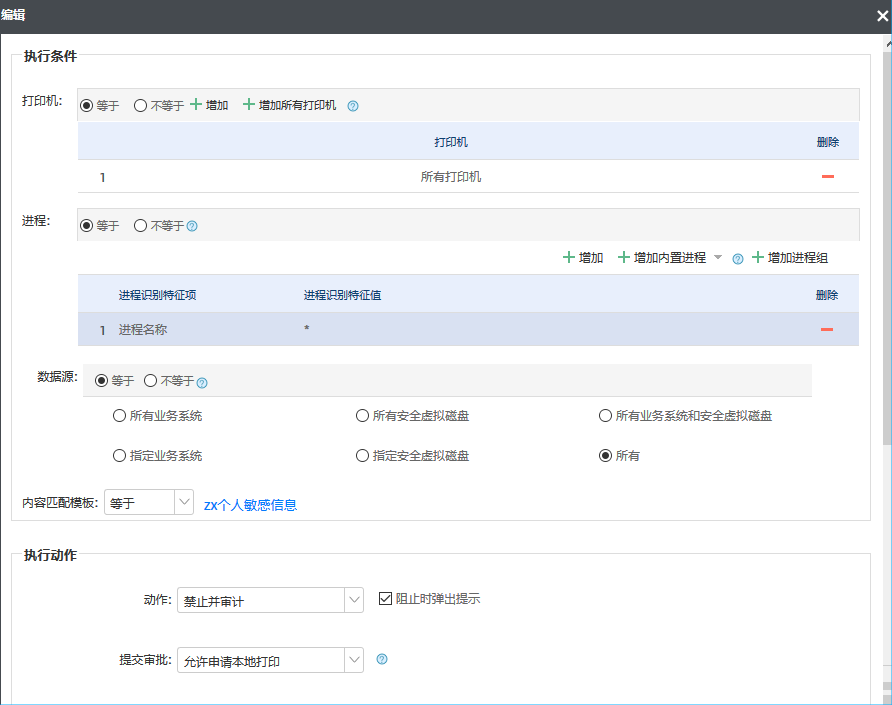


图 9‑18 打印审计策略配置

将策略下发至终端后，终端用户打印文档时，如果文档中包含敏感信息将会被阻止打印，如果打印非敏感文件将不受影响。

进入【数据防泄露|终端数据通道管控策略|打印控制审计信息】可以查看本策略产生的审计信息，如图 9‑19所示：

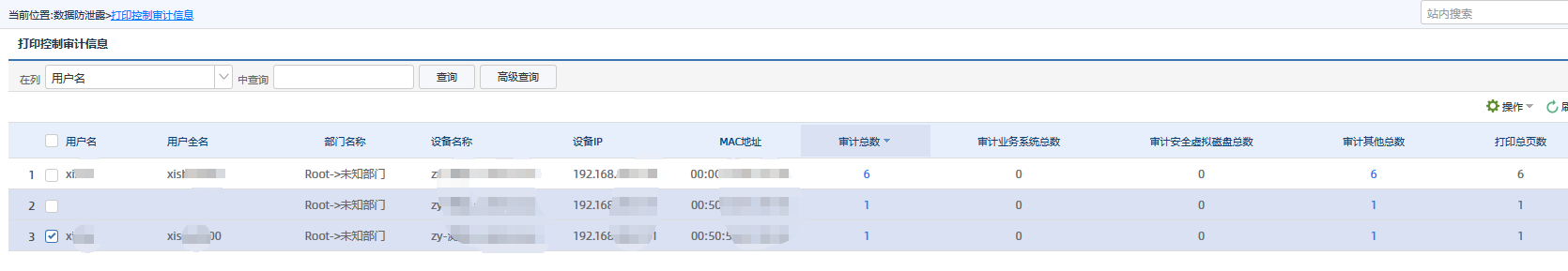


图 9‑19 打印审计信息

### 即时通讯审计策略

通过设置即时通讯审计策略，终端安全助手收到策略后可以根据策略内容实现对终端使用的即时通讯聊天软件进行内容审计和控制，目前可有效控制的即时通讯工具包括“QQ、微信网页版、微信客户端、企业微信”等，可有效的对这些即时通讯聊天客户端进行“启动控制、文本控制、聊天图片控制、发送可识别文件控制、发送不可识别文件控制、接受可识别文件控制、接受不可识别文件控制”。从而可以有效的对即时通讯客户端工具进行管理和控制。从而保证企业涉密和安全信息数据不会轻易被窃取和传播，大大减低风险和管理成本。

进入【数据防泄露|终端数据通道管控策略|即时通讯审计策略】，点击增加策略，进入【策略设置】页面。配置项说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 聊天客户端 | 支持的即时通讯软件名称 |
| 启动控制 | 配置是否允许运行该软件 |
| 文本控制 | 配置该软件是否能发送文字信息 |
| 聊天图片控制 | 配置该软件是否能发送图片信息发送可识别文件控制 |
| 模板条件 | 配置当聊天文本、文件存在等于或不等于敏感规则模板时，进行后续动作 |
| 敏感规则模板 | 配置匹配的敏感规则模板，支持配置多条敏感规则模板 |
| 关键字匹配时控制 | 配置当满足“模板条件”、“敏感规则模板”时，对应的控制方式 |
| 发送可识别文件控制 | 配置该软件是否能发送可识别文件，可识别文件指DLP能够支持识别的文件格式，如doc、docx等 |
| 发送不可识别文件控制 | 配置该软件是否能发送不可识别文件，不可识别文件时指dll、exe等非文档类的文件 |
| 弹出提示 | 配置该策略在被触发式客户端提示格式 |
| 文件服务器配置 | 指定网络服务器共享位置，截取出来的图像文件将会被备份到此目录，此目录需要有写的权限 |
| 审计范围 | 配置对聊天客户端中帐号的审计范围 |

【注意】对于Web微信，默认仅支持ie如需支持其它浏览器和邮箱，需配置扩展配置：use\_kfw=1.

进入【数据防泄露|信息查询|即时通讯审计信息】可以查看本策略产生的审计信息。本页面支持两种显示方式：【聊天模式】、【列表模式】。两种模式下，管理员均可以查看聊天信息中命中的敏感模板内容并对聊天信息进行审批。

【聊天模式】下，审计信息会实时地以类似即时通讯软件会话页面的格式展现。选择设备、发送方账号，再选择接收方账号，即可看到双方被审计的聊天内容。本模式支持图片的查看。

【列表模式】下，每一条审计信息都以详细信息的格式显示。管理员可以将本页面的审计信息导出为Excel文件。

策略示例：

需求：禁止终端用户通过QQ外发敏感文件

配置步骤：

配置即时通讯审计策略，配置QQ的敏感规则模板，关键字匹配时控制选择“发送时阻止”，如图 9‑22所示：



图 9‑22 即时通讯审计策略配置

将策略下发至终端，当用户通过QQ发送敏感文件时就会被阻止，但不影响非敏感文件的发送。

### 邮件审计策略

通过邮件审计策略，终端安全助手收到策略后可以对终端上通过Web和邮件客户端发送的邮件，根据策略中的执行条件进行过滤，对符合条件的邮件实施审计和管控。

进入【数据防泄露|终端数据通道管控策略|邮件审计策略】点击增加策略，进入【策略配置】，点击增加，弹出【编辑Email控制列表】弹窗，其中配置项如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 基本配置 |  |
| 邮件 | 仅支持发送邮件的管控和审计 |
| 使用工具 | 按需选择审计web邮件或客户端邮件，可同时勾选。支持的浏览器是IE，Web邮箱是QQ邮箱，126邮箱，163邮箱，yeah邮箱等，支持的客户端有Outlook，Foxmail |
| 执行条件 |  |
| 执行条件匹配规则 | 全部匹配，要求邮件匹配本条中所有执行条件，才认为匹配并做出管控动作。存在匹配，只要邮件能匹配本条中一项执行条件，即认为匹配并做出管控动作 |
| 收件人 | 添加对收件人的条件过滤，支持\*匹配，多个用分号分隔。例如可配置\*或\*@leagsoft.com;\*qq.com。此外，也支持对邮箱组内地址的匹配 |
| 抄送人 | 添加对抄送人的条件过滤，规则同上 |
| 检查邮件标题 | 增加邮件标题关键字过滤条件，仅当邮件标题包含（或不包含）敏感关键字时候执行相关审计（或其他）操作 |
| 检查附件内容 | 增加附件关键字过滤条件，仅当附件包含（或不包含）敏感关键字时候执行相关审计（或其他）操作 |
| 检查邮件正文内容 | 增加附件关键字过滤条件，仅当附件包含（或不包含）敏感关键字时候执行相关审计（或其他）操作 |
| 检查正文大小 | foxmail、outlook计算的是正文内容的字节数大小，图片不计算，图表只审计汉字的大小。（即相当于把所有邮件内容复制到txt中后计算的大小）web邮件计算的是字数，一个汉字，标点，英文字母即为一个字数。（例如单词hello为5个字数大小） |
| 检查附件大小 | 控制附件大小条件，多个附件时候进行累加 |
| IP地址 | 邮件服务器IP地址的过滤，支持IP地址段，多个IP等的配置，支持域名，web邮件支持163;QQ;126配置 |
| 端口 | 邮件服务器端口 |
| 管控动作 |  |
| 动作 | 基本审计：勾选时审计收件人、抄送人、邮件标题3项；审计内容：勾选时审计收件人、抄送人、标题、正文、完整内容6项；审计附件：审计邮件的附件；阻止：阻止发送邮件；上传审计附件：，需配置LVFS地址；审计前询问用户是否继续：勾选后弹出提示框将审计此邮件行为，用户选择“是”将继续，选择“否”取消；上传文件前询问用户是否继续：勾选后上传附件时弹出询问框，用户选择“是”将继续，选择“否”取消；弹出消息：勾选后审计邮件时助手右下角弹出提示信息，提示内容若“弹出提示”中配置了则弹出自定义的提示内容，未配置则弹出默认消息“根据管理规定，您操作的相关记录将会被上传到后台数据库中备份”；邮件网关审批：经过审批后，才能发送邮件，需部署邮件网关才生效 |

【注意】

1、当配置了附件关键字过滤，但邮件不带有附件的时候，直接放行不做审计等操作。

2、多个附件，只有部分附件含敏感关键字时，所有附件都将被审计。

3、 “抄送人”不支持空匹配。当本条内容为：“收件人”包含a且“抄送人”包含a，时（执行动作为“允许”），若某邮件收件人包含a，未配置抄送人，则该邮件不会被匹配，也不会被执行“允许”操作

4、各个条件之间为“与”的关系，即当所有的条件（关键字，大小，IP等）都满足时才进行审计（或阻止）的操作。

5、默认Web邮箱仅支持ie的qq邮箱和163邮箱，如需支持其它浏览器和邮箱，需配置扩展配置：use\_kfw=4。

进入【数据防泄露|信息查询|邮件审计信息】可以查看本策略产生的审计信息，并导出为Excel的文件以分析。

**策略示例：**

需求：禁止用户通过邮件的形式外发敏感文件。

配置步骤：

配置邮件审计策略，添加邮件控制规则，基本配置都勾选上，执行条件勾选检查附件内容，指定敏感规则，选择已经配置好的敏感规则模板；管控动作勾选“基本审计”“审计内容”“审计附件”“阻止”，如图 9‑23所示：

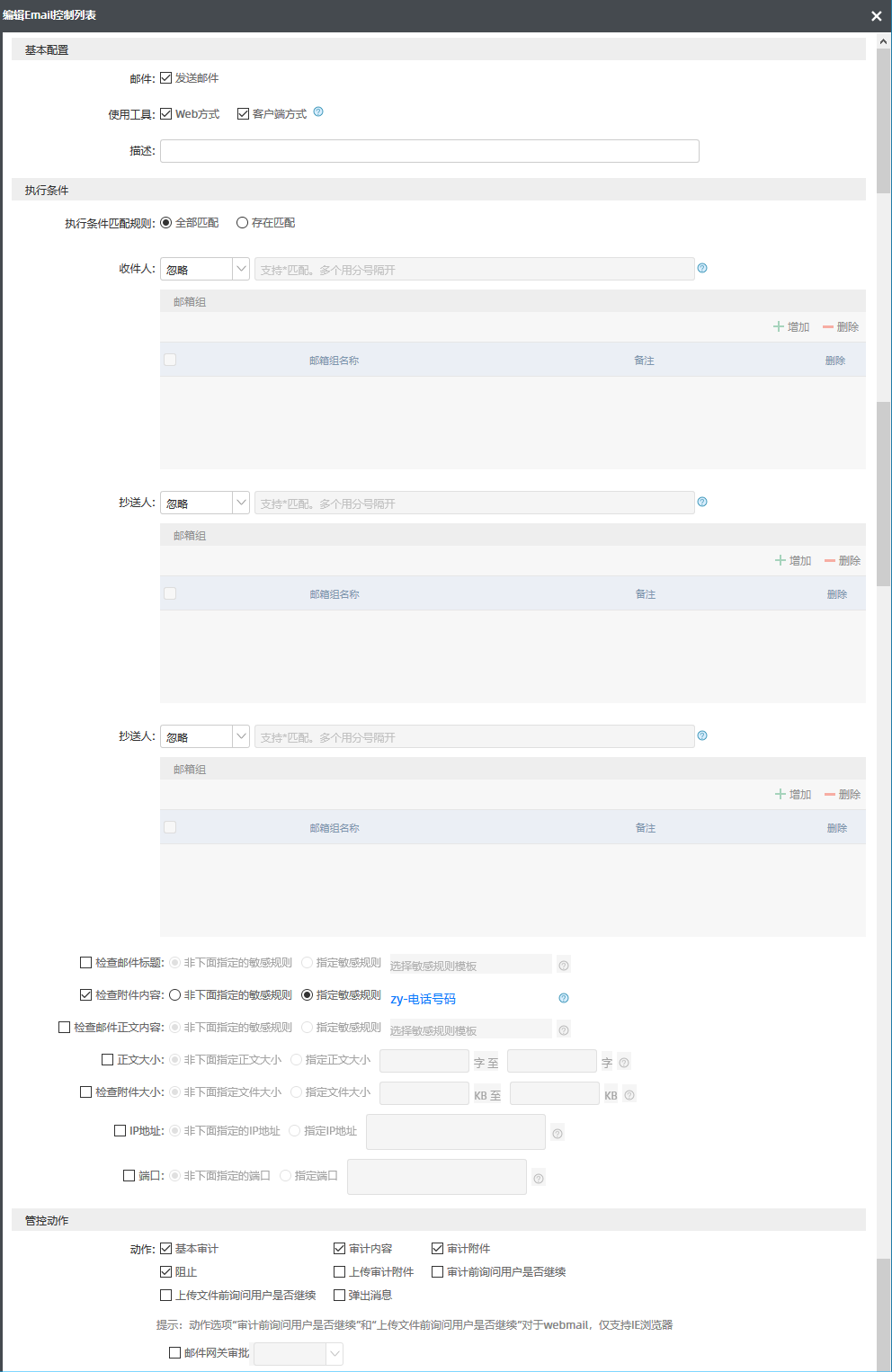


图 9‑23 邮件审计策略配置

将策略下发至终端，当用户发送的邮件附件属于敏感文件时，将会被阻止，但发送非敏感的附件可以正常发送。

进入【数据防泄露|信息查询|邮件审计信息】可以查看本策略产生的审计信息，如图 9‑24所示：

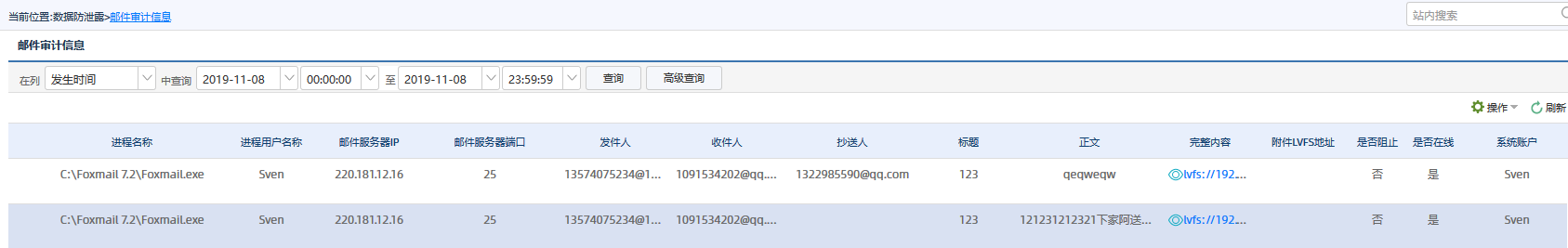


图 9‑24 邮件审计信息

### 移动存储管理

终端用户在日常办公中经常需要通过 U 盘等介质进行数据拷贝，如何对这类介质进行合理的管理控制是困扰很多企业的一个难题。在企业内特别是政府部门中，移动存储介质的管理目前主要依靠制度管理，由于种种原因，这些政策、制度、要求往往难以真正得到贯彻落实。目前，存储保密信息的移动介质缺少身份认证、接入控制等技术防护措施，自身安全防护能力较弱，企业移动存储介质经常处在失控状态，已成为信息安全工作的难点。

LeagView 移动存储介质管理方向大致可以分为三大块，分别为：统一规范使用、使用权限控制及文件加密存储。需要结合非授权外联策略和文件读写操作审计策略才能达到全面管控的效果。

* 统一规范使用

移动存储设备注册，即为每一个移动存储设备生成一个唯一标识，这个唯一标识不能随着设备的读写、更改属性、格式化等日常操作而变更。有了唯一标识的设备就相当于持有身份证的公民，可以合法的在企业内部使用，而没有获得唯一标识的设备则不允许接入办公电脑。

通过非授权外联策略控制，禁用未注册U盘，未经注册的移动存储设备接入办公电脑时会被阻止，并且弹出注册提示框，用户可根据需要自行注册，并提交到后台进行审批。如图 9‑25所示：

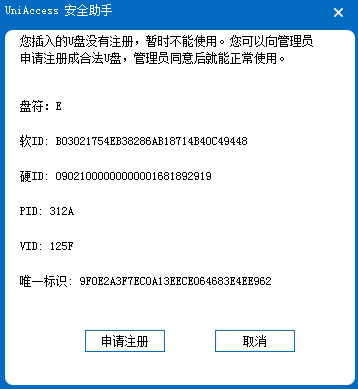


图 9‑25 未注册U盘注册提示

若终端接入的是未允许在本设备上使用的注册U盘，也可以通过指引提交U盘变更申请。

审计管理员（audit账户）登录Web控制台，进入【审批处理|移动存储管理|】【我的待审批】页面展示终端用户提交的注册申请，审批通过后对应的移动存储设备会被注册，并在【移动存储设备信息】页面中显示。

【移动存储设备信息】页面展示所有已注册过的移动存储设备，并可以对移动存储设备的注册、授权、挂失、领用、核销回收等管理。

如果企业内部统一采购了U盘，需要批量注册，审计管理员（audit账户）登录Web控制台，进入【审批处理|移动存储管理|移动存储设备信息】可以在本页面点击下载USB注册工具，安装成功后，插入移动存储设备，通过USB注册工具来对其注册。也可以通过点击操作，选择“手工注册”，来注册移动存储设备。

* 使用权限控制

在 LeagView 中，移动存储设备的日常管理和使用权限管理是分开的。其中【审批处理|移动存储管理|】页面，是设备注册、领用、使用范围、使用时间范围、设备状态等参数配置页面。而移动存储设备的使用权限则通过【数据防泄露|终端数据通道管控策略|非授权外连策略】以及【数据防泄露|终端数据通道管控策略|文件读写操作审计策略】这两个策略实现的。

在移动存储设备权限控制中，非授权外连策略主要是用于移动存储设备接入许可判断（判断移动存储设备是否注册，是否可使用）及移动存储设备可执行程序（移动存储设备内后缀为 exe、com 等文件）运行权限判断。

文件读写操作审计策略主要是对移动存储设备的读写、复制/剪切、导入/导出等操作进行权限控制，未经授权的操作会被阻止。经过策略的灵活配置可以降低在使用移动存储设备时企业核心数据的泄露风险（主动泄密与被动泄密），同时降低移动存储病毒对于企业内部网络的危害。

* 文件加密存储

LeagView 移动存储管理中，如需文件加密存储，则使用安全U盘。安全U盘的介绍参见9.3.12安全U盘。

## 水印服务

办公数字化、高效率的同时，企业信息和数据的安全性也收到了挑战， LeagView提供了数据防扩散方案，通过有代理、无代理水印服务，对屏幕、打印、业务系统进行水印保护，防止通过拍照、截屏、打印等方式泄露和扩散企业信息和数据。做到泄露前教育、警示；泄露后有据可凭，依据泄露结果追溯定位泄露源，防止造成更严重的泄露扩散，保护企业信息安全。

### 有代理水印

有代理水印即需要安装客户端使用的水印功能，使用有代理水印需要配合【全局信息|策略基础数据设置|自定义数字水印】与【数据防泄露|信息查询|屏幕控制策略】、【数据防泄露|信息查询|打印控制策略】才可生效，实现屏幕水印、打印水印。

【全局信息|策略基础数据设置|自定义数字水印】即配置水印方案。可配置内容包括即水印的参数，包括：水印格式、水印显示位置、水印字号、密度、颜色等。详情参见10.1.5自定义数字水印。

【数据防泄露|信息查询|屏幕控制策略】可配置触发水印的进程/进程组，并指定在屏幕显示哪一个自定义数字水印方案。详情参见章节——9.3.8屏幕控制策略

【数据防泄露|信息查询|打印控制策略】可配置触发水印的打印场景、范围；并指定使用哪种自定义数字水印方案。详情参见章节——9.3.6打印控制策略

* 屏幕水印

通过【数据防泄露|信息查询|屏幕控制策略】实现，管理员可以配置：当终端用户打开特定程序、进入特定业务系统或安全虚拟磁盘时，屏幕显示水印。水印内容可以包括：当前时间、用户名、ip地址等信息。水印方案相关详情参见10.1.5**错误!未找到引用源。**。

系统内置进程包含：浏览器、文档编辑器、数据库查询分析器、Telnet/SSH终端、图片编辑器、邮件客户端、工程图纸编辑器、软件开发编辑器。

屏幕水印支持触发形式：

1. 开机触发；
2. 访问指定业务系统或虚拟安全磁盘触发；
3. 访问指定格式的文档触发；
4. 启用指定进程触发；
5. 访问包行指定敏感信息的文档内容时触发。

* 打印水印

通过设置【数据防泄露|信息查询|打印控制策略】，配合【全局信息|策略基础数据设置|自定义数字水印】实现的，支持明文、图片、矢量二维码等水印方案的应用实现。

重点说明——打印矢量水印

打印水印除支持明文、矢量、图片、二维码水印外，针对打印还有独特的打印矢量水印。它区别于矢量水印4\*3点阵的形式，仅在打印场景下生效。打印矢量水印。打印矢量水印以点的形式付于所打印文档中文字的一角，在打印结果中点的数量在用户水印方案设置数字的基础上，根据文档页面中实际文字数量情况随机显示。

* 数字盲水印

数字盲水印实现水印视觉干扰最小化情况下，防止用户通过截屏手段泄露企业信息和数据。

数字盲水印在屏幕上实现0视觉影响，不对屏幕显示进行干预处理，而在用户截屏的瞬间对截屏数据进行加水印，水印信息肉眼几近不可见，支持一般常用截图工具。企业自研发通讯工具或非常用截图工具需定制改功能。

配置实现数字盲水印目前仅支持特殊配置方式，通过【全局信息|策略基础数据设置|自定义数字水印】配置水印方案，描述行里配置hide\_warter=4保存，即完成了数字盲水印配置。如果水印方案中同时还开启了其他水印类型，将同时生效（例如：同时配置了明文水印，且明文水印透明度不为100%，那么既有明文水印信息，截图结果中也会有数字盲水印信息，可以通过数字盲水印追溯页面进行追溯）。

### 水印追溯

系统支持多种水印类型，其中，明文水印、图片水印都属于所见即所得，无需其他特殊追溯手段，二维码水印追溯，通过微信二维码扫描工具扫描即可看到定位到具体泄露源头。所以重点介绍一下矢量水印、打印矢量水印、数字盲水印追溯。追溯功能在当前系统中分布与多个菜单对应多种不同类型的水印追溯，具体说明如下：

* 矢量水印追溯

矢量水印以矢量水印点阵图形为基本单元，以代表“0”的矢量图形为起点标识，通过4\*3的组合方式组成一个完整矢量水印矩阵，矩阵平铺于水印介质上（屏幕/打印结果）。

步骤一：追溯矢量水印首先要从所得泄密结果图片中找到代表“0”的水印图形，明确起点位置。

步骤二：以起点位为依据，向右向下找出矩阵4\*3矩阵中其他所有图形。如一个矩阵范围内图形部分模糊或不完整，可利用其矩阵重复平铺的特性，在周围其他矩阵中寻找和补全。

步骤三：将图形对应的字符按顺序输入【数据防泄露|信息查询|屏幕矢量水印审计信息】页面中查询栏，即可得到相应追溯信息。如未能获得完整的12位字符（包括起始位“0”），缺少的字符位以%代替，进行部分追溯。

* 打印矢量水印追溯

打印矢量水印是将矢量水印点附加于文档中文字的一角来实现。追溯时将附加了打印矢量水印的的对应字符或附加了打印矢量水印点对应的一行字符输入【数据防泄露|信息查询|打印矢量水印审计信息】中查询栏，即可得到相应追溯信息。

* 数字盲水印追溯

在数字盲水印保护下截得的图片，可在获得泄露图片后上传到【数据防泄露|水印服务|水印追溯】菜单下进行追溯。追溯结果成上下两部分在追溯结果图片中显示。

上半部分是一个完整色块，其内显示一个9位的字符串（即水印提取结果），下半部分是由64个方块组成，每个方块中显示内容均一致，选取最清晰的进行识别即可。

64个方块中的水印字符以“#”标记起始，5列2行，一共十个字符，除去起始标识“#”，得到与上半部分相同的9位字符串（即水印提取结果），输入到【数据防泄露|水印服务|水印追溯】页面查询条件中，即可得到追溯结果。

* 自定义数字水印

即自定义水印方案，支持明文水印、矢量水印、图形矢量水印、图片水印、二维码水印以及数字盲水印。通过【全局信息|策略基础数据设置|自定义数字水印】菜单进行配置。

进入【全局信息|策略基础数据设置|自定义数字水印】点击增加按钮即可创建新的自定义水印方案。配置项说明如下：

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 基本选项 |  |
| 水印格式 | 定义明文水印显示内容，支持宏替换参数设置 |
| 首页头部无水印百分比 | 适用于打印场景下红头文件使用的水印方案，通过设置打印时水印避开红头文件首页标题位置。 |
| 数字水印显示位置 | 定义明文水印的的显示样式 并可以开启二维码、图片、矢量等其他水印类型，支持多选 |
| 水印字体、字号 | 定义明文水印字体及字号大小 |
| 水印密度 | 定义水印行、列间距 |
| 水印颜色 | 定义明文、矢量水印的文字/点的颜色 |
| 水印透明度 | 支持0-100透明度设置，即不透明到完全透明，完全透明情况下水印将不可见。 |
| 单行模式 | 勾选单行模式后，明文水印在加载对象上仅显示一行，单行的显示位置可通过对其方式进行设置。  如不勾选，则明文水印内容会在加载对象上重复平铺。 |
| 水印位置 | 定义水印在加载对象上的范围。 |