★完全公开

奇安信天擎终端安全管理系统 V10.0

管理员手册

创建时间：2023 年 12 月 06 日

修改时间：2025 年 4 月 8 日

网络安全服务热线：95015

公司网址：https://www.qianxin.com/

联系地址：北京市西城区西直门外南路 26 号院 1 号楼

邮编：10004

● 版权声明

奇安信集团，保留所有权利。
奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。
对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。
由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

● 免责声明

本免责声明（“**本声明**”）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称“**本产品**”）。**如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。**

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。**您有责任定期检查免责声明部分的内容**，以了解是否发生了变更。**如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。**

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**

2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，**您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。**

3. 您明确理解并同意，**您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5）政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。**

4. **对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。**

5. 对于从**非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品**，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛

伊木马程序或者黑客软件。**使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。**

6. **上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。**

7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利： **在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**

8. 本声明受中华人民共和国法律的约束并依据其解释。

9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

1. 奇安信天擎简介 29

1.1. 产品简介 29

1.2. 产品主要功能 29

1.3. 典型部署场景 30

1.3.1. 互联网络部署方案 30

1.3.2. 隔离网络部署方案 31

1.3.3. 多级级联部署方案 32

1.3.4. 高级版 EDR 部署方案 33

1.4. 典型部署形态 34

1.4.1. 单机部署 34

1.4.2. 集群部署 34

2. 基础功能 36

2.1 基本概念 36

2.1.1. 策略 36

2.1.2. 任务 36

2.1.3. 日志 36

2.1.4. 管理员 36

2.1.5. 强制策略 36

2.1.6. 用户策略 36

2.1.7. 自动分组 36

2.1.8. NAT 地址 37

2.2. 轻量模式 37

2.3. 第三方联动 39

2.4. 典型场景 39

2.4.1. 如何手动删除已卸载的终端 39

2.4.2. 如何进行终端资产管理 39

2.4.3. 如何与 LDAP 服务器进行联动 40

2.4.4. 奇安信零信任与天擎一体化管理 46

2.4.4.1. 零信任数据源配置 47

2.4.4.2. 客户端单点登录配置 48
2.4.5. 第三方产品联动 *51*
2.4.6. IPv6 场景 *51*
3. 终端管理 52
3.1. 终端概况 52
3.1.1. 终端详情 *52*
3.1.2. 终端安全管理 *53*
3.2. 终端分组 55
3.3. 终端任务 56
3.3.1. 分发任务 *56*
3.3.2. 任务执行统计 *58*
3.3.3. 任务管理功能 *58*
3.3.4. 任务设置 *59*
3.3.5. 迁移终端 *59*
3.4. 策略管理 59
3.4.1. 新建、编辑策略 *60*
3.4.2. 自动切换服务器 *63*
3.4.3. 终端兼容配置 *64*
3.4.3.1. HOOK 白名单 65
3.4.3.2. SSL 证书替换白名单 65
3.4.3.3. 网络访问白名单 65
3.5. 终端日志 65
3.5.1. 终端部署日志 *65*
3.5.2. 终端更新日志 *66*
3.5.3. 自我保护日志 *66*
3.5.4. 终端排障日志 *66*
3.5.5. 终端硬件变化日志 *67*
4. 软件管理 68
4.1. 基本概念 68

4.1.1. 软件 68
4.1.2. 软件中心 68
4.2. 软件中心 68
4.2.1. 本地软件 68
4.2.1.1. 软件分类 69
4.2.1.2. 软件上传 70
4.2.1.3. 高级筛选 74
4.2.1.4. 自定义列 75
4.2.2. 云中心软件 75
4.2.2.1. 软件云中心 76
4.2.2.2. 上架设置 76
4.2.2.3. 高级筛选 77
4.2.2.4. 自定义列 78
4.3. 软件管理策略 78
4.3.1. 终端模块 79
4.3.2. 上报已安装软件 79
4.3.3. 软件变更审计 79
4.3.4. 本地软件 80
4.3.5. 定制本地软件 80
4.3.6. 云中心软件 81
4.3.7. 定制云中心软件 81
4.3.8. 个性化定制 82
4.3.9. 更新时间段 82
4.3.10. 安装超时时间 83
4.3.11. 下载设置 83
4.3.12. 更新设置 83
4.3.13. 忽略更新软件列表 84
4.3.14. 必装软件 84
4.3.15. 禁止安装 85
4.3.16. 来源管控 86

4.3.17. 字体统计 87
4.3.18. 关闭云中心软件 87
4.3.19. 任务并发 87
4.3.20. 下载失败重试 87
4.3.21. 客户端软件管家全局配置 88
4.3.22. 软件管理业务告警 88
4.4. 软件终端任务 88
4.4.1. 分组软件任务 88
4.4.2. 终端软件任务 89
4.4.3. 软件查询任务 91
4.5. 终端软件概况 91
4.6. 软件安装统计 92
4.7. 字体统计 94
4.8. 正版化管理 96
4.8.1. 添加统计规则 96
4.8.2. 正版化信息统计 96
4.8.3. 软件活跃度统计 97
4.9. 软件日志 97
4.10. 软件报表 98
4.11. 活跃度统计 98
4.11.1. 添加计划报表任务 98
4.11.2. 统计报表 99
4.12. 业务设置 100
5. 病毒防护 101
5.1. 基本概念 101
5.1.1. 文件等级的定义 101
5.1.2. 病毒扫描 102
5.1.3. 信任区 103
5.1.4. 隔离区 103

5.1.5. 实时防护 103
5.1.6. 主动防御 104
5.2. 病毒防护策略 106
5.2.1. 通用设置 106
5.2.1.1. 检测引擎设置 106
5.2.1.2. 未知文件鉴定 108
5.2.1.3. 信任区 108
5.2.1.4. 文件数字签名 109
5.2.1.5. 隔离区设置 109
5.2.2. 病毒扫描设置 110
5.2.2.1. 病毒处理方式 110
5.2.2.2. 扫描对象设置 111
5.2.2.3. 扫描限制 112
5.2.2.4. 深度查杀 112
5.2.3. 实时防护 112
5.2.3.1. 病毒处理方式 112
5.2.3.2. 实时防护 113
5.2.3.3. 防护文件类型 113
5.2.3.4. 防护操作类型 113
5.2.3.5. 防护资源占用 114
5.2.4. 主动防御 115
5.2.4.1. 病毒处理方式 115
5.2.4.2. 系统防护 115
5.2.4.3. 入口防护 115
5.2.4.4. 系统加固 116
5.2.4.5. 网络防护 117
5.2.5. 定时查杀 118
5.2.5.1. 定时查杀 118
5.2.6. 弹窗设置 119
5.2.6.1. 弹窗模式 119

5.2.7. 高级威胁防御 120
5.2.8. 信创终端病毒防护策略 121
5.2.9. macOS 终端病毒防护策略 124
5.3. 终端任务 126
5.3.1. 全盘扫描 126
5.3.2. 快速扫描 128
5.3.3. 强力查杀 128
5.3.4. 文件专杀 129
5.3.5. 隔离区恢复 129
5.3.6. 查杀未处理 129
5.4. 业务管理 129
5.4.1. 病毒概况 129
5.4.2. 病毒日志 131
5.4.2.1. 病毒查杀日志 131
5.4.2.2. 查杀任务日志 132
5.4.2.3. 攻击防护日志 132
5.4.2.4. 系统防护日志 132
5.4.2.5. 网页安全防护日志 132
5.4.3. 病毒报表 132
5.4.3.1. 报表汇总 132
5.4.3.2. 按终端统计 134
5.4.3.3. 按病毒统计 134
5.4.4. 扫描分析 135
5.4.4.1. 扫描列表 135
5.4.4.2. 列表详情 135
5.4.5. 主防分析 136
5.4.5.1. 实时防护分析 136
5.4.5.2. 主动防御分析 136
5.4.6. 黑白名单 137
5.5. 日常运维管理 138

5.5.1. 提升和保持终端部署率 138
5.5.2. 通过定期扫描提升内网安全 138
5.5.3. 更新病毒库 138
5.5.4. 更新杀毒引擎 139
5.5.5. 更新客户端程序 139
5.5.6. 检修云查杀质量 140
5.5.7. 日常运维告警 140
5.5.8. 处理紧急问题 140
5.5.8.1. 误报处理 140
5.5.8.2. 病毒快速处理 141
5.6. 典型场景 142
5.6.1. 适配网络环境 142
5.6.1.1. 全互联网环境 142
5.6.1.2. 半隔离网 143
5.6.1.3. 隔离网 143
5.6.2. 勒索防护专项 143
6. 补丁管理 145
6.1. 基本概念 145
6.1.1. 漏洞 145
6.1.2. 补丁 145
6.1.3. 补丁号 146
6.1.4. CVE 号 146
6.1.5. 补丁库 147
6.1.6. 补丁库的发布时间 147
6.1.7. 补丁日 147
6.1.8. 灰度分发 147
6.1.9. 奇安信天擎补丁通告 148
6.2. 补丁分发自动化运维思路 150
6.3. 补丁更新设置 151

6.3.1. 服务器更新设置 151
6.3.2. 终端更新设置 151
6.4. 补丁管理策略 151
6.4.1. 补丁安装设置 152
6.4.2. 补丁安装范围 153
6.4.3. 补丁下载安装顺序 154
6.4.4. 补丁及时生效 154
6.4.5. 其他设置 155
6.5. 终端任务 156
6.6. 补丁运维管理 156
6.6.1. 终端补丁概况 156
6.6.2. 补丁文件 157
6.6.3. 停服系统 157
6.6.4. 补丁统计 158
6.6.5. 补丁日志 158
6.6.6. 补丁报表 159
6.6.6.1. 报表汇总 159
6.6.6.2. 按终端统计 160
6.6.6.3. 按分组统计 160
6.6.6.4. 按补丁统计 160
6.7. 终端用户自助修复 160
6.8. 日常运维管理 161
6.9. 典型场景 162
6.9.1. 服务器可连接互联网 162
6.9.2. 纯隔离网 162
6.9.3. 小带宽网络下安装补丁的推荐方案 162
6.9.4. 补丁下载与安装网络优化 163
6.10. FAQ 164
6.10.1. 补丁卸载后，扫描不到 164
6.10.2. 补丁安装失败如何处理 164

7. 主机防火墙 165

7.1. 基本概念 165

7.1.1. 主机防火墙 165

7.1.2. 接管系统防火墙 165

7.2. 主机防火墙策略 165

7.2.1. 主机防火墙设置 165

7.2.1.1. 主机防火墙 165

7.2.1.2. 防火墙规则 166

7.2.1.3. 接管系统防火墙 167

7.2.1.4. 日志上报配置 168

7.3. 业务管理 168

7.3.1. 防火墙概况 168

7.3.2. 防火墙日志 169

7.3.3. 防火墙报表 169

7.3.3.1. 报表汇总 170

7.3.3.2. 按终端统计 170

7.3.3.3. 按分组统计 171

8. 威胁检测与响应（EDR） 171

8.1. 基本概念 171

8.1.1. EDR 171

8.1.2. 威胁情报 171

8.1.3. IOC 172

8.1.4. 进程树 172

8.1.5. 数据字典 172

8.1.6. 威胁响应 172

8.1.7. 筛选 172

8.1.8. 版本 173

8.2. 基础版基本功能 173

8.2.1. 威胁概况 173

8.2.2. EDR 策略 *174*
8.2.3. 威胁告警 *174*
8.2.4. 终端调查 *176*
8.2.5. 威胁处置 *177*
8.3. 高级版基本功能 178
8.3.1. 威胁概况 *178*
8.3.2. 攻击图谱 *179*
8.3.3. EDR 策略 *180*
8.3.3.1. 终端数据采集 180
8.3.3.2. 采集排除设置 181
8.3.4. 威胁告警 *181*
8.3.5. 威胁追踪 *184*
8.3.6. 终端调查 *185*
8.3.7. 威胁处置 *186*
8.3.8. 告警规则信任 *188*
8.3.9. 自定义规则 *189*
8.3.10. 威胁事件评估 *190*
9. 安全登录 191
9.1. 基本概念 192
9.2. 安全登录的设置项 192
9.3. 安全登录使用流程 194
9.4. 典型场景 198
9.4.1. UKEY 损坏、网络不通如何应急登录 *198*
9.4.2. 非龙脉厂商 UKEY 能使用安全登录吗？ *199*
9.4.3. UKEY 被锁定了如何处理? *199*
9.4.4. 用户如果忘记了 UKEY 的 PIN 码如何处理？ *201*
9.4.5. 如何制作一把管理员 UKEY *201*
10. 安全评估 202
10.1. 基本概念 202

10.1.1. 得分 202
10.1.2. 评估类别 202
10.1.3. 否决项 203
10.1.4. 定性标准 203
10.1.5. 评估标准 203
10.2. 基本功能 204
10.2.1. 安全评估业务设置 204
10.2.2. 安全评估标准 204
10.2.3. 安全评估概况 205
10.2.3.1. 终端视角 205
10.2.3.2. 评估项视角 206
10.3. 安全评估策略 206
10.4. 安全评估任务 207
10.5. 安全评估日志 207
10.6. 典型场景 208
10.6.1. 如何快速完成对终端的安全性及合规性标准检查？ 208
10.6.2. 进程对应的软件升级后进程也发生变化，如何减少调整保证设置的黑白名单依然有效？ 208
10.6.3. 评估后发现问题后如何修复 208
10.6.4. 如何计算评估得分 209
11. 基线核查 210
11.1. 基本概念 210
11.1.1. 得分 210
11.1.2. 定性标准 210
11.1.3. 检查标准 210
11.2. 基本功能 211
11.2.1. 基线核查终端定性设置 211
11.2.2. 基线核查标准 212
11.2.3. 基线核查概况 213

11.2.4. 基线核查详情 213
11.3. 基线核查策略 214
11.4. 基线核查任务 215
11.5. 基线核查日志 216
11.6. 基线核查情况统计 216
11.7. 典型场景 217
11.7.1. 如何快速完成对终端的安全性及合规性标准检查？ 217
11.7.2. 进程对应的软件升级后进程也发生变化，如何减少调整保证设置的黑白名单依然有效？ 217
11.7.3. 检查发现问题后如何修复 217
12. 数据防泄漏 218
12.1. 基本概念 218
12.2. 内容知识库 218
12.2.1. 业务说明 218
12.2.2. 内容识别元素 219
12.2.3. 内容添加/维护 219
12.3. 基本功能 223
12.3.1. 数据安全运维基本思路 223
12.3.2. 发送者/接收者 224
12.3.3. Windows 终端数据防泄漏策略设置 224
12.3.3.1. 外发数据实时检测 224
12.3.3.2. 功能配置 226
12.3.4. 信创终端数据防泄漏策略设置 226
12.3.4.1. 外发数据实时检测 226
12.3.4.2. 功能配置 228
12.3.5. 数据泄漏事件 228
12.3.6. 泄漏事件信息溯源 228
13. 安全水印 229
13.1. 基本概念 229

13.1.1. 打印水印 229
13.1.2. 屏幕水印 230
13.1.3. 截屏水印 230
13.2. WINDOWS 终端基本功能 231
13.2.1. 安全水印运维基本思路 231
13.2.2. 打印水印策略设置 231
13.2.3. 屏幕水印策略设置 232
13.2.4. 截屏水印策略设置 233
13.2.5. 屏显水印进程维护 233
13.3. 信创终端基本功能 234
13.3.1. 安全水印基本介绍 234
13.3.2. 打印水印策略设置 234
13.3.3. 屏幕水印策略设置 234
13.3.4. 截屏水印策略设置 235
13.4. MACOS 终端基本功能 235
13.4.1. 安全水印基本介绍 235
13.4.2. 屏幕水印策略设置 236
13.5. 水印信息溯源 236
14. 终端管控 237
14.1. 基本概念 237
14.1.1. 外设管理 237
14.1.2. 进程管理 238
14.1.3. 外发管控 238
14.2. 基本功能 238
14.2.1. 终端维度的互联网出口状态展示 238
14.2.2. 单点维护-进程信息 239
14.2.3. 单点维护-网络信息-网络配置 239
14.2.4. 单点维护-网络信息-网络流量 240
14.2.5. 单点维护-网络信息-网络连接 240

14.2.6. 外设库 240
14.2.6.1. 外设上报 240
14.2.6.2. 外设库统计 241
14.2.6.3. 外设库 241
14.2.6.4. 外设明细 244
14.2.6.5. 外设库更新 244
14.2.7. 进程知识库 244
14.2.7.1. 进程规则 244
14.2.8. WIFI 库 247
14.2.9. 网络出口名单 249
14.3. WINDOWS 终端管控策略 251
14.3.1. 外设管理 251
14.3.2. 进程管理 252
14.3.3. 能耗管理 253
14.3.4. 网络管控 254
14.3.5. 违规外联 254
14.3.6. 远程协助 255
14.3.7. 服务管控 256
14.3.8. 桌面加固 256
14.3.9. 外发管控 257
14.4. 信创终端管控策略 258
14.4.1. 外设管理 258
14.4.2. 违规外联 258
14.4.3. 远程协助 259
14.4.4. 进程管理 259
14.4.5. 能耗管理 260
14.4.6. 网络管控 260
14.4.7. 桌面加固 261
14.4.8. 服务管理 261
14.5. MACOS 终端管控策略 262

14.5.1. 外设管理 *262*
14.5.2. 网络管控 *262*
14.6. 管控日志 262
14.7. 管控报表 263
14.7.1. 外设管理报表 *263*
14.7.2. 进程管理报表 *264*
14.7.3. 违规外联管理报表 *265*
14.7.4. 能耗管理报表 *265*
14.7.5. 网络管控管理报表 *266*
15. 终端审计 267
15.1. WINDOWS 终端审计 267
15.1.1. 文件审计 *267*
15.1.1.1. 文件审计运维基本思路 267
15.1.1.2. 文件审计策略设置 267
15.1.1.3. 文件信息溯源 269
15.1.1.4. 文件追踪 270
15.1.1.5. 文件审计运维基本思路 270
15.1.2. 行为审计 *270*
15.1.2.1. 行为审计运维基本思路 270
15.1.2.2. 行为审计策略设置 271
15.1.3. IM 软件库更新设置 *274*
15.1.3.1. 系统更新设置 274
15.1.3.2. 终端更新设置 274
15.2. 信创终端审计 275
15.2.1. 基本思路 *275*
15.2.2. 策略设置 *275*
15.2.3. 审计日志 *277*
16. 移动存储 277
16.1. 基本概念 277

16.1.1. 设备注册 277
16.1.2. 仅注册 278
16.1.3. 加密 U 盘 278
16.1.4. 设备分类 279
16.1.5. 安全 U 盘 280
16.1.6. 外出管理 281
16.1.7. 跨服务器兼容（U 盘漫游） 281
16.2. 基本功能 282
16.2.1. Windows 终端 282
16.2.1.1. U 盘注册 282
16.2.1.2. U 盘注册类型 283
16.2.1.3. 信创终端 291
16.2.1.4. U 盘使用管理 298
16.3. 移动存储申请审核 301
16.4. 移动存储全局设置 302
16.4.1. 移动存储服务器标识 ID 302
16.4.2. 跨服务器兼容设置 303
16.4.3. U 盘统一配置管理 303
16.4.4. 加密 U 盘个性化设置 305
16.5. 移动存储策略 305
16.5.1. 未注册 U 盘和未授权 U 盘的初始使用设置 305
16.5.2. 终端提示策略设置 305
16.5.3. 移动存储客户端策略设置 306
16.5.4. 安全 U 盘审计策略设置 306
16.5.5. 移动存储例外 307
16.5.6. 自动审核 308
16.6. 移动存储日志 308
16.6.1. U 盘插拔日志 308
16.6.2. 管理员注册日志 309
16.6.3. 安全 U 盘日志 309

16.6.4. 终端申请日志 310
16.7. 移动存储报表 310
16.7.1. 终端申请次数趋势图 310
16.7.2. U 盘类型占比统计 311
16.7.3. U 盘状态占比统计 311
16.7.4. 按分类统计各类型的注册 U 盘数量 311
16.7.5. 按终端统计各类型的注册 U 盘数量 312
16.8. 典型场景 312
16.8.1. 如何设置终端默认所有未授权 U 盘权限为禁用 312
16.8.1.1. 实现目的 312
16.8.1.2. 操作步骤 312
16.8.1.3. 提示消息设置 312
16.8.2. 注册 U 盘为加密分类盘及使用说明 313
16.8.2.1. 实现目的 313
16.8.2.2. 注册步骤 313
16.8.3. 安全 U 盘使用 316
16.8.3.1. 安全 U 盘登录 316
16.8.3.2. 文件导入以及导出 316
17. 安全空间 317
17.1. 基本概念 317
17.1.1. 安全空间 317
17.1.2. 个人空间 317
17.1.3. 安全空间授权 317
17.2. 安全空间管理 318
17.2.1. 业务说明 318
17.2.2. 空间定义基本元素 318
17.2.3. 空间添加/维护 319
17.3. 基本功能 319
17.3.1. 安全空间运维基本思路 319

17.3.2. Windows 终端安全空间策略设置 *319*
17.3.2.1. 添加空间 319
17.3.2.2. 离线管理 331
17.3.2.3. 安全盘初始 332
17.3.2.4. 个人空间配置 332
17.3.3. 信创终端安全空间策略设置 *333*
17.3.3.1. 添加空间 333
17.3.3.2. 个人空间配置 335
17.3.4. Windows 终端多网切换策略设置 *336*
18. 移动安全 336
18.1. 移动安全空间 336
18.1.1. 终端概况 *336*
18.1.1.1. 分组查询 336
18.1.1.2. 筛选 336
18.1.1.3. 自定义列 337
18.1.1.4. 导出 338
18.1.1.5. 查看终端详情 338
18.1.1.6. 终端操作 338
18.1.2. 安全空间策略 *339*
18.1.2.1. 新建终端策略 339
18.1.2.2. 查看策略详情 341
18.1.2.3. 策略执行情况查看 342
18.1.2.4. 策略维护 342
18.2. 移动终端管控 342
18.2.1. 定制终端策略 *343*
18.2.1.1. 新建终端策略 343
18.2.1.2. 查看终端策略 344
18.2.1.3. 终端定位查询 344
18.2.1.4. 终端远程控制 345

18.3. 移动应用商店 345
18.3.1.1. 编辑应用 346
18.3.2. Android 应用管理 346
18.3.2.1. 添加应用 346
18.3.2.2. 删除应用 347
18.3.2.3. 应用上架 347
18.3.2.4. 应用下架 348
18.3.2.5. 封装详情 348
18.3.2.6. 下载 348
18.3.3. IOS 应用管理 349
18.3.4. H5 应用管理 349
18.3.5. 应用统计 349
18.4. 移动应用防护 350
18.4.1. 应用防护概况 350
18.4.2. 应用防护策略 350
18.4.2.1 新建策略 350
18.4.2.2 维护策略 354
18.4.3. 应用防护审计 355
18.4.3.1. 应用使用审计 355
18.4.3.2. 应用加固审计 355
18.4.3.3. 运行环境审计 356
18.4.3.4. 敏感行为审计 356
18.4.3.5. 应用访问地址审计 356
18.4.3.6. 应用截屏审计 357
18.5. 移动威胁感知 357
18.5.1. 风险感知 357
18.5.1.1. 终端风险概况 358
18.5.1.2. 应用风险概况 361
18.5.2. 风险感知策略 361
18.5.3. 风险感知配置 363

18.5.4. 风险评估 *366*
18.5.4.1. 执行动作 366
18.5.4.2. 风险评估 366
18.5.4.3. 合规评估 367
18.5.4.4. 评估规则 368
18.5.5. 风险感知日志 *368*
18.5.5.1. 风险日志 368
18.5.5.2. 已拦截风险日志 369
18.5.5.3. 已处理风险日志 369
18.5.5.4. 专杀日志 370
18.6. 移动安全浏览器 370
18.7. 移动安全相机 371
18.8. 移动业务配置 372
18.8.1. 客户端部署 *372*
18.8.1.1. Android 客户端部署 372
18.8.1.2. IOS 客户端部署 374
18.8.2. Agent 管理 *374*
18.8.3. 终端管理配置 *374*
18.8.3.1. 终端管理配置项 375
18.8.3.2. NAC 准入配置 375
18.8.3.3. ICG 准入配置 376
18.8.3.4. 客户端界面配置 376
19. 安全小助手 **376**
19.1. 基本概念 376
19.2. 垃圾清理 376
19.2.1. 基本功能 *377*
19.2.1.1. 扫描本地垃圾 377
19.2.1.2. 清理本地垃圾 378
19.3. 垃圾清理库更新设置 382

19.3.1. 系统更新设置 *382*
19.3.2. 终端更新设置 *382*
19.4. 启动项管理 382
19.4.1. 基本功能 *382*
19.4.1.1. 检测系统启动项 382
19.4.1.2. 优化启动项 384
19.5. 启动项管理更新设置 387
19.5.1. 系统更新设置 *387*
19.5.2. 终端更新设置 *387*
20. 文件分发 388
20.1. 基本概念 388
20.1.1. 文件分类 *388*
20.1.2. 分发前置条件 *389*
20.1.3. 筛选 *389*
20.2. 文件分发策略 389
21. 弹窗防护 391
21.1. 基本概念 391
21.2. 基本功能 392
21.2.1. 策略配置 *392*
21.2.1.1. 拦截模式设置 392
21.2.1.2. 终端关闭软件拦截设置 393
21.2.1.3. 历史弹窗记录设置 393
21.2.2. 弹窗防护本地规则 *394*
21.2.2.1. 终端上报弹窗添加规则 394
21.2.2.2. 手动添加规则 394
21.2.2.3. 规则的发布 395
21.2.3. 弹窗防护日志 *396*
21.2.4. 弹窗防护云规则 *396*
21.2.5. 捕获弹窗 *397*

21.2.6. 历史弹窗记录 398
21.3. 弹窗规则库更新设置 400
21.3.1. 系统更新设置 400
21.3.2. 终端更新设置 400
21.4. 典型场景 400
21.4.1. 如何处理软件弹窗未拦截的情况 400
21.4.2. 如何更新弹窗防护规则库 401
21.4.3. 如何处理弹窗误拦截的情况 401
22. 系统设置 401
22.1. 通用设置 401
22.2. 安全设置 409
22.3. 日志清理 410
22.4. 数据外发 410
23. 强制合规 412
23.1. 基本概念 412
23.2. 基本功能 413
23.2.1. nac 联动 413
23.2.1.1. 网络水印打点 413
23.2.1.2. 网络水印例外 414
23.2.2. 准入认证客户端 414
23.2.2.1. 认证类型与方式 414
23.2.2.2. 准入认证配置 415
23.2.2.3. 执行动作配置 416
23.2.2.4. 无线认证选项 417
23.2.2.5. 显示选项 418
23.2.2.6. 高级配置 419
23.2.2.7. 其他配置 419
23.2.3. 安检合规 420
23.2.3.1. 检查设置 420

23.2.3.2. 系统配置安全 421
23.2.3.3. 系统状态安全 422
23.2.3.4. 系统运行安全 423
23.2.4. 准入概况与设备合规 424
23.2.5. 天擎与准入同台 425
24. 多级级联 427
24.1. 基本概念 427
24.1.1. 级联部署 427
24.1.2. 级联策略 427
24.1.3. 级联报表 427
24.1.4. 级联更新管理 427
24.2. 基本功能 428
24.2.1. 级联关系 428
24.2.2. 级联策略 430
24.2.3. 级联报表 431
24.2.4. 级联更新管理 432
24.2.5. 登录下级管理中心 433
25. 更新管理 435
25.1. 基本概念 435
25.1.1. 版本号 435
25.1.2. 在线更新 437
25.1.3. 离线更新 437
25.1.4. P2P 437
25.1.5. 版本更新 437
25.1.6. 自动更新 438
25.1.7. 手动更新 438
25.1.8. 定时更新 438
25.1.9. 覆盖安装 438
25.2. 管理系统更新 439

25.2.1. 在线更新 439
25.2.2. 离线工具更新 441
25.2.3. 覆盖安装更新 442
25.3. 终端更新 443
25.3.1. 终端更新配置 443
25.3.2. 在线更新 447
25.3.3. 离线更新 449
25.4. 典型场景 450
25.4.1. 隔离网部署的管理中心如何更新 450
25.4.2. 孤岛终端如何更新 450
25.4.3. 如何降低更新带来的风险 450
25.4.4. 如何减小更新时占用带宽对业务的影响 451
25.4.5. 如何在更新管理中心后暂不更新终端 451
25.4.6. 终端灰度发布实践案例 451
26. 告警中心 455
27. 报表中心 457
27.1. 视图 457
27.2. 仪表板 459
27.3. 周期报告 461
28. 用户中心 463
28.1. 用户 463
28.2. 用户分组 463
28.3. 组织架构 464
28.4. 权限 465
28.5. 应用 467
28.6. 用户设置 467
28.7. 审批工作流 471
28.7.1. 工作流管理 471

28.7.1.1. 审批角色 472
28.7.1.2. 新建工作流 472
28.7.2. 个人中心 474
28.7.2.1. 当前用户的申请信息 474
28.7.2.2. 当前用户的审批信息 474
28.7.2.3. 自动审批 475
28.8. 个人中心 475
29. 运维管理 475
30. 系统日志 480
30.1. 系统运行日志 480
30.1.1. 系统更新日志 480
30.2. 系统运行日志 481
30.3. 管理员日志 481
31. 许可证管理 482
31.1. 许可证概况 482
31.2. 许可证使用情况 483
31.3. 许可证帮助文档 483
31.4. 更新许可证注意事项 484

1. 奇安信天擎简介

1.1. 产品简介

奇安信天擎终端安全管理系统 V10.0（以下简称“奇安信天擎或者管理系统”）是一款面向政企客户网络环境的平台化终端安全产品，基于奇安信全新的“川陀”终端安全平台构建，集成高性能病毒查杀、漏洞防护、主动防御引擎，深度融合威胁情报、大数据分析和安全可视化等创新技术，通过防病毒、补丁管理、运维管控、基线合规检查、网络准入、终端审计、数据防泄漏、终端检测与响应（EDR）等安全功能，为政企单位业务终端提供体系化安全防护能力，并助力客户持续开展基于数字化指标的安全运营。

1.2. 产品主要功能

- **有效查杀已知/未知病毒**

结合云查杀引擎、脚本查杀引擎、启发式查杀引擎、人工智能查杀引擎、系统修复引擎、主动防御技术，有效查杀已知和未知病毒；通过联动天眼产品有效抵御 APT 攻击。

- **智能化的补丁管理**

可对全网终端进行漏洞扫描并与漏洞类型进行多维关联按需修复，补丁分发流控机制有效提升企业信息系统整体漏洞防护等级。

- **可靠的安全运维管控**

能有效的对终端进行网络管控、非法外联控制、外设使用控制、基线核查等，提升终端安全运维效率和安全性。

- **灵活的移动存储管控**

给予不同的移动存储介质相应的授权试用范围和读写权限，同时支持设备状态的追踪与管理，实现对移动存储设备的灵活管控，保证终端与移动存储介质进行数据交换和共享过程中的信息安全要求。

- **多场景的安全水印**

由打印水印、屏幕水印、截屏水印组成的安全水印，覆盖打印、拍照、截屏等场景，进行安全水印的输出和信息溯源，对通过打印、拍照、截屏等方式造成的数据泄漏进行有效预防和追溯。

◆ **完善的安全审计**

通过终端/用户、分组、时间、文档类型等多视角、多维度、多层次对终端文件的操作行为、流转行为、打印行为、光盘刻录行为、网站访问行为、邮件外发行为和 IM 聊天行为进行审计。并支持对特定文件类型添加水印，实现文件溯源以及完整流转场景的还原。

◆ **精确的弹窗防护**

通过专业团队持续精准化运营，结合自主规则，精确拦截第三方软件广告等弹窗，用户在授课、会议时无需担心被弹窗干扰。

◆ **全方位终端数据泄露防护**

覆盖终端设备、终端应用、终端网络等多个数据泄漏途径，对个人敏感信息、商业敏感信息等数据泄漏进行识别和防护，并通过对泄漏片段的快速溯源来定位泄漏事件，为企事业单位的数据资产保驾护航。

◆ **高级威胁检测与响应**

通过对终端操作系统、应用及用户的行为全面持续地详细记录和分析，可以持续洞察终端的安全活动信息，结合大数据威胁情报和终端异常行为等线索对内网沦陷终端进行快速检索、定位和告警，并提供针对威胁事件自动化响应、调查、溯源和修复的能力，在对抗高级威胁中获得更好的效果与更快的效率，最大限度压缩攻击者的攻击时间，减少高级威胁最终达到目的可能性。

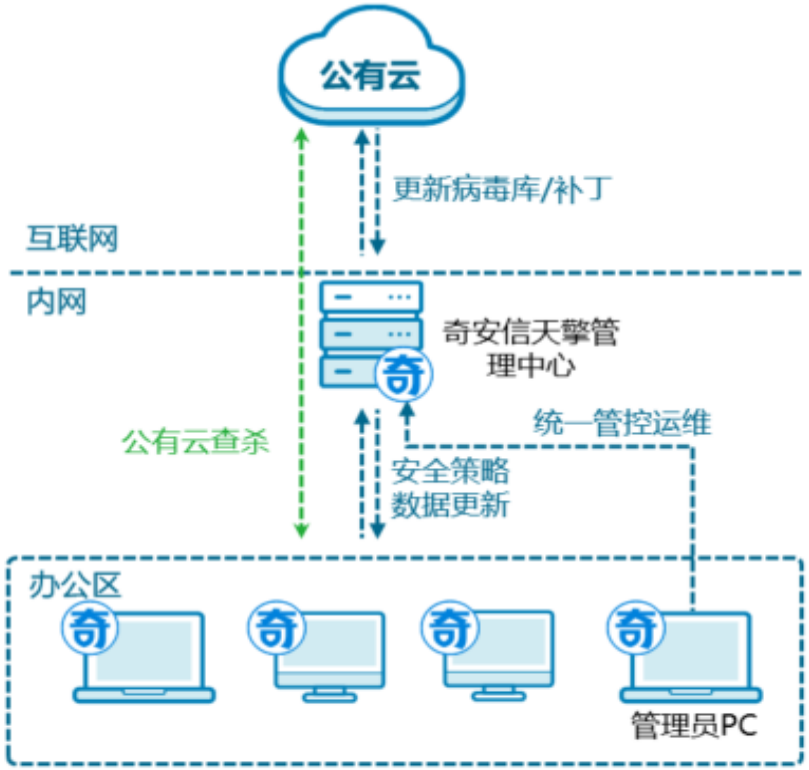
1.3. 典型部署场景

1.3.1. 互联网络部署方案

◆ **方案特点**

本方案适用于能够连接互联网环境的客户，客户网络中部署管理系统，办公终端安装奇安信天擎客户端，通过管理中心对办公终端做统一的安全防护和管理。

◆ **部署示意图**



互联网环境部署

在网络内部署奇安信天擎，通过在线安装或者离线安装包的方式安装奇安信天擎客户端。管理中心通过互联网连接到云端的升级服务器进行升级、更新，然后客户端通过管理中心统一进行升级、更新及策略下发，可以极大地节省企业总出口带宽。

客户端会根据管理中心下发的安全策略，进行体检、杀毒和漏洞修复等安全操作。可以设定终端是从管理中心更新病毒、补丁库，还是从互联网更新。

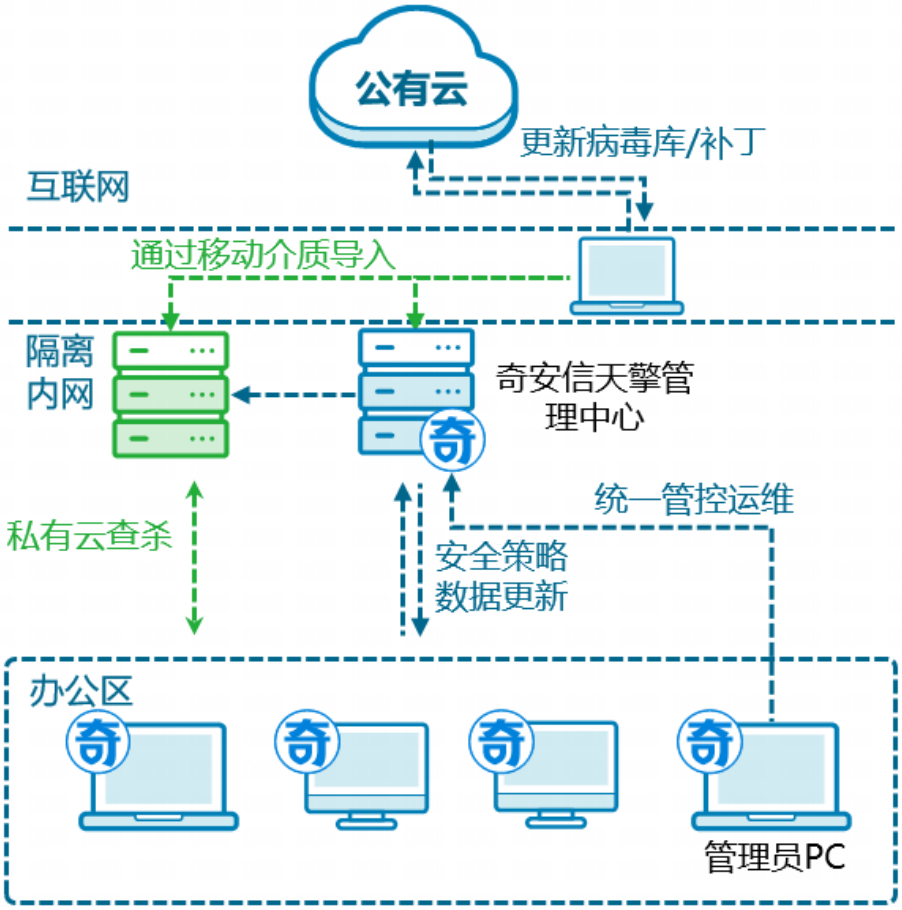
终端可连接云端进行云查杀，极大地提高终端病毒的查杀能力。

1.3.2. 隔离网络部署方案

- **方案特点**

该方案适用于无法连接互联网环境的客户，网络中部署一套管理系统，网内中的终端安装奇安信天擎客户端，通过管理中心进行统一的安全防护和管理，管理中心的病毒、补丁等更新程序通过离线升级工具进行更新。

- **部署示意图**



隔离网环境部署

在客户网络中部署管理系统，通过在线安装或者离线安装包的方式安装终端客户端，客户端会根据管理中心下发的安全策略，进行体检、杀毒和漏洞修复等安全操作。

部署私有云安全鉴定中心，保证能和管理中心网络连通即可。提高内网的病毒查杀能力，帮助客户快速、精准定位和查杀威胁较高的恶意样本。

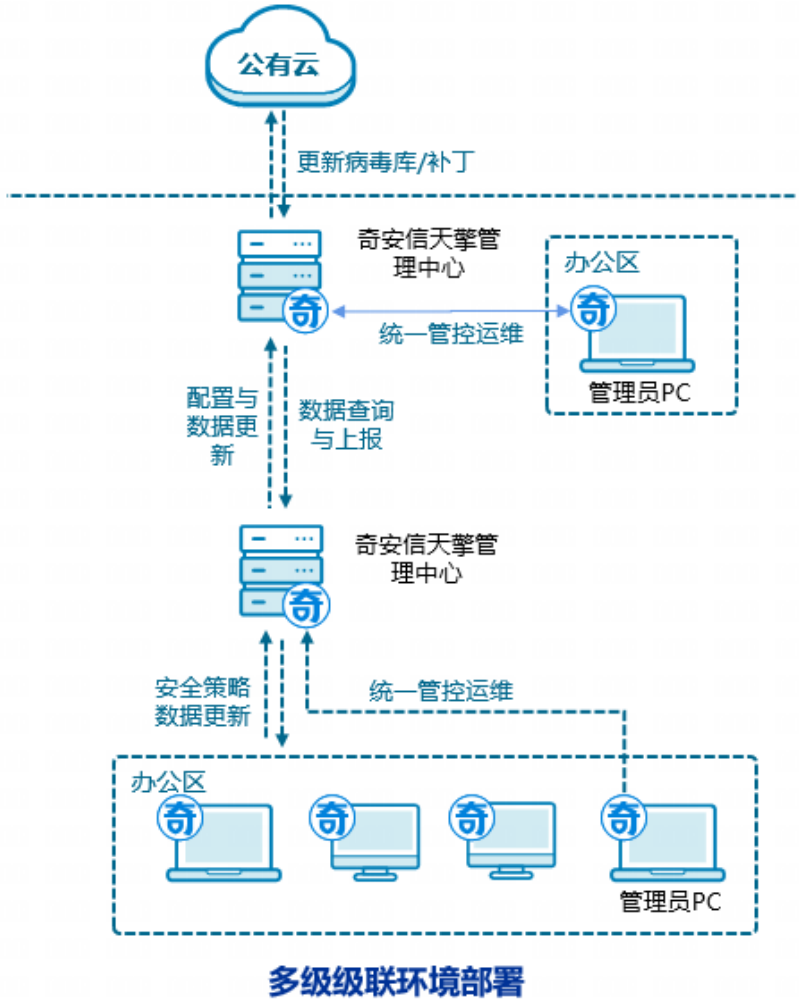
在有互联网的环境中使用隔离网更新工具，定期从云端相关服务器下载病毒、木马库、补丁库；然后使用移动存储介质更新到内网的管理中心，用户的终端连接到内网管理中心进行自动升级和漏洞修复。

1.3.3. 多级级联部署方案

- **方案特点**

该方案适用于多级管理的客户，总部网络中部署一套管理系统，网内中的终端安装奇安信天擎客户端，系统所处环境可参照 1.3.1 或 1.3.2 进行；通过管理中心进行统一的安全防护和管理，管理中心的病毒、补丁等更新程序通过互联网或者离线升级工具进行更新。

◆ 部署示意图



总部和二级分布在各网络中部署管理系统，通过在线安装或者离线安装包的方式安装终端客户端，总部的安全配置、策略管理以及相关库版本更新等参考1.3.1或1.3.2的介绍。

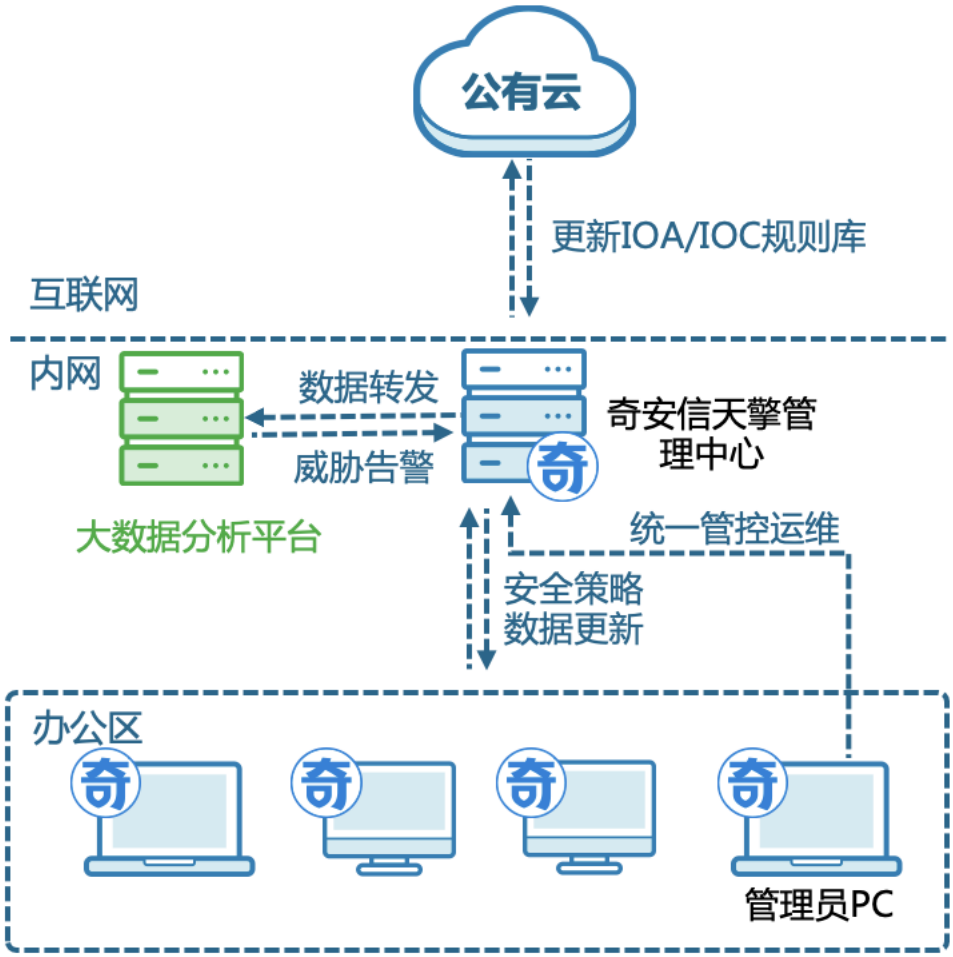
对于二级管理系统，在部署客户端后可以申请挂接到总部管理系统，总部审批通过后可以为其二级系统配置更新源、下载源以及灰度更新策略；总部管理系统可以实时查询下级终端状态数据，以及查看二级管理系统定时上报的日志数据。

1.3.4. 高级版EDR部署方案

◆ 方案特点

本方案适用于部署高级版EDR的客户，通过部署终端大数据分析平台对客户端采集的大量终端行为数据进行存储、计算、检索、分析、溯源等操作，进而快速发现高级威胁。

◆ 部署示意图



高级版EDR部署

客户端根据管理中心下发的安全策略对终端行为数据进行采集，上报管理中心并转发至大数据分析平台进行数据关联分析、威胁溯源、威胁告警等。

1.4. 典型部署形态

1.4.1. 单机部署

单机部署是指在单台服务器上完成奇安信天擎的部署，运维简单，一般不需要专业的 IT 运维工程师，适用于挂载终端数量较小，管理场景简单的客户。

1.4.2. 集群部署

集群部署是指在多台服务器上完成奇安信天擎的部署，为了保证服务的高可用，将服务在各服务器上均运行一份实例。这种部署方式承载能力强，但是需要更多的资源，运营维护相对复杂，适用于挂载终端数量较多，管理场景相对复杂的客户；目前集群部署支持 Linux 系统，不支持 Windows 系统。

集群部署的高可用性是指当集群中的一台服务器因故障宕机时，服务系统仍然能够提供正常的业务服务，要实现集群的高可用性也受到以下条件的约束：

1） 集群机器的数量需要满足高可用要求，每种类型的服务集群需要提供至少 3 台服务器；例如在标准部署方案中，6 台和 9 台的部署模式具备高可用性，4 台的部署模式因为应用服务集群只能分配 1 台服务器，所以并不具备高可用性；

2） 要保证各服务器之间资源的独立性，不应存在某种资源出错导致多台服务器同时出错的情况，如出现这种场景则无法保障高可用性；也可以说，故障节点是以直接安装部署天擎的服务器操作系统为计算单位的。常见的非独立场景如多台服务器共用同一存储设备，存储设备出错会导致多台服务器同时故障；或多台服务器是部署在同一物理服务器上的虚拟服务器，物理服务器出错导致多台虚拟服务器同时出错；

3） 集群高可用性需要外部负载方案进行支持；集群对外服务都由应用服务集群提供，例如应用服务集群由 3 台服务器组成，外部访问者请求到 3 台服务器中的哪一台应该是由外部负载方案决定的，如果外部策略是所有访问都指定到其中一台服务器，那么这台服务器宕机就会造成系统不可用从而不具备高可用性；负载方案应能够实现当某台应用服务器宕机时请求不再分配到这个服务器上；常见的负载方案包括 F5 设备、LVS、DNS、浮动 IP 等，具体方案需要根据客户的实际情况进行选择；

4） 集群应保留一定的负载能力，当少量服务器宕机时，其他服务器能够承担相同的负载压力；反之如果没有冗余负载能力，当出现服务器宕机时，其他服务器也会因为压力服务出错，严重的会因雪崩效应导致整个服务系统崩溃；

5） 每个类型的集群容许不大于三分之一的服务器宕机，但并不是指整个集群容许三分之一的服务器宕机；如 9 台标准部署中，应用集群、大数据集群、数据库集群分别有 3 台服务器，各类型容许 1 台宕机，整个系统容许最多 3 台同时宕机，但并不是任意 3 台宕机都能保证集群可用；6 台标准部署中存在集群复用，就要考虑最多 2 台宕机不能出现在同一类型的集群中；

6） 高可用性并不等于服务器宕机过程中服务系统对外部应用无感知，而是指系统能够快速的自动恢复，恢复时间还依赖于负载策略等；原因如宕机瞬间已经分配到这个服务器上的请求一定会失败，宕机前后负载策略通过何种方式能在多长时间内切换请求等；减少影响的方法可以是外部应用增加重试机制，这个不在系统部署范畴内描述或实现。

集群高可用性的另一种场景是当更多服务器宕机甚至服务器所在机房整体故障的情况下，要求整个系统的可用性。这种场景需要采用双机房备份、两地三中心等部署机制解决，目前面向此类场景的部署方案需要专业的 IT 运维工程师进行设计和实施，未在天擎标准化部署方案中，如有此类场景需求，请先联系业务线的相关同事。当前可以明确的是双机房、两地三中心等方案，都需要客户提供达到要求的网络基础设施；支持冷备方案尚不具备双机房双活的解决方案；具体要求和实施标准均以实际沟通为准。

2. 基础功能

2.1 基本概念

2.1.1. 策略

策略是配置项的集合，用于将企业的安全管理制度转换为终端可执行的指令。根据安全业务特性，由 N 个配置项组成。分为终端策略和用户策略。

2.1.2. 任务

任务是管理员要做的一件事，比如给全网终端做一次病毒扫描、定期让全网终端执行一个运维脚本。

2.1.3. 日志

日志分为两大类，一类是记录在终端发生的事件，一类是记录服务端运行的关键事件或管理员操作。

2.1.4. 管理员

拥有管理权限的用户则是管理员。

2.1.5. 强制策略

策略类型分为普通策略和强制策略。上级分组的强制策略的优先级高于下级分组上的策略，用于统一和强制生效策略。

2.1.6. 用户策略

用户策略指按照终端上登录的用户分发的策略。用于按照终端的使用人来配置策略。

2.1.7. 自动分组

支持手动划分终端的分组和自动分组。

普通分组支持按照接入点、IP 地址、终端名、工作组自动划分终端分组。

自定义组支持按照接入点、IP 地址、终端名、工作组、操作系统、内存大小自动划分终端分组。

2.1.8.NAT 地址

NAT 地址：指服务器视角看见的终端 IP 地址。如果终端与服务器之间有网络设备做了地址转换，则 NAT 地址不同于终端的 IP 地址。

IP 地址：与服务器通信的网卡的 IP 地址。

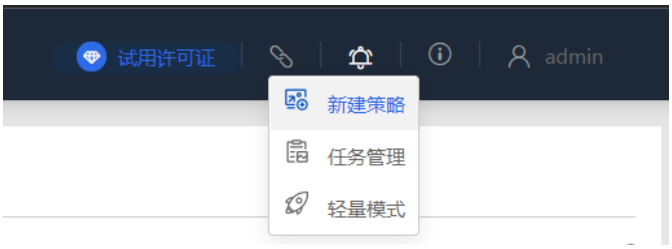
2.2. 轻量模式

针对低配置终端的专用模式，可降低资源占用并兼容系统安全，轻量模式下仅保留"病毒防护、补丁管理、外设管理、远程协助"等基础安全功能，其他功能将从终端上卸载。

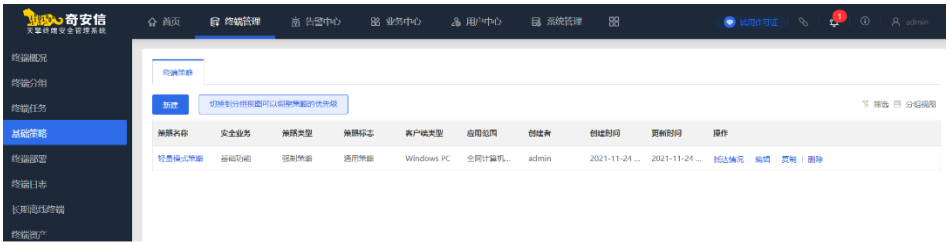
功能入口 1：管理中心-快捷功能-轻量模式。

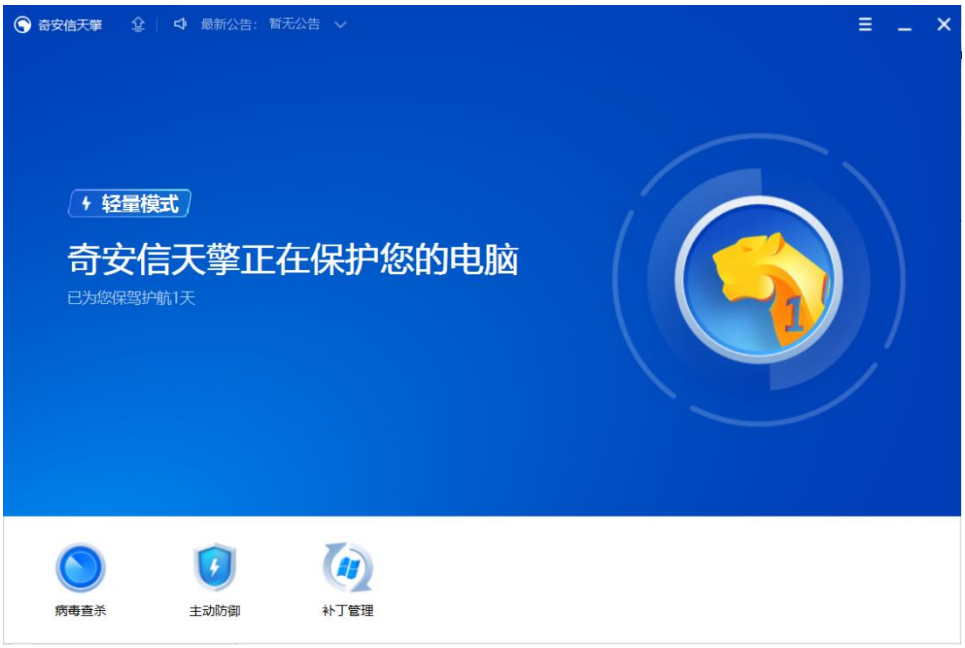
功能入口 2：管理中心-终端管理-基础策略。

快捷开启轻量模式，一键创建轻量模式的终端策略。



开启轻量模式
·开启轻量模式将会大幅降低终端的资源占用，提升终端的使用流畅性。
·为降低资源占用并兼容系统安全，轻量模式下仅保留“病毒防护、补丁管理、外设管理、远程协助”等基础安全功能，其他功能将从终端上卸载。
开启轻量模式
取 消




奇安信天擎
最新公告：暂无公告
轻量模式
奇安信天擎正在保护您的电脑
已为您保驾护航1天
病毒查杀
主动防御
补丁管理

【注意】启用该功能后，会卸载除病毒防护、补丁管理、外设管理、远程协助以外的所有模块。该功能配置前请检查相关策略的涉及终端的模块使用情况，如果有非上述模块的请确认卸载模块对终端无影响后再进行设置。

2.3. 第三方联动

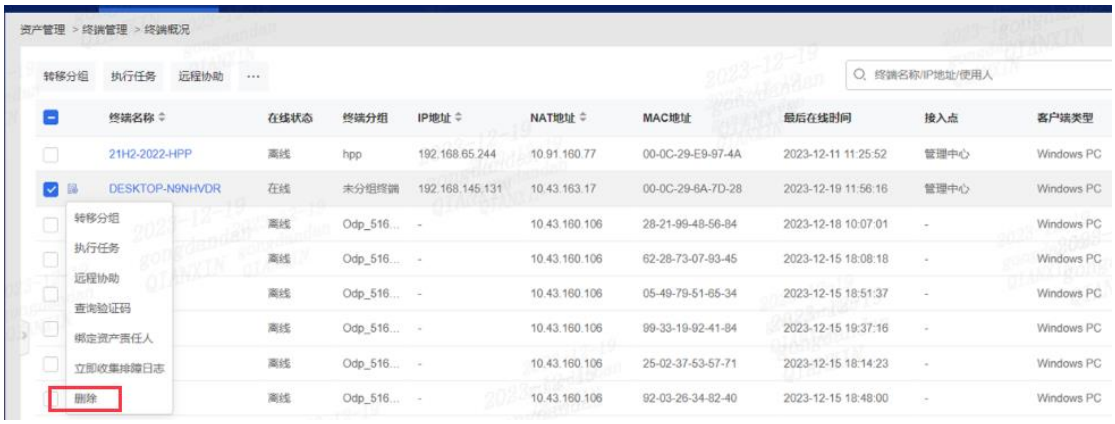
操作入口：系统管理>用户中心>应用。

功能说明：目前天擎提供了数据开放平台（ODP）、数据外发（Syslog）、联动处置平台(OpenC2)以及智慧防火墙联动工具;已支持的系统有智慧防火墙、天眼、NGSOC，在进行联动配置时需先为第三方系统创建应用 Key 和应用密钥，操作入口如上,具体配置操作及联动开发参考文档中心《第三方系统联动对接》。

2.4. 典型场景

2.4.1. 如何手动删除已卸载的终端

奇安信天擎终端在卸载的时候，会自动向管理中心发一条卸载日志，这样管理中心就可以不再显示该终端的信息。但有一些特殊的场景，例如终端卸载时已经断网，或者直接重装系统，都会导致卸载日志无法发送到奇安信天擎，这时候管理中心看到的是一台长期离线的终端。如果需要腾出这种异常卸载的终端占用的许可点数，或者其他管理原因，需要手动删除，可以在 终端管理>终端概况 里手动删除。



2.4.2. 如何进行终端资产管理

管理员可以通过终端概况查看资产信息。

为了减少管理员的资产登记工作量，可以选择让终端用户自助进行资产登记。先设置需要终端用户自助登记的资产项（参考 22.1 通用设置章节中的资产登记部分），然后导航到“资产管理>终端管理>基础策略>基础设置”里设置强制弹窗让终端用户进行登录。

2.4.3. 如何与 LDAP 服务器进行联动

希望实现与 LDAP 服务器联动，按照实名使用人进行管理，即可按照使用人分发策略、查找日志等操作管理终端。

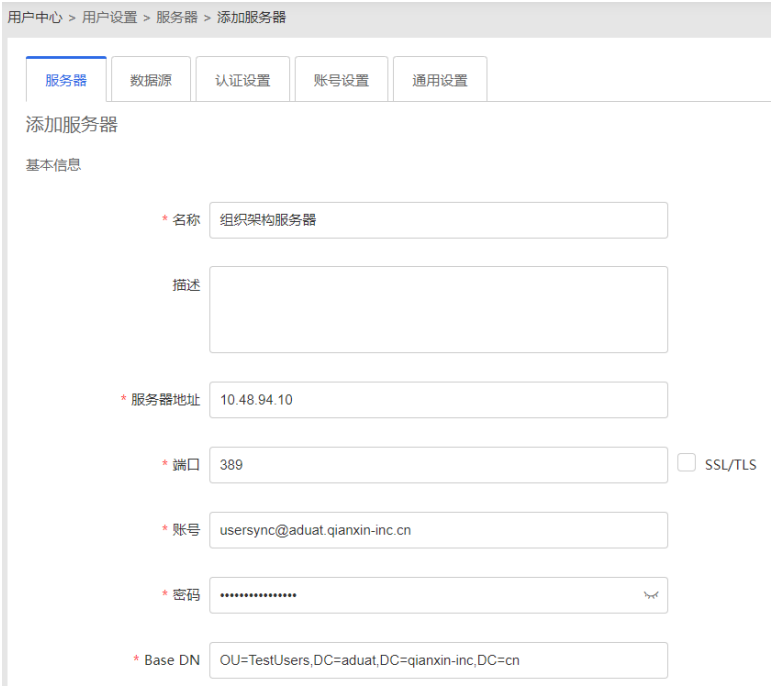
1） 配置 LDAP 服务器和认证源。

a） 配置“LDAP 服务器”。

i. 支持 OpenLDAP 类型，为了保证填写的各项内容的正确性，可借助 OpenLDAP 可视化工具 LdapAdmin 进行辅助，请访问其官网下载。

ii. 导航到“系统管理>用户中心>用户设置”，添加“服务器”，依次填写“基本信息、分组设置、用户设置”。

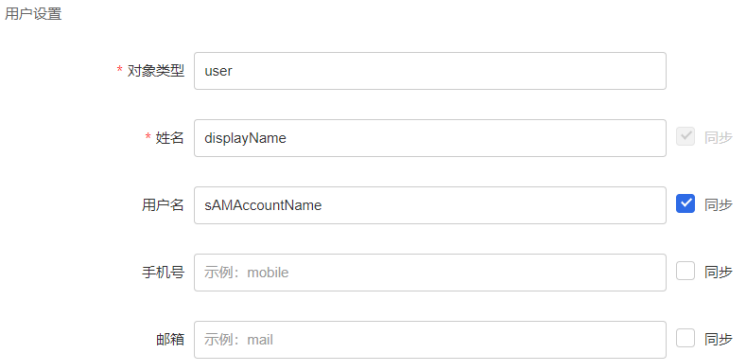
基本信息：



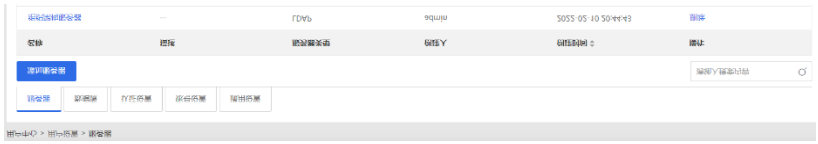
分组设置：

用户设置：

通常同步用户姓名和用户名，按照实际需要配置。



完成服务器添加



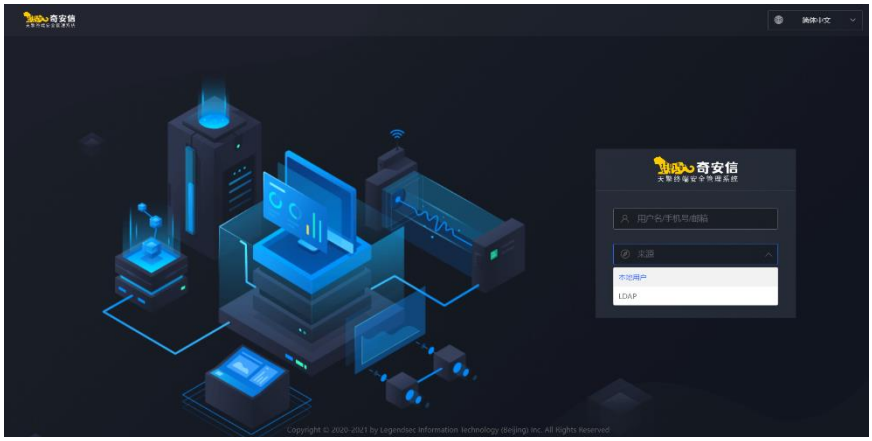
b) 添加数据源，同步组织架构。

添加一个数据源，并设定同步到组织架构中的位置和自动同步的时间。

c） 配置认证因子。

i. 导航到“系统管理>用户中心>用户设置>认证设置>基础认证因子”，添加因子。

ii. 一级因子中增加刚添加的因子，完成添加后管理中心可以使用该 LDAP 的用户登录管理中心（如果是管理员，需要再配置管理员权限）。



2) 开启用户登录（实名认证）。

a) 导航到基础策略，开启“用户登录”。

b) 终端用户登录

终端用户登录后，则可以执行用户策略，在主面板也查看登录的使用人。

3) 配置分发用户策略。

4) 查看日志

如果终端产生日志，管理员可以查看到终端的使用人，方便快捷定位到人。

重要提示：

1) 配置好服务器、数据源，且同步完数据后，请务必按照文档添加因子，否则无法使用登录功能。

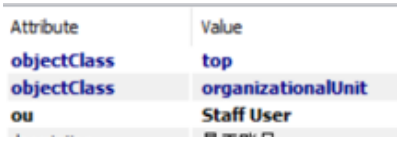
2) 同步数据可能因为应用程序所在的服务器受 ACL 限制，访问不到 LDAP 服务器而失败。可通过下图中【测试连接】按钮进行测试，请保证测试连接通过。

3) 请一定确保在页面填写的各个配置与 LDAP 的属性保持一致，因为大部分同步失败都是因为填写配置错误导致。

LDAP 字段辅助说明：

【用户设置】中除对象类型使用“Value”字段的值（属性的值），其余均使用“Attribute”字段的值（属性名称），根据实际 LDAP 中拥有的内容填写，用户名、手机号、邮箱三项中必须填写一项，否则用户登录时报错【用户不存在】。

名称栏	示例	填写说明
Base DN	OU=TestUsers,DC=aduat,DC=qianxin-inc,DC=cn	LDAP 目录的根，建议使用 LDAPAdmin 工具查看或者登录域控查看。
SSL/TLS		根据 LDAP 实际情况决定是否使用 SSL/TLS，通常可不勾选。
分组名称	ou	注意**小写**，标准 OpenLDAP 中 **ou** 表示分组名称，可直接填写 ou，或根据 LDAPAdmin 工具中展示的“Attribute name”字段的值填写。
分组 ID	DN	注意**大写**，标准 OpenLDAP 中 **DN** 表示分组唯一标识，可直接填写 DN。
父分组 ID	DN	注意**大写**，标准 OpenLDAP 中 **DN** 表示分组唯一标识，可直接填写 DN。

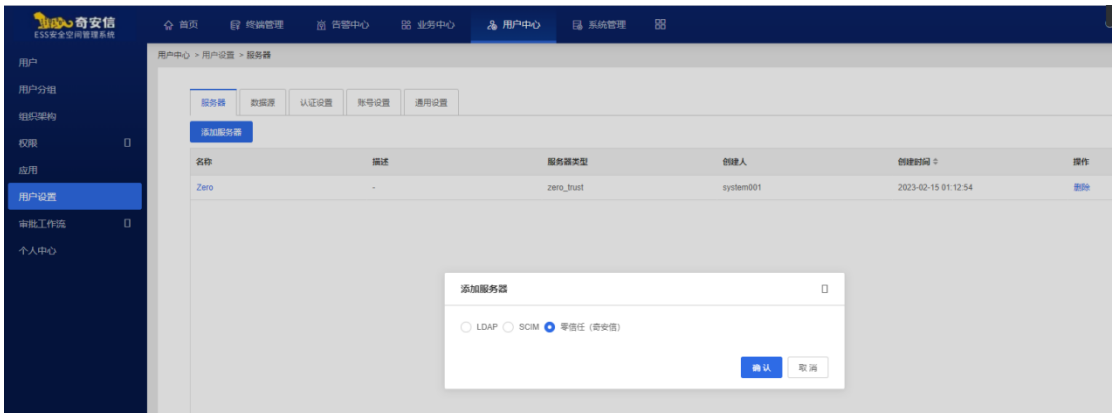
分组路径	OU=TestUsers,DC=aduat,DC=qianxin-inc,DC=cn	**同步整个组织架构**，填写 Base DN 的内容。 **同步某个分组**，填写具体的路径。例如同步“TestUsers”这个分组下的用户，则填写 OU=TestUsers,DC=aduat,DC=qianxin-inc,DC=cn 。
对象类型【分组设置】	organizationalUnit	分组的类型。如果【objectClass】有多个值，请按照实际需要选择。 
对象类型【用户设置】	User	用户的类型。如果【objectClass】有多个值，请按照实际需要选择。
姓名	displayName	一般可直接填写 displayName，或者根据 LdapAdmin 工具选择实际的姓名字段。
用户名	sAMAccountName	一般可直接填写 sAMAccountName，或者根据 LdapAdmin 工具选择实际的姓名字段。
邮箱	mail	一般可直接填写 mail，或者根据 LdapAdmin 工具选择实际的姓名字段。

2.4.4. 奇安信零信任与天擎一体化管理

希望实现与奇安信零信任产品联动实现一体化管理终端，即在终端用户上实现一个“客户端”，提升终端用户的操作体验。可实现自动安装零信任客户端，用户登录与零信任客户端登录实现单点登录。

2.4.4.1. 零信任数据源配置

1) 导航进入“系统管理>用户中心>用户设置>服务器”，点击[添加服务器]，选择“零信任（奇安信）”。



2) 添加服务器信息，请参考如下表格所示。

配置项	配置子项	值
基本信息	api 地址	https://TAC 地址:8443/manage
	client_id	483975
	client_secret	82ewdd8jhsg23500
	获取组织架构地址	/api/scim/v2/bizdata/record/.search
	获取用户地址	/api/scim/v2/bizdata/record/.search
分组设置	分组名称	name
	分组 ID	id
	父分组 ID	parentId
	组织成员	organizations.#.value
用户设置	用户 ID	id
	姓名	displayName
	用户名	userName
	邮箱	emails;value

3) 导航进入“系统管理>用户中心>用户设置”配置“数据源”，点击[添加数据源]，输入名称，选择服务器（为上一步骤添加的零信任服务器），同步分支，选择同步到天擎的目标位置，设置自动同步时间设置。根据配置的同步频率将选择的服务器的数据同步到配置的天擎目标分支。

【注意】如果想要用零信任数据源联动登录，需要修改单点认证的数据源和终端策略中的用户登录数据源。

2.4.4.2. 客户端单点登录配置

1) 导航进入“系统管理>用户中心>用户设置”配置“数据源”，从“奇安信零信任”等第三方系统同步组织架构和用户，或者自建用户。

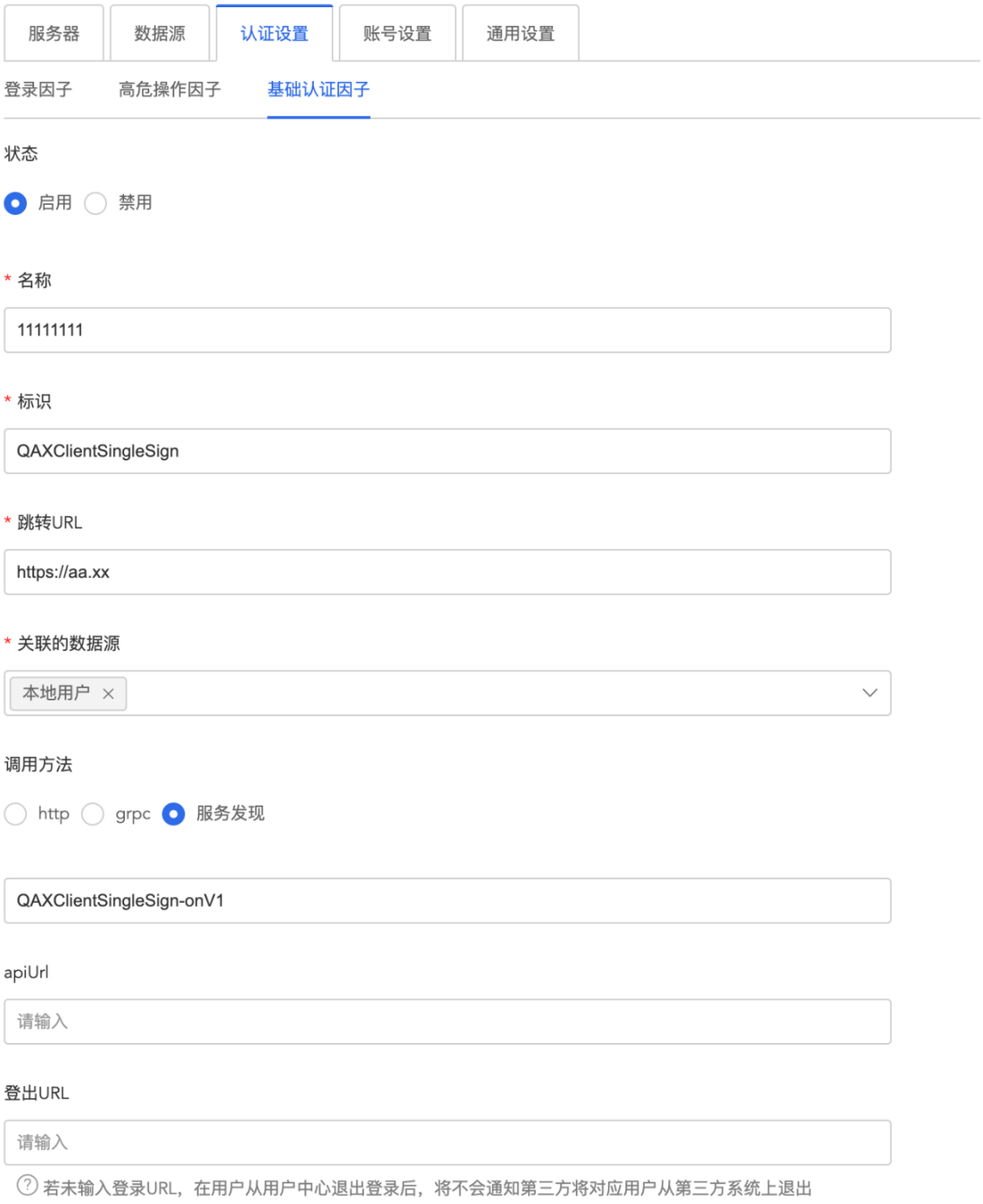
2) 导航进入“管理中心>用户中心>用户设置>认证设置>基础认证因子”添加一个“单点因子”。

   a) 配置名称。

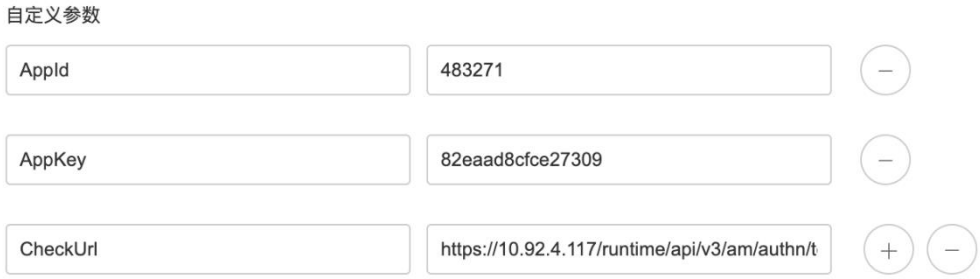
   b) 配置“标识”为“QAXClientSingleSign” （标志不能修改）。

   c) 配置“服务发现”中服务名为“QAXClientSingleSign-onV1” （服务名不能修改）。

   d) 跳转 URL 必填可填写“https://aa.xx”



e) 在“自定义参数”中配置AppId、AppKey，和CheckUrl。AppId和AppKey在零信任系统中生成。CheckUrl是零信任的验证接口地址(https://{零信任接口ip}/runtime/api/v3/am/authn/token/verify)。



f) 关联数据源为第一步配置的零信任数据源。

3) 配置一条基础策略，开启第三方联动安装零信任客户端，并勾选“联动安装零信任客户端”选项和零信任客户端下载地址；此处填写的地址需保证分发的终端均可访问。

4) 在基础策略中开启单点登录。如果是从第三方系统同步用户则配置为这个“数据源”，自建用户则配置为“本地用户”。

2.4.5. 第三方产品联动

导航进入“资产管理>终端管理>基础策略>第三方联动”，配置项“第三方产品联动”勾选“开启切换接入点联动”，由第三方产品指定客户端连接的接入点，勾选该选项，请不要开启自动切换接入点和自动切换服务器的功能，否则会导致本功能失效。

支持策略分发联动，客户端会接收和执行第三方系统分发的策略，不执行本系统分发的策略。需要第三方系统遵照联动开发规范进行适配。

2.4.6. IPv6 场景

适用于 IPv4 网络与 IPv6 网络共存的环境，一套同时对 IPv4 和 IPv6 网络的终端做安全管理。安全管理上操作与 IPv4 单栈网络是一样的，只是在部署有差异。

1) 部署管理系统，部署时仍需部署在 IPv4 的网络，并作为管理中心 web 的地址入口，再发布一个 IPv6 的地址用于管理 IPv6 网络里的终端（在“系统设置”中配置“终端通信地址”）。管理系统的部署参考《奇安信天擎终端安全管理系统 V10.0R5-单机安装部署手册》。

2) 在基础策略中配置终端处于双栈网络时使用 IP 协议版本的策略。

3. 终端管理

3.1. 终端概况

在首页可概览终端资产概况，跳转到“终端概况”详细页面，也可通过菜单栏：资产管理>终端管理>终端概况，终端概况页面可查看终端详情和对终端进行安全管理。

支持显示 macOS 终端的概况信息

3.1.1. 终端详情

功能入口：资产管理>终端管理>终端概况，点击计算机名称，可以查看此终端的详情。

终端详情包括：

- 概览。查看终端的基本信息（终端名称、型号、在线状态、登录域、开关机时间、分组信息、模块安装信息）配置信息及资产信息。
- 策略。查看终端当前的策略配置信息。
- 硬件信息。查看终端的各种硬件配置（CPU、主板、内存、硬盘、显卡、显示器、网卡、电脑品牌、设备出厂日期、硬盘序列号和硬件变化信息等）。
- 操作系统。包括查看系统信息、账号信息。
- 进程信息。查看终端当前的进程信息，可以结束进程。
- 准入状态。查看安检详情。
- 基线核查得分详情。
- 网络信息。查看和配置网络。
- 病毒防护信息。

3.1.2. 终端安全管理

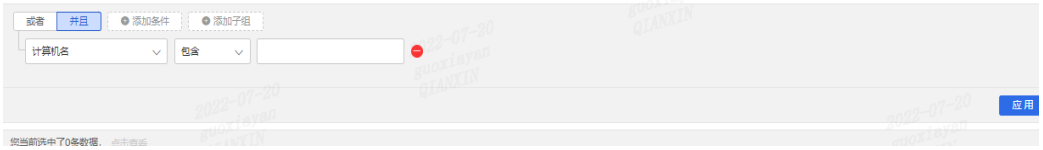
- 功能入口：资产管理>终端管理>终端概况，可对终端转移分组、配置单终端任务、查询退出和卸载客户端的验证码、绑定资产责任人、收集客户端排障日志操作、发起远程协助、删除终端等操作。

注：macOS 终端，不支持收集排障日志。

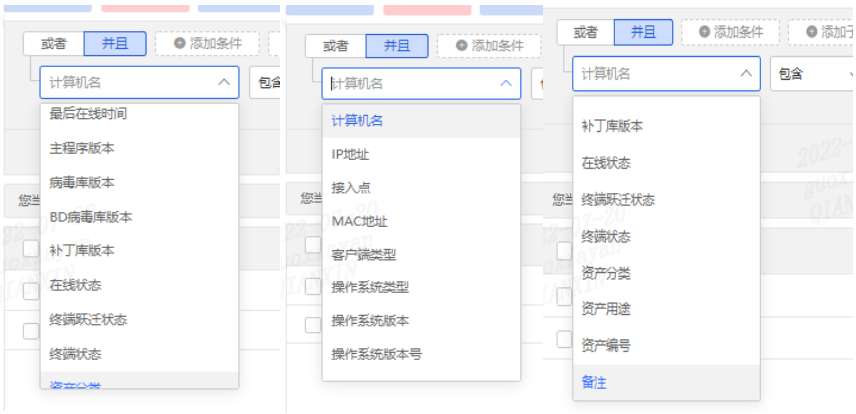
- 高级筛选功能

功能说明：点击高级筛选后，进行筛选关系和筛选条件的选择。

筛选关系有或者、并且两种。



筛选条件有以下多种



选择后，点击应用可进行相应条件的筛选。

3.2. 终端分组

终端分组用于分类管理终端，即批量对终端配置策略、分发任务、查看报表等操作。

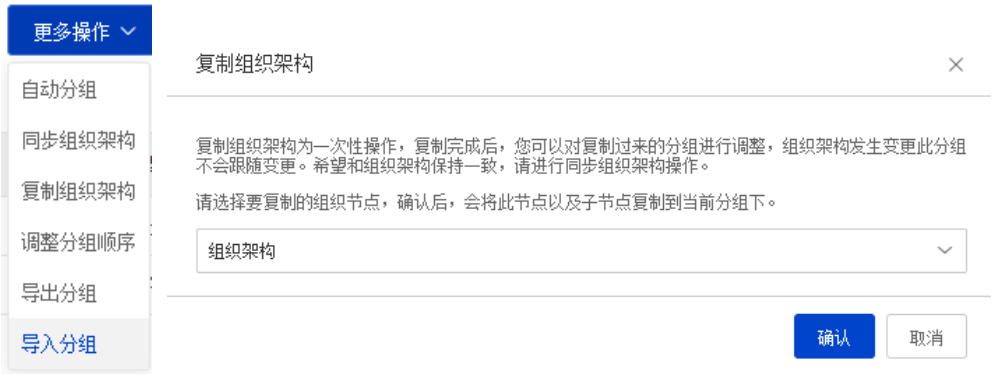
普通分组：普通分组定义管理员管理终端的范围，一台终端只能属于一个普通分组。

自定义组：自定义组可以理解为自定义筛选条件，管理员可通过设置分组规则将终端划分到自定义组中，而不改变所在的普通分组。一台终端可以属于多个自定义组，而不会有分组冲突。

点击选择任意分组，可以编辑分组信息和自动分组规则。

可以手动对终端所在的分组进行维护，也可以选择采用自动分组策略。自动分组是根据终端的一些属性如 IP 地址、终端名、计算机工作组进行自动分组，需要管理员在添加分组或编辑分组时设置自动分组规则。如果没有设置自动分组规则，或者终端的属性不属于任何自动分组的规则，则终端会被划分到根分组“全网计算机”。

点击更多操作，可以为选择的分组同步组织架构、复制组织架构以及自动分组、调整分组顺序、导入导出分组。

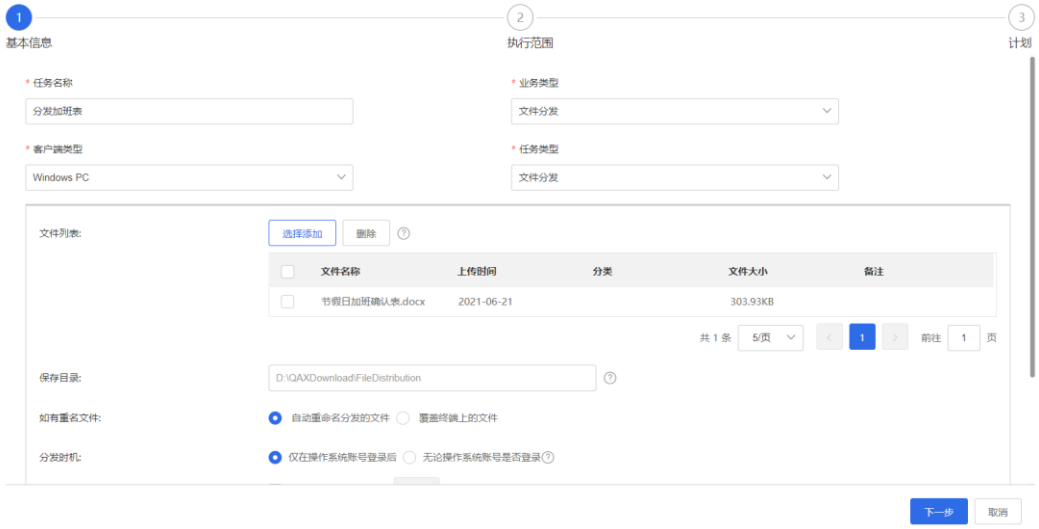


3.3. 终端任务

3.3.1. 分发任务

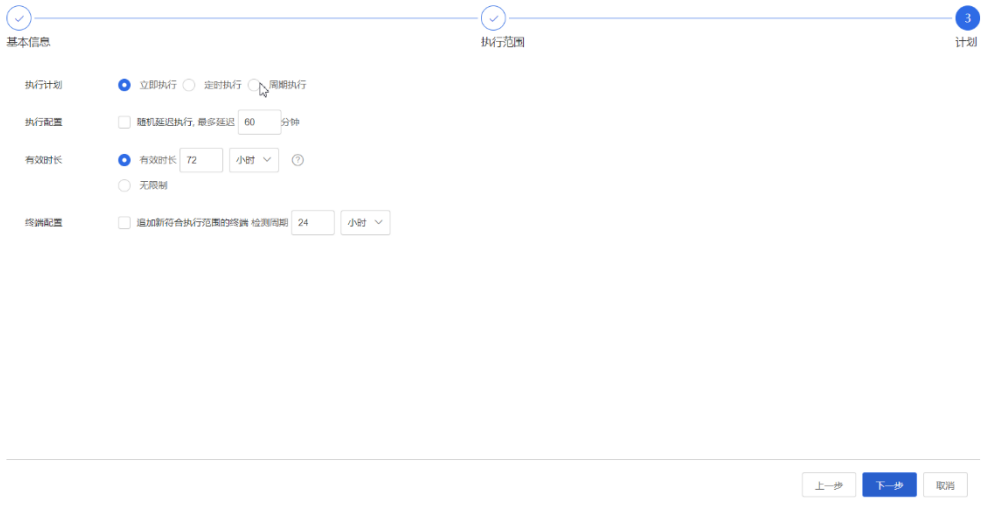
导航到“终端管理>终端任务”，新建和编辑终端任务分为 3 步骤，配置基本信息、执行范围、计划。

A. 基本信息，配置任务的名称、具体内容。



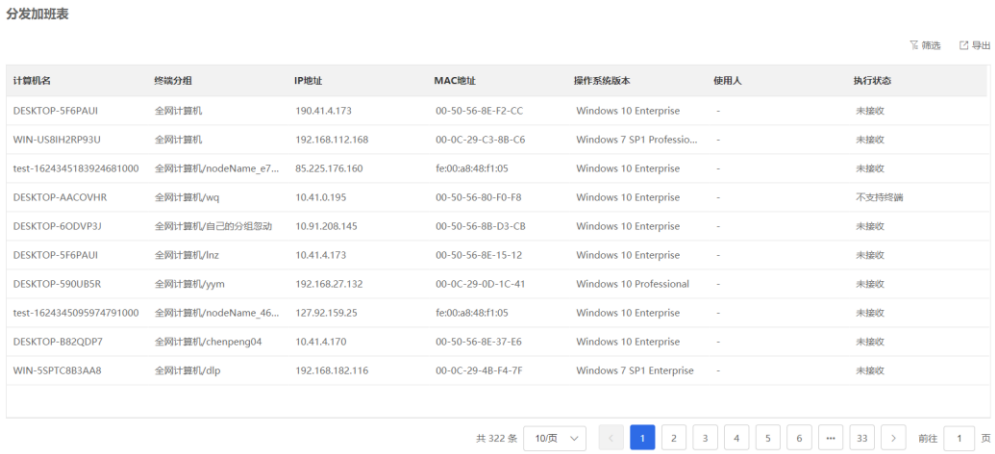
B. 执行范围，配置任务的执行的终端范围。

C. 计划，配置任务在什么时候、什么条件下执行。



D. 查看任务执行结果

具备完整的任务状态（未接收，已接收待执行，执行中，执行成功，执行失败，管理员取消，用户取消，终端不支持，到期停止执行）、执行失败的原因（不同类型的任务的失败原因各不相同，取决于功能特性）、执行时间。



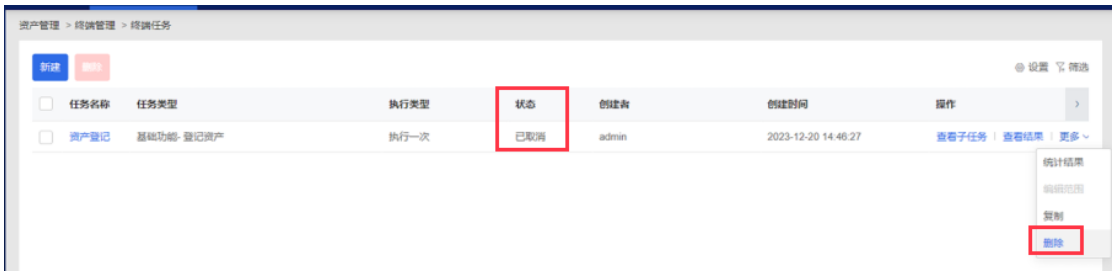
【注意】任务下发功能是为了方便管理员执行一些快捷功能作用，但是在使用过程中可能因为配置检查不够或下发文件脚本的兼容性问题导致下发后出现无法预料的结果。建议操作时通过分组分批下发。同时随时观察下发任务的执行情况，以确保结果和预期一致。

3.3.2. 任务执行统计

导航到“终端管理>终端任务，找到需要统计的任务即可查看任务执行结果的统计结果。

3.3.3. 任务管理功能

可对已创建的终端任务进行管理，对执行中的任务可进行取消操作；对已取消的任务可进行删除操作。



3.3.4. 任务设置

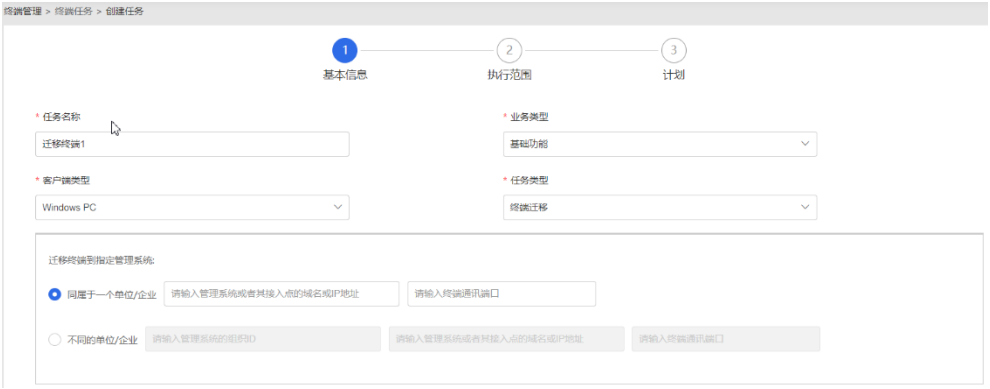
可设置自动清理已完成的历史任务和限制任务数量。将默认限制周期任务的最大运行数量为 20 个，限制追加终端的任务的最大数量为 100 个，以避免无限制的新增任务将会导致服务器的资源耗尽。

3.3.5. 迁移终端

迁移终端指将一套管理系统下的终端迁移到另外一套管理系统中。

迁移终端是通过“任务”将终端迁移到另外一套管理系统中，需要提前部署目的管理系统，然后在原管理系统创建迁移终端的任务。

入口：终端管理>终端任务。



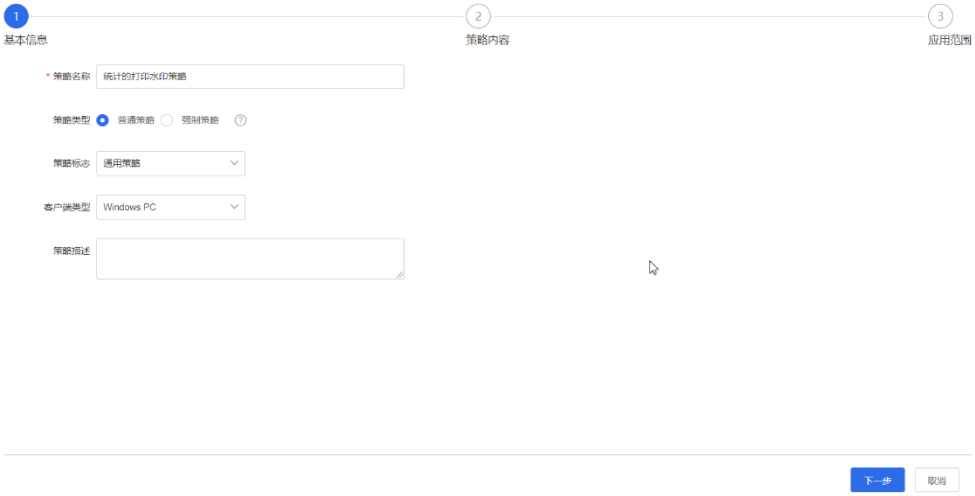
3.4. 策略管理

策略是配置项的集合，用于将企业的安全管理制度转换为终端可执行的指令。根据安全业务特性，由 N 个配置项组成。分为终端策略和用户策略，两者的分发方式一致。

3.4.1.新建、编辑策略

导航到“安全防护”或“数据安全”下各个业务的策略管理下，新建和编辑策略分为 3 步骤，配置基本信息、策略内容、应用范围。

A. 基本信息



B. 策略内容

C. 应用范围

D. 策略类型

- 普通策略：普通策略是下级组的策略优先级高于上级组。
- 强制策略：强制策略是上级组的策略优先级高于下级组。

【注意】如果策略中具有列表形式的策略配置项，策略最终生效结果需结合“覆盖”、“合并”的策略冲突处理方式。策略冲突处理方式为“合并”，将按照优先级高低依次将策略配置项内容串联一起。策略冲突处理方式为“覆盖”，优先级高的策略配置项覆盖优先级低的策略配置项。

E. 策略标志

策略的标签，用于策略管理中方便筛选。

F. 配置项模式

- 开启/关闭：“关闭该配置项不会被启用，策略内容中关闭的配置项，不会与其他策略冲突，也不会与其他策略的配置项合并。
- 允许终端用户修改：“允许终端用户修改”的配置项也会被启用，区别在于应用到终端后，终端用户可以修改配置项内容，并且被修改后终端配置项不再刷新为策略配置项内容（即使管理员又修改了策略内容），除非管理员在策略中修改为“不允许终端用户修改”。

G. 策略冲突处理方式

- 策略的优先级由其在分组树上的深度决定，深度越深则普通策略的优先级越高，深度越浅则普通策略的优先级越低；强制策略的优先级与普通策略相反，深度越浅则强制策略的优先级越高。

•自定义组必须挂在某一个普通分组上，其深度等于所挂的组织结构组。自定义组的策略的优先级高于组织结构组的，不论是否开启强制执行。

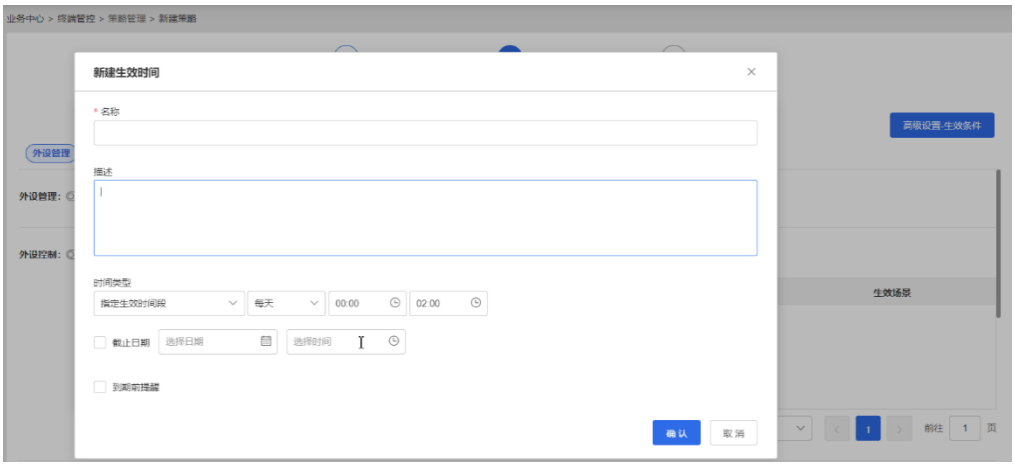
H. 策略管理原则

- 如果需要策略不会被下级覆盖则必须将配置项设为“强制策略”或者不分配给下级管理员创建策略的权限。
- 如果需要刷新（覆盖）下级组的策略则必须将新建 “强制策略”覆盖已有策略。

I. 策略生效时间

策略生效时间指策略的配置项的生效时间。

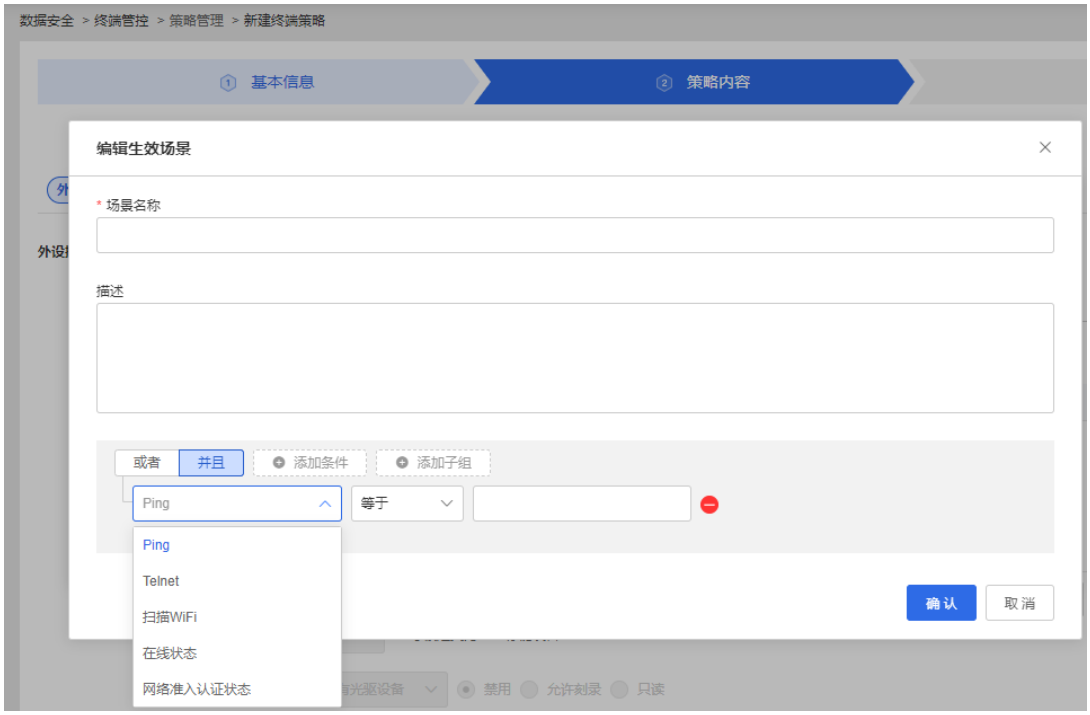
在策略的“高级设置”中配置策略的生效时间，在策略的配置项中关联本策略的高级设置中创建的生效时间。



策略生效场景

策略生效时间指策略的配置项的生效场景，生效场景目前支持网络场景，支持按照“Ping、Telnet、扫描 WiFi（无线网络）、终端的在线状态”单个或者组合条件判断终端所处的网络场景。

在策略的“高级设置”中配置策略的生效场景，在策略的配置项中关联本策略的高级设置中创建的生效场景。

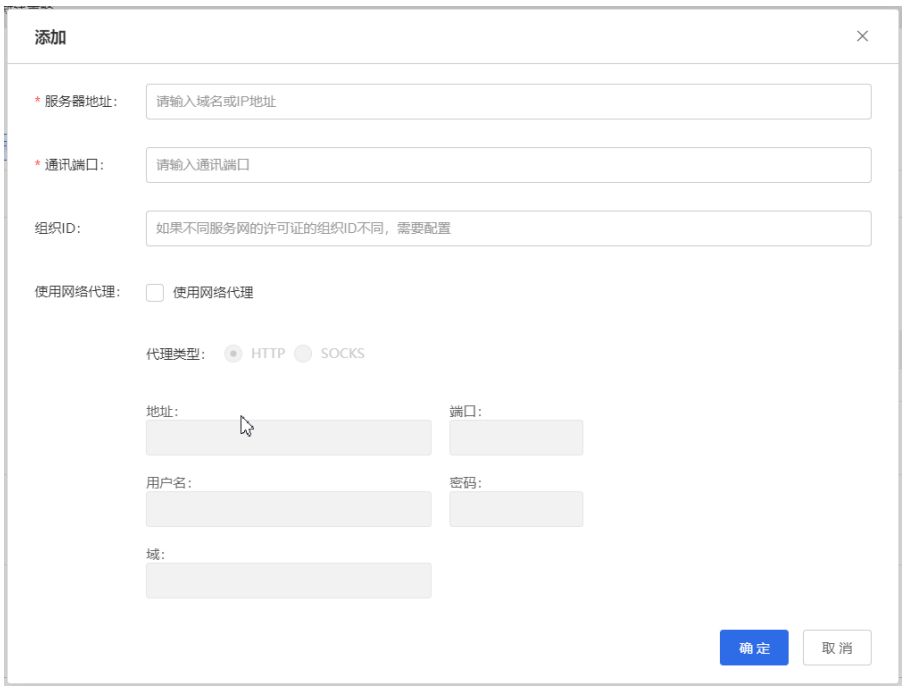


【注意】该场景配置后，建议通过少量终端验证配置成功后，再进行大规模策略应用。防止场景不生效导致策略不符合预期。

3.4.2. 自动切换服务器

自动切换服务器终端在多套管理系统之间自动迁移的功能。用于按照安全域管理的场景，终端根据接入的安全域自动切换到对应的奇安信天擎管理系统中。

入口：管理中心>终端管理>基础策略>通讯设置。



3.4.3. 终端兼容配置

客户端程序在对终端安全的保护过程中，对于不同的安全问题会采用有针对性的技术方式。在部署过程中，特别是跟一些使用同类技术方式的软件共存时，可能会出现兼容性问题。系统提供了一些便捷配置来实现与其它软件的兼容共存。

3.4.3.1. HOOK 白名单

操作入口：资产管理>终端管理>基础策略>白名单设置>HOOK 白名单。

解决问题：应用软件冲突，HOOK 注入其他软件后引起的进程崩溃等问题。

应用场景：客户端应用软件发生冲突时使用。

3.4.3.2. SSL 证书替换白名单

操作入口：资产管理>终端管理>基础策略>白名单设置>SSL 证书替换白名单。

解决问题：为了解决 SSL 加密连接中存在的安全问题，系统在某些场景会采用替换 SSL 证书的方式，可能会引起一些网站和程序的工作异常。可以尝试将其地址或进程加白来进行兼容。

应用场景：需要对网站加白，加白之后则不审计网站。

3.4.3.3. 网络访问白名单

操作入口：资产管理>终端管理>基础策略>白名单设置>网络访问白名单。

解决问题：目标地址加白，被加白的地址在进行访问和数据传输时不再被处理。

【注意】网络白名单应该包括天擎管理中心、天擎应用服务器、内网网关、VPN 地址、零信任地址、准入服务器地址、DNS 服务器、打印服务器等。建议部署前进行配置。以防止终端出现网络问题。

3.5. 终端日志

3.5.1. 终端部署日志

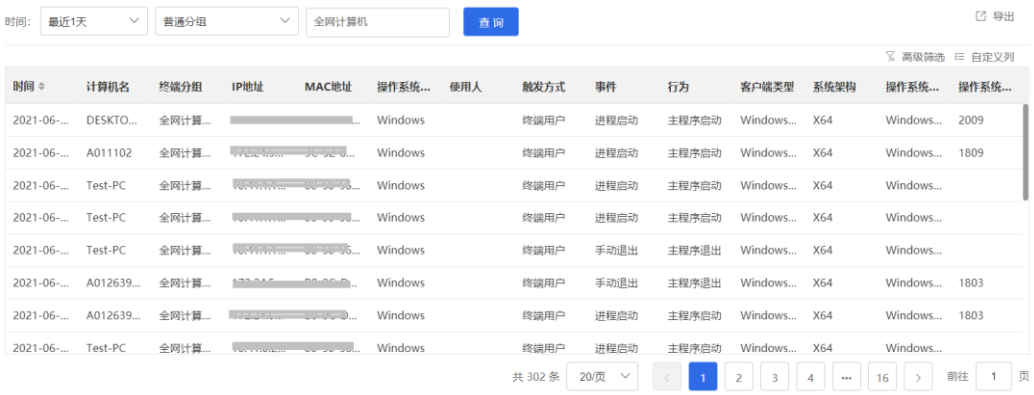
记录该管理中心下的终端的部署信息，包括模块的安装和卸载，支持筛选和导出，支持展示的字段自定义。

3.5.2.终端更新日志

记录该管理中心下的终端的更新信息，包括软件库、病毒库等，支持筛选和导出，支持展示的字段自定义。

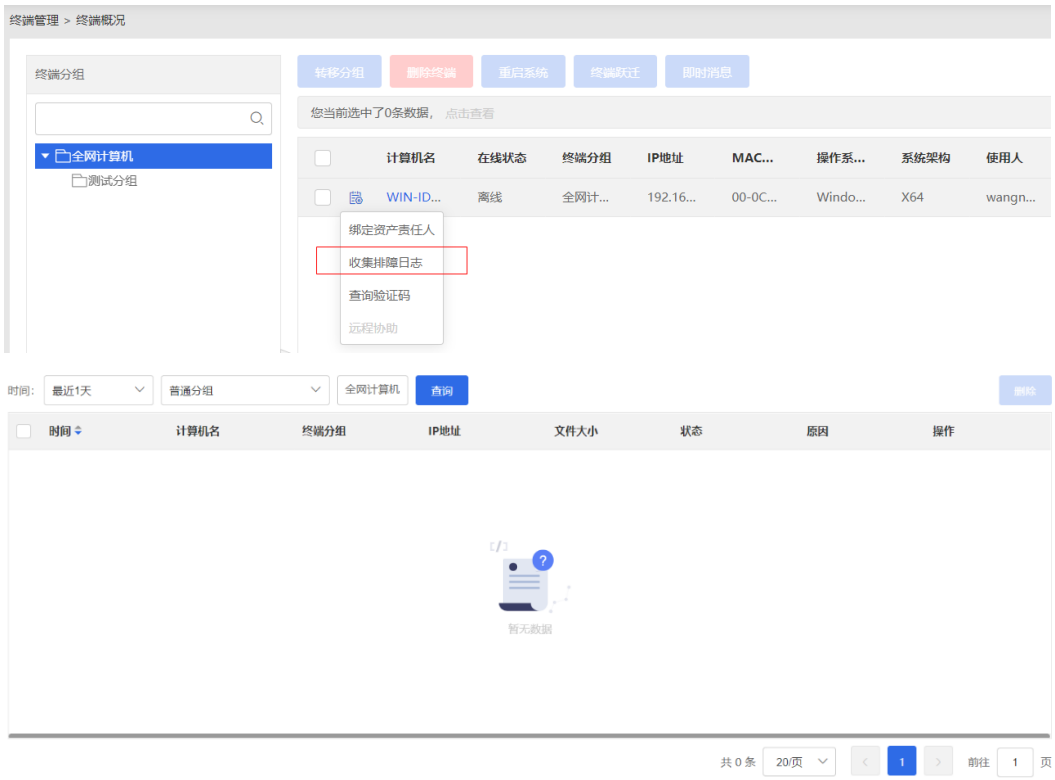
3.5.3.自我保护日志

记录该管理中心下的终端的自我保护，包括主程序启动退出等，支持筛选和导出，支持展示的字段自定义。



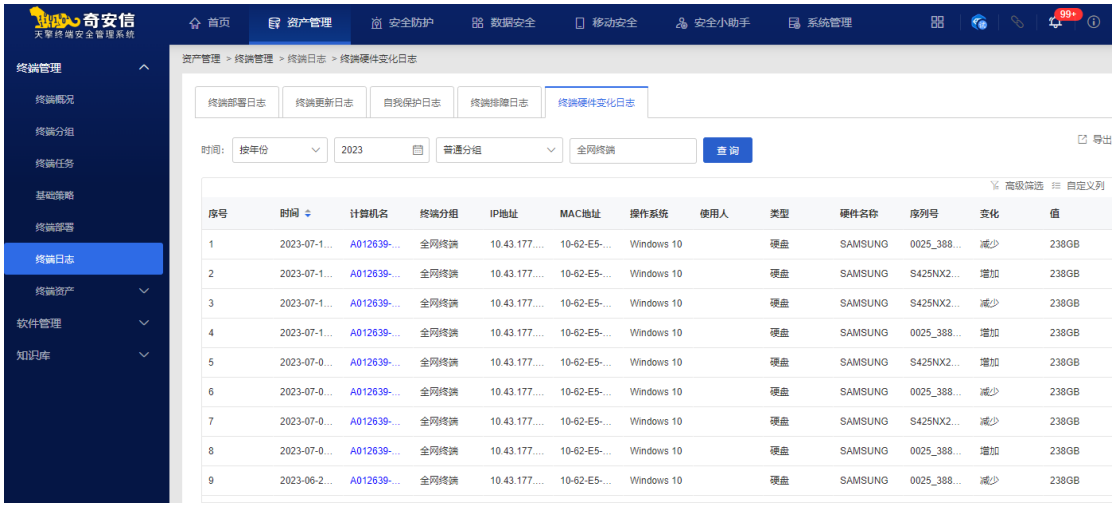
3.5.4.终端排障日志

记录该管理中心下的收集的运行日志用于排障定位，包括主程序安装、运行日志、系统进程列表、网络情况等信息，支持手动删除日志记录和日志文件。（在终端概况单击终端的事件菜单）。



3.5.5. 终端硬件变化日志

记录该管理中心所管终端上的硬件变化信息，如内存、硬盘的变化情况及变化值。



4. 软件管理

为政企客户提供从终端软件资产梳理，到正版化软件、违规软件分析管控的闭环、有效的软件管理方案，管理者亦可依托软件管理提供的安全下载资源，建立私有软件商店，实现全网统一、安全的软件应用基线，软件管理旨在全力为管理者在最大程度降低日常运维的同时实现针对软件的 可见、可管、可信可控的管理预期。

4.1. 基本概念

4.1.1. 软件

应用软件主要是指运行于计算机操作系统中，根据应用的不同定位，帮助用户解决软件下载和安装的问题。

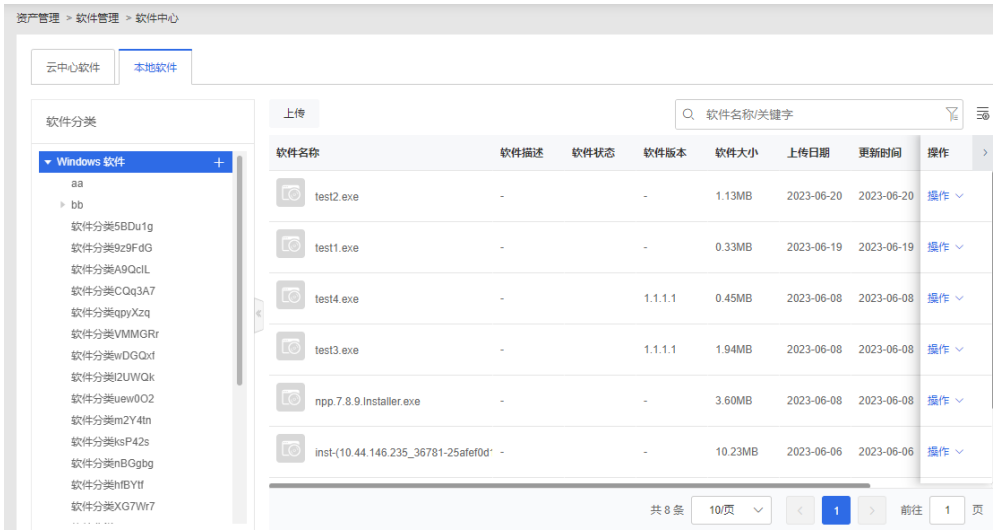
4.1.2. 软件中心

软件中心提供私有软件中心软件的同时支持管理员对内部软件的上传和下载同时对上传的软件进行安全检查。

4.2. 软件中心

4.2.1. 本地软件

本地软件库是软件管理系统的核心功能模块之一，用于上传企业私有软件或者一些公网没有的软件安装包，可以对软件进行编辑，上架，下架，删除，更新，回退。界面如下图所示：



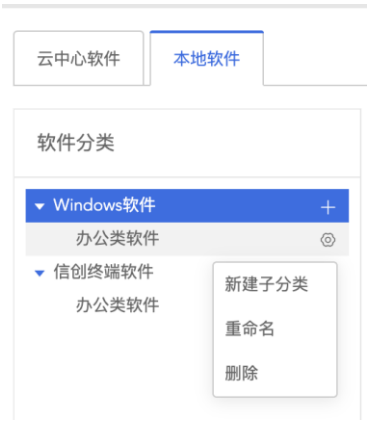
4.2.1.1. 软件分类

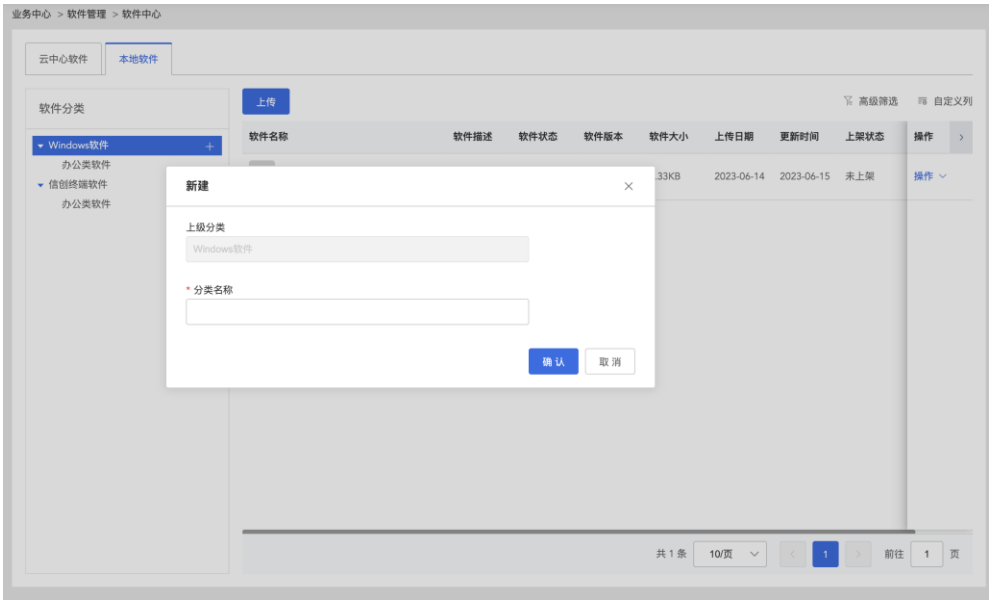
按照软件的用途不同将对其进行自定义分类。

A、**新建**。点击右侧的+，新建软件分类，填写分类名称。

B、**重命名**。选中需要命名的分组，右键 选择重命名，进行名称的修改。

C、**删除**。点击选中需要删除的分组，右键 选择删除，对该分类进行删除。

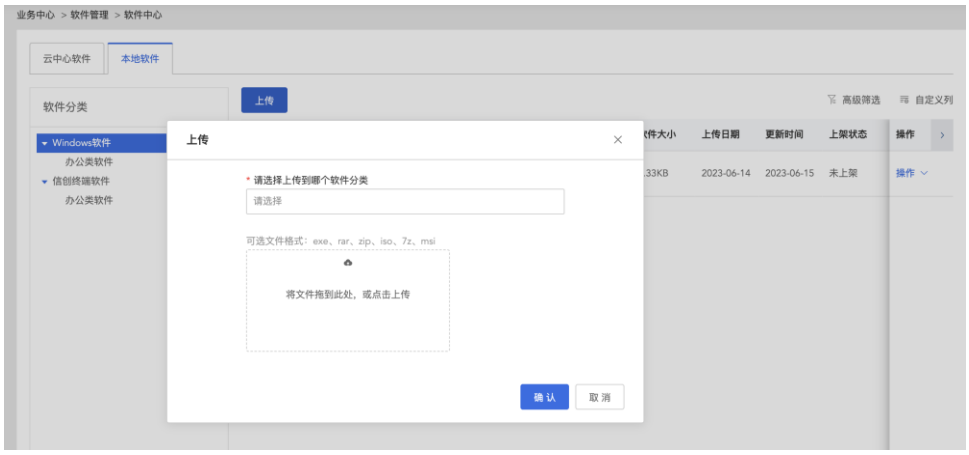




4.2.1.2. 软件上传

管理员将需要上架的企业内部软件上传到本地软件中心。

A. **上传**。点击上传，选择软件分类将需要上传的软件上传到本地软件中心。文件格式支持 exe,rar,zip,iso,7z,msi，其弹窗如下：

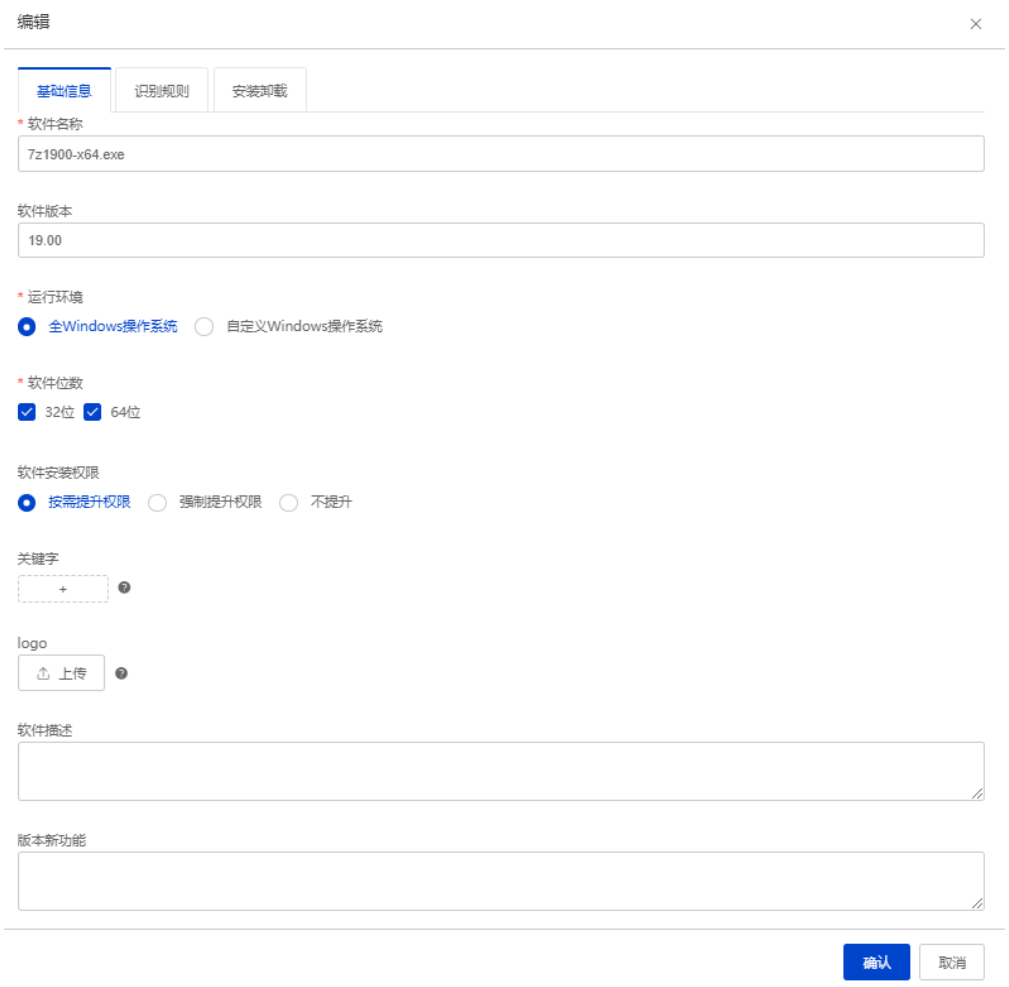


等待上传完成后，会自动生成文件的 MD5 值，管理员可以通过 MD5 值进行软件的校验。

云查校验：若文件在上传过程中有未知威胁，软件中心会进行云查鉴定，确保软件的安全性，并对用户进行弹窗提醒告知用户做相应的处理。

B. **编辑** 对已经上传完成的软件进行编辑处理，可配置项包括基础信息，识别规则，安装卸载。

基础信息：配置中可以对软件的名称，运行环境，软件位数，软件安装权限，关键字，logo 进行定制修改。



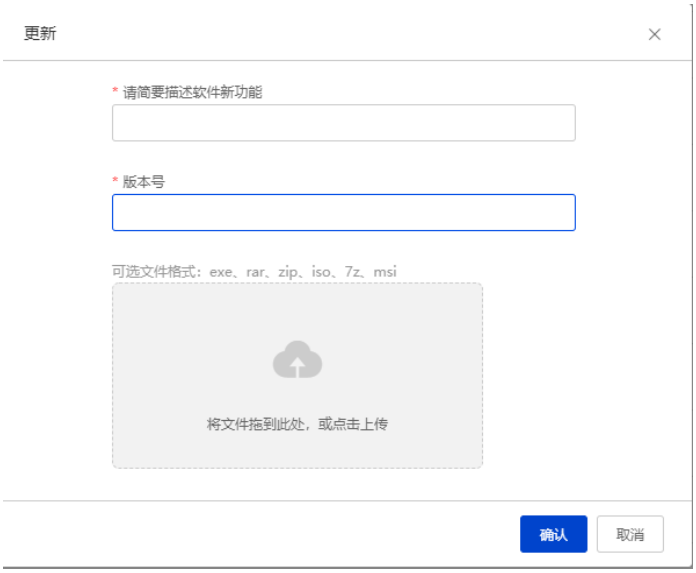
识别规则：配置可以对注册表，自定义组合，配置主程序进行设置。

示例：①软件安装在注册表的标志，如蓝信+在注册表的键值为LanxinSoftCustom

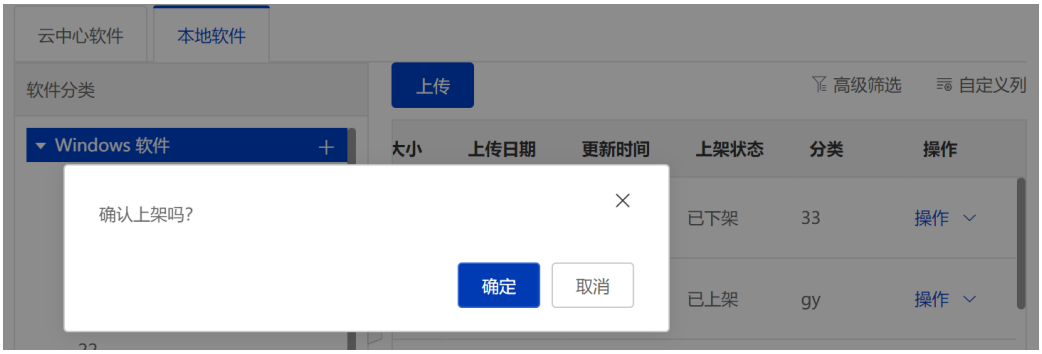
②软件运行时在进程中的主程序名，如蓝信+的主程序名为LxMainNew.exe

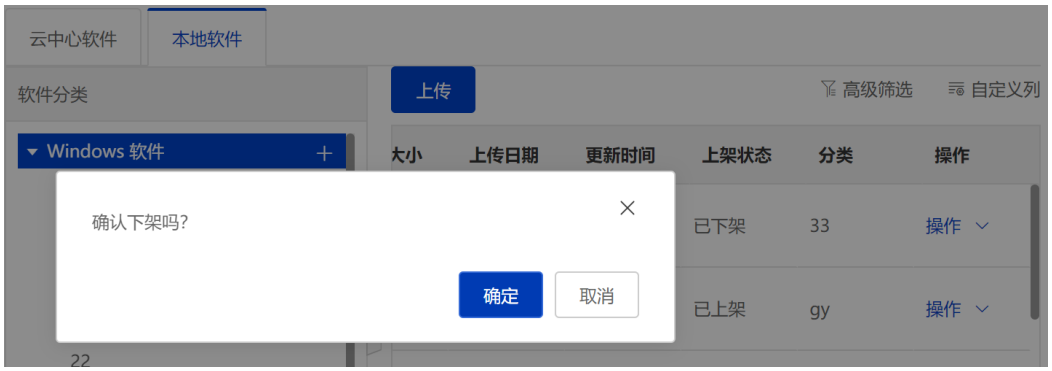
安装卸载：可以配置软件的静默安装和静默卸载参数，当此软件安装或卸载时通过静默的方式呈现。

C. **更新：**选中需要更新的软件将高版本的软件上传到本地软件中心。



D. **上架/下架** 选中需要上架或者下架的软件，未上架的软件可将其选择上架，已上架的软件可选择将其下架。

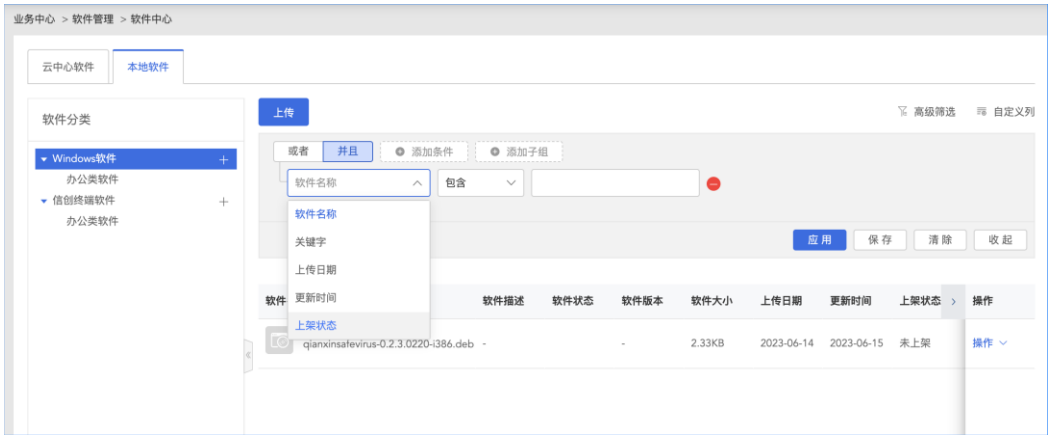




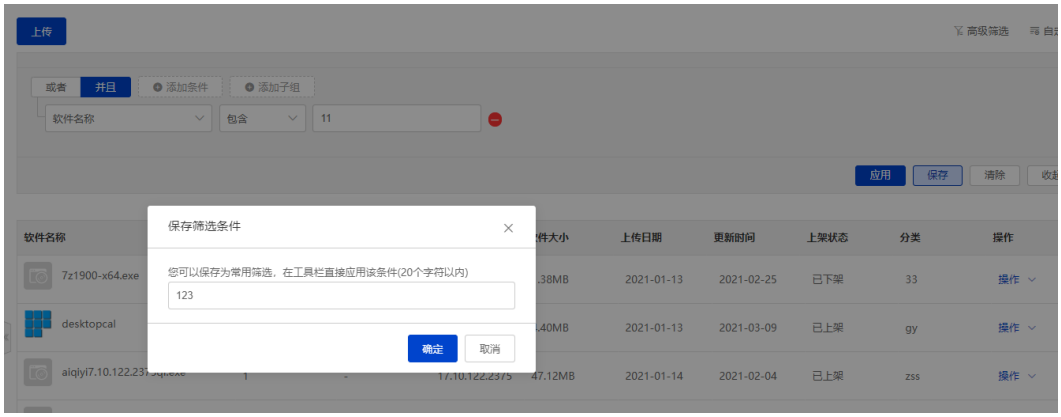
E. **转移分组**：将软件的当前分组转移到其他分组，完成软件所在分组的变更。

4.2.1.3. 高级筛选

高级筛选可以按照软件名称，关键字，上传日期，更新时间，上架状态对本地软件进行筛选：

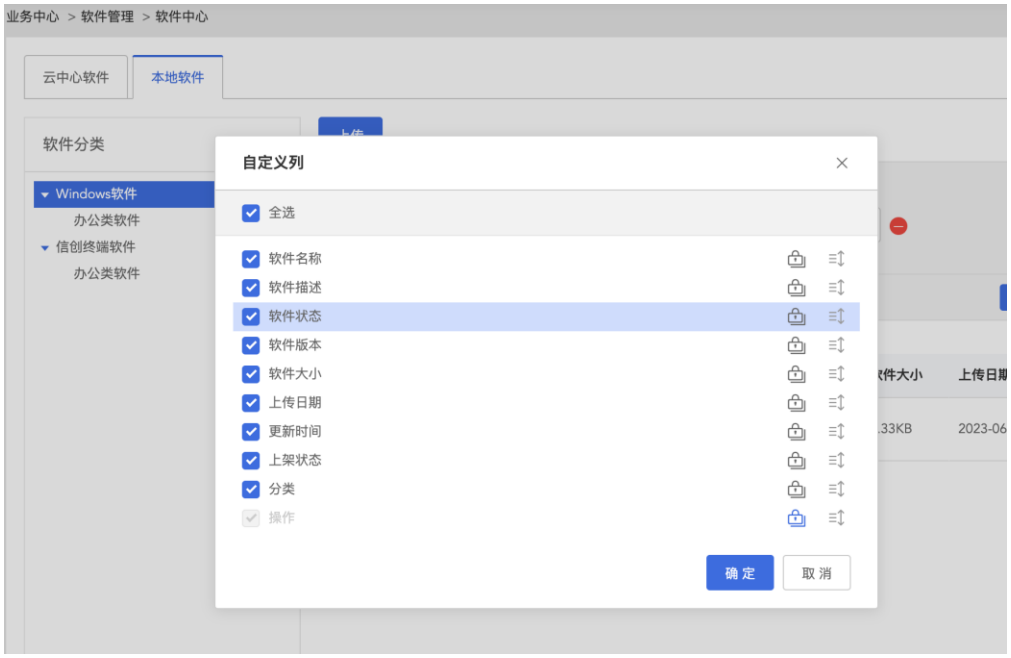


点击**应用**后即可按照当前条件筛选出查询结果，点击**保存**可将当前条件保存后方便下次进行筛选。



4.2.1.4. 自定义列

自定义选择需要显示的软件信息，包括软件描述，软件状态，软件名称，软件版本，软件大小，上传日期，更新时间，上架状态，分类。

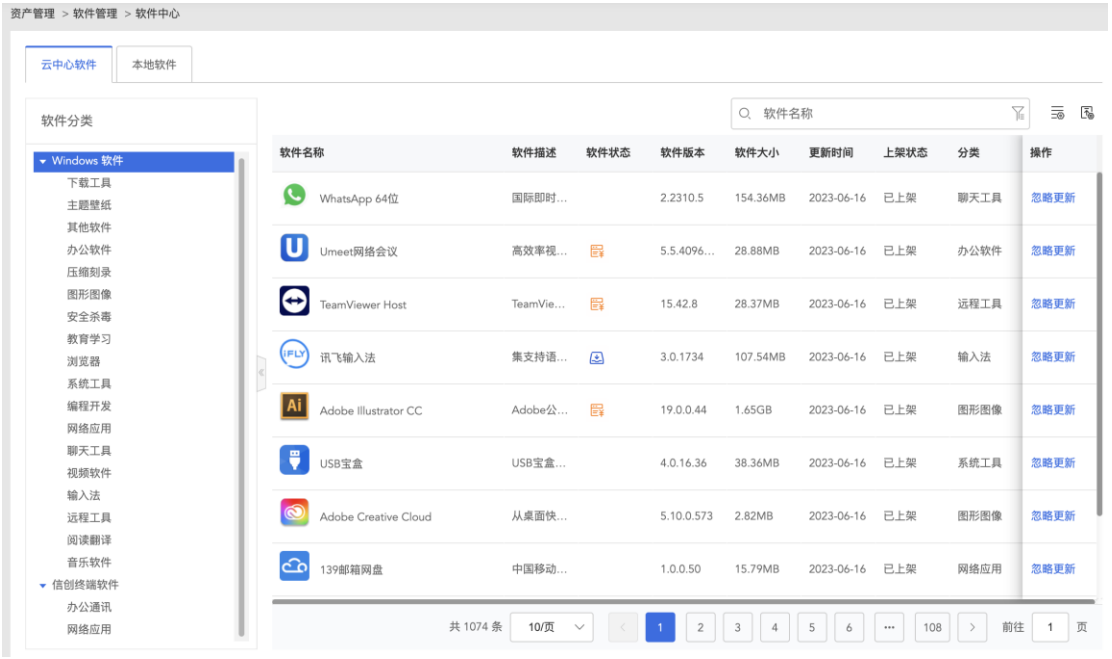


4.2.2. 云中心软件

云中心软件是由奇安信软件运营团队进行定期更新维护，客户可根据实际业务使用情况开启即可。

4.2.2.1. 软件云中心

云中心软件内的软件为天擎自运营软件资源，软件分类包括：下载工具、主题壁纸、办公软件、压缩刻录、图形图像、安全杀毒、教育学习、浏览器、系统工具、编程开发、网络应用、网银、聊天工具、视频软件、输入法、远程工具、阅读翻译、音乐软件、其他软件 19 个分类，软件资源丰富。



4.2.2.2. 上架设置

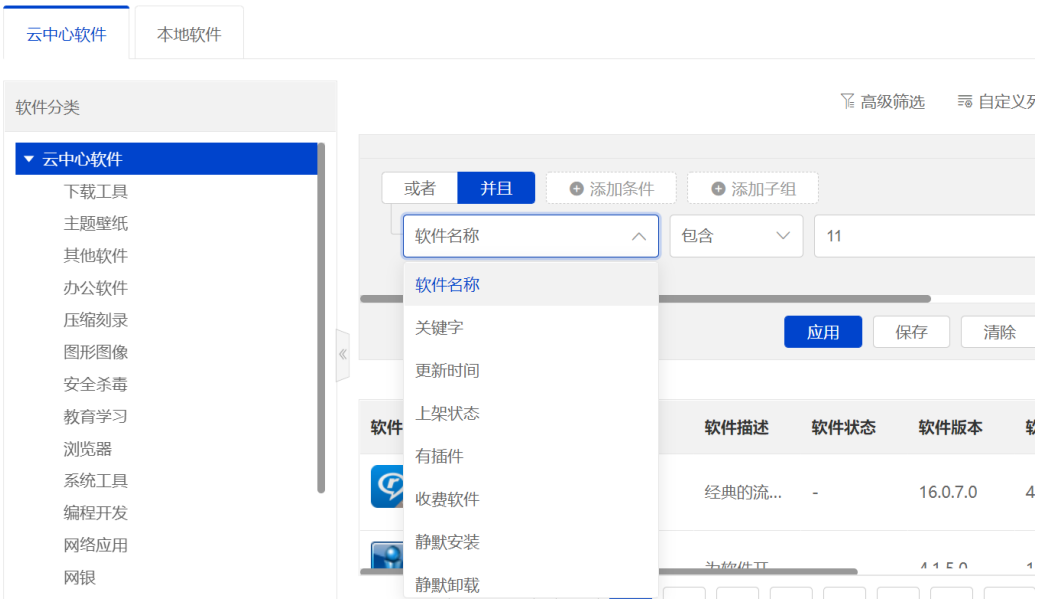
云中心软件上架设置包括黑名单和白名单两种方式。

A. **黑名单**：将需要设置的软件类别和软件添加到黑名单中，该软件上架状态立刻变成下架状态，不允许用户进行下载。

B. **白名单：**将需要设置的软件类别和软件添加到白名单中，该软件上架状态为已上架，允许用户下载。

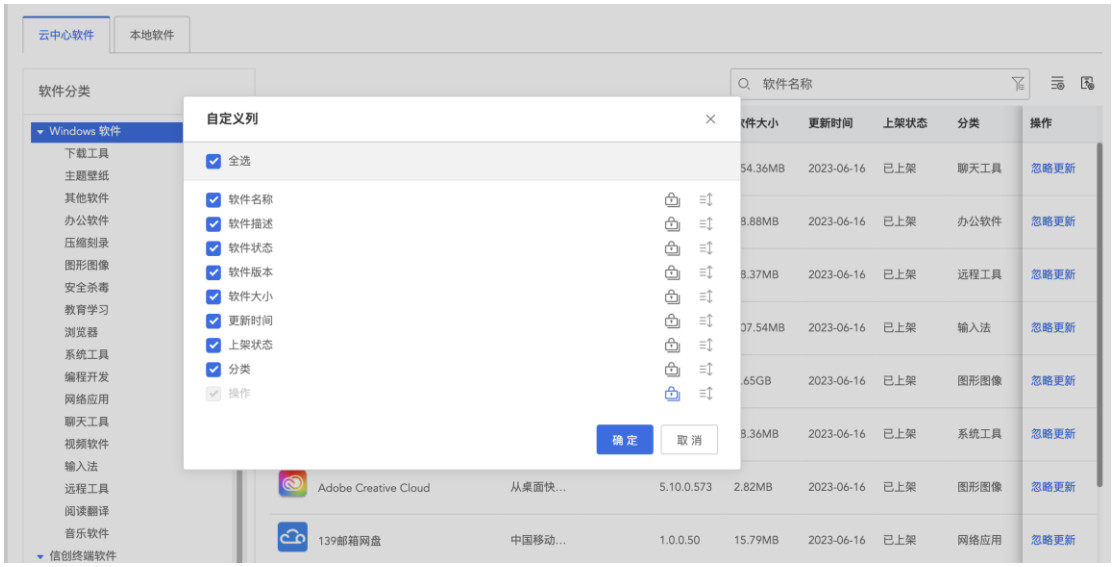
4.2.2.3. 高级筛选

高级筛选可以按照软件名称，关键字，更新时间，上架状态，有插件，收费软件，静默安装，静默卸载对云中心软件进行筛选：



4.2.2.4. 自定义列

自定义选择需要显示的软件信息，包括软件描述，软件状态，软件名称，软件版本，软件大小，上传日期，更新时间，上架状态，分类。



4.3. 软件管理策略

本章节主要介绍企业软件管理系统的使用。

4.3.1.终端模块

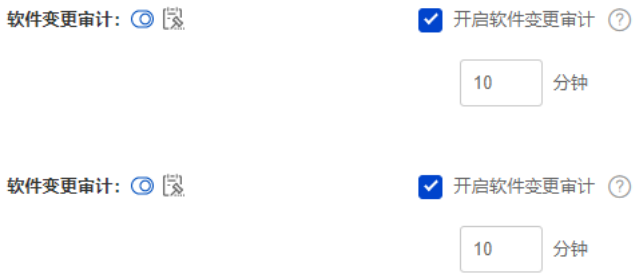
可以设置终端显示的模块，以及在“终端管理”，“基础功能”终端定制中设置中，设置软件管理和软件统计模块。常用于仅统计终端的软件安装情况，而不使用软件管理功能。

4.3.2.上报已安装软件

在“软件管理>策略管理>基础设置”功能内“开启上报已安装软件”配置，对客户端会自动采集终端上已经安装的软件，若开启了此选项，终端会强制采集终端安装的软件。

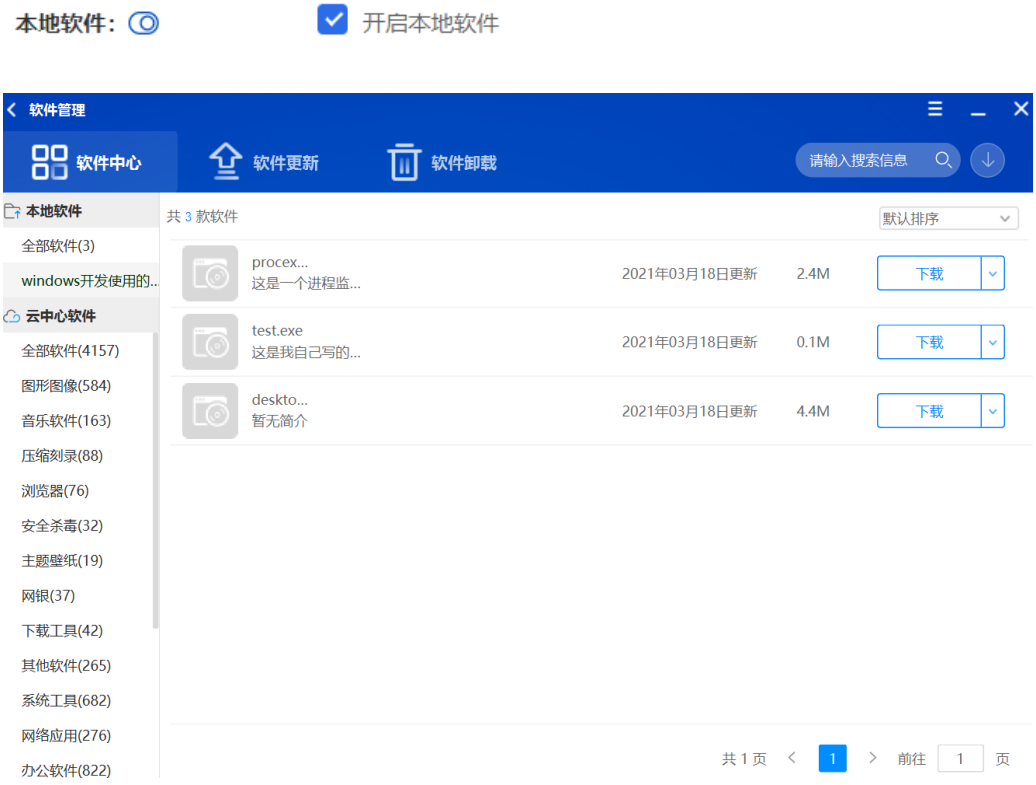
4.3.3.软件变更审计

勾选“软件变更审计”即开启软件变更审计，变更时间可以设置自定义采集时间。



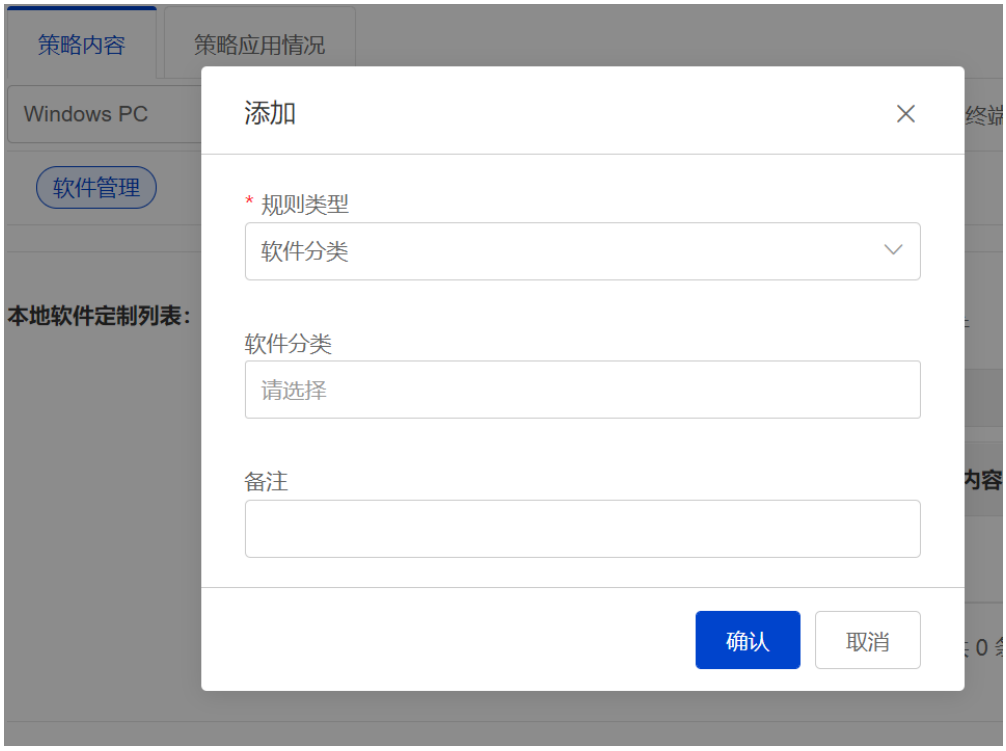
4.3.4.本地软件

开启本地软件后可以在终端软件管理中显示本地软件。



4.3.5.定制本地软件

选择需要定制的软件在终端软件管理中展示，可在终端分组策略中配置。添加规则可按照软件分类和软件两个维度来管理。



4.3.6. 云中心软件

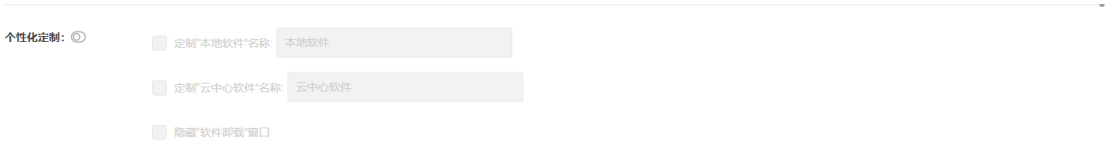
开启云中心软件后可以在终端软件管理中显示云中心软件。

4.3.7. 定制云中心软件

选择需要定制的软件在终端软件管理，云中心软件中展示，可在终端分组策略中配置。添加规则可按照软件分类和软件两个维度来管理。

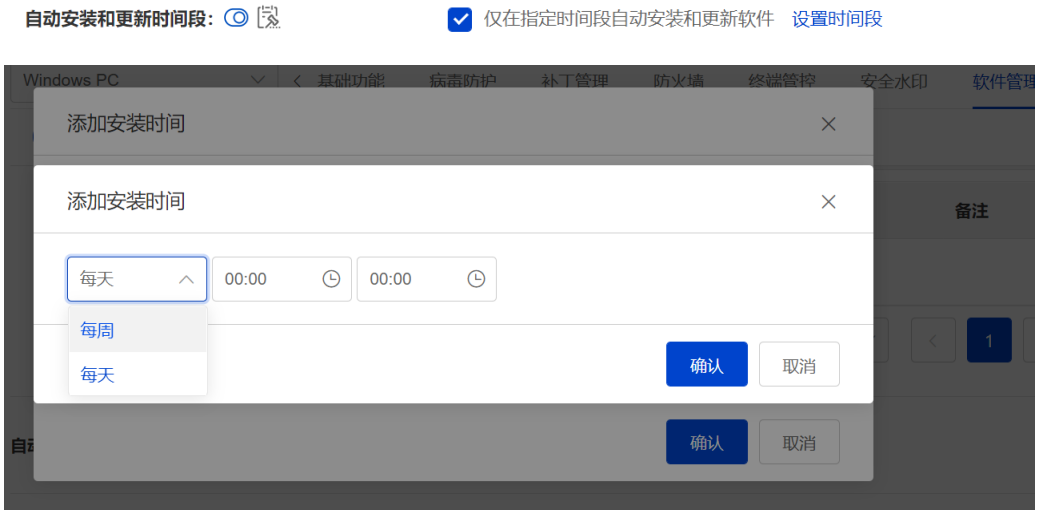
4.3.8. 个性化定制

对终端软件管理中显示的名称及功能页面是否展示进行定制，包括本地软件名称和云软件名称和软件卸载是否展示的配置。



4.3.9. 更新时间段

通过自定义设置时间段，软件的更新能在指定的时间段内完成。时间频率为每周或者每天。



4.3.10. 安装超时时间

单个软件安装的最长时间，当超过设置的最长时间后该软件将不会自动安装，等待下一个周期到来后接着继续安装。

4.3.11. 下载设置

软件下载目录默认是在（D:\QAXDownload\software），管理员可以手动设置，软件需要安装的目录，若此目录不存在，会自动创建目录。可设置是否在下载收费软件，有插件软件时提醒，自动清理软件安装包，当软件包保留自自定义设置的时间后系统会自动清除，软件在下载过程中关闭主界面可设置继续下载软件，停止下载软件，每次询问终端用户三种提示方式。

4.3.12. 更新设置

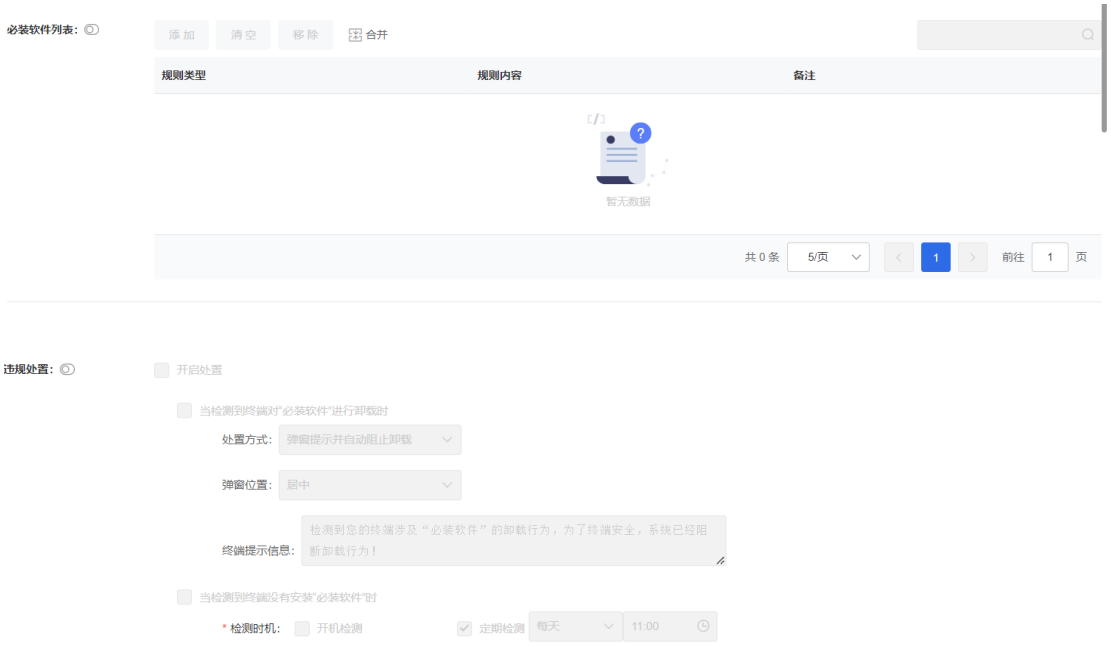
设置软件的更新提醒，可按照每天，每周，自定义时间和不提醒及自动更新几种方式。

4.3.13. 忽略更新软件列表

将需要忽略的软件添加到忽略软件列表中，有新版本后该软件会自动忽略升级。添加规则包括软件分类和软件两种规则。

4.3.14. 必装软件

将需要终端必须安装的软件在“软件管理>策略管理>必装软件>必装软件列表”内进行添加配置，也可在“软件管理>策略管理>必装软件>违规处置”内对卸载必装软件的违规行为进行管控配置，终端收到策略后，会按照配置执行必装软件的防卸载和卸载后的自动安装及安装失败后的相关处置管理。

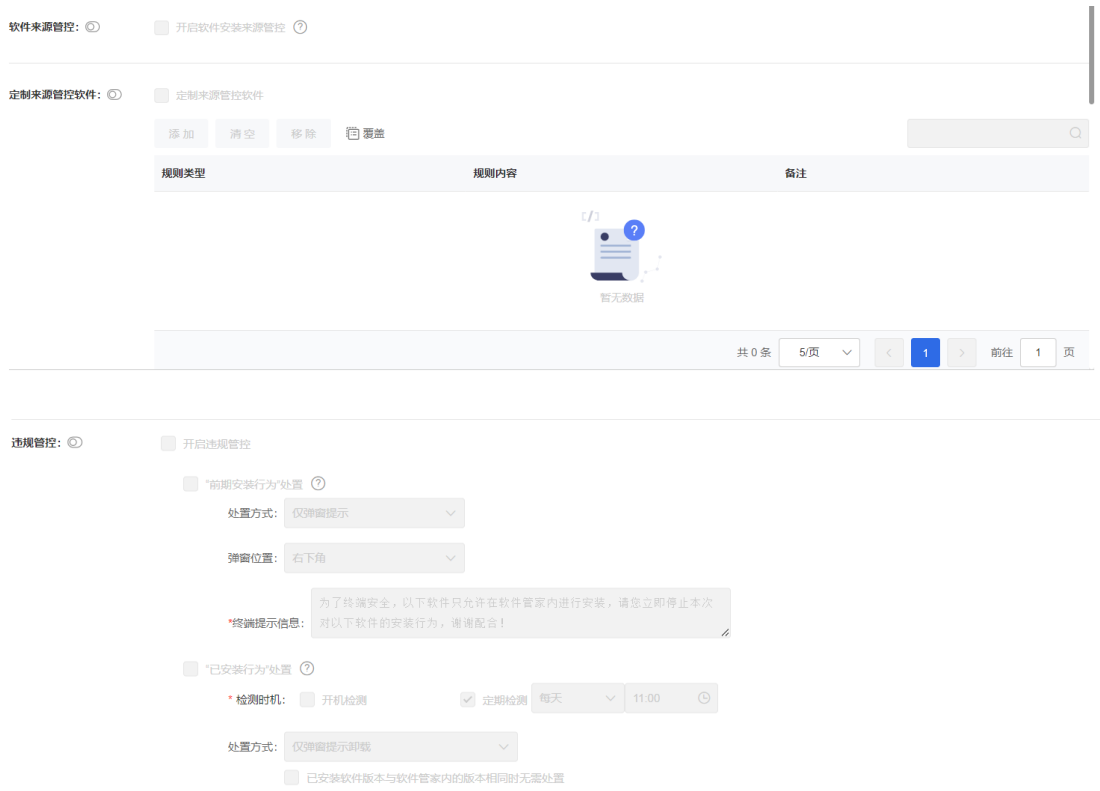


4.3.15. 禁止安装

将禁止终端安装的软件在“软件管理>策略管理>禁止安装>定制禁止安装软件列表”内进行添加配置，也可在“软件管理>策略管理>禁止安装>违规处置”内对禁止软件的安装违规行为进行管控配置，终端收到策略后，会按照配置执行禁止安装软件的安装行为管控以及禁止安装软件安装后的相关处置管理。

4.3.16. 来源管控

在“软件管理>策略管理>来源管控”功能内可“开启软件安装来源管控”，并对“违规管控”进行配置。终端收到策略后，会对软件的安装来源进行管控，按照配置执行非软件管家来源软件的安装行为管控以及软件安装后的相关处置管理。如果您仅需要对本地软件库内特定的几款软件的安装来源进行管控，可在“软件管理>策略管理>来源管控>定制来源管控软件”内对软进行进行选择配置。



当需要对一些拦截进程需要加白时，可在“软件管理>策略管理>来源管控>管控白名单”内进行添加配置，配置后，终端不在对以下文件的来源进行管控。

4.3.17. 字体统计

在“软件管理>策略管理>字体统计”功能内“开启已安装字体上报”配置，对客户端会自动采集终端上已经安装的字体，若开启了此选项，终端会强制采集终端安装的字体。也可对字体变化检测周期进行配置。

4.3.18. 关闭云中心软件

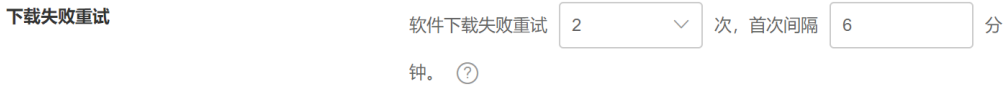
在“软件管理>业务设置”中选择关闭云中心软件，开启此选项后即可关闭云中心软件，终端中不在显示云中心软件。

4.3.19. 任务并发

设置软件安装和更新的任务并发数。

4.3.20. 下载失败重试

设置软件下载失败后，下载重试次数和间隔时间。



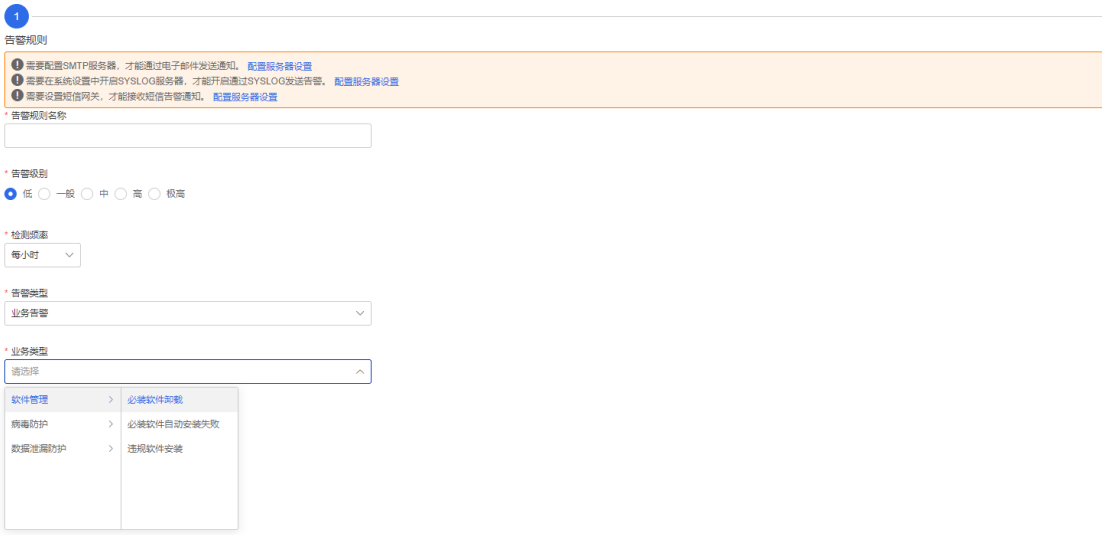
4.3.21. 客户端软件管家全局配置

在“软件管理>业务设置”中可开启受限账号使用客户端软件管理、开启软件管理中文输入。

注：受限账号指非操作系统管理员账号。

4.3.22. 软件管理业务告警

可在告警中心>告警规则内对软件管家业务设置必装软件卸载、必装软件自动安装失败、违规软件安装场景进行告警设置，当监控到网内终端触发告警规则后，会在控制台进行事件告警提醒，管理员可及时获知告警事件及详情，对告警事件进行分析处理。

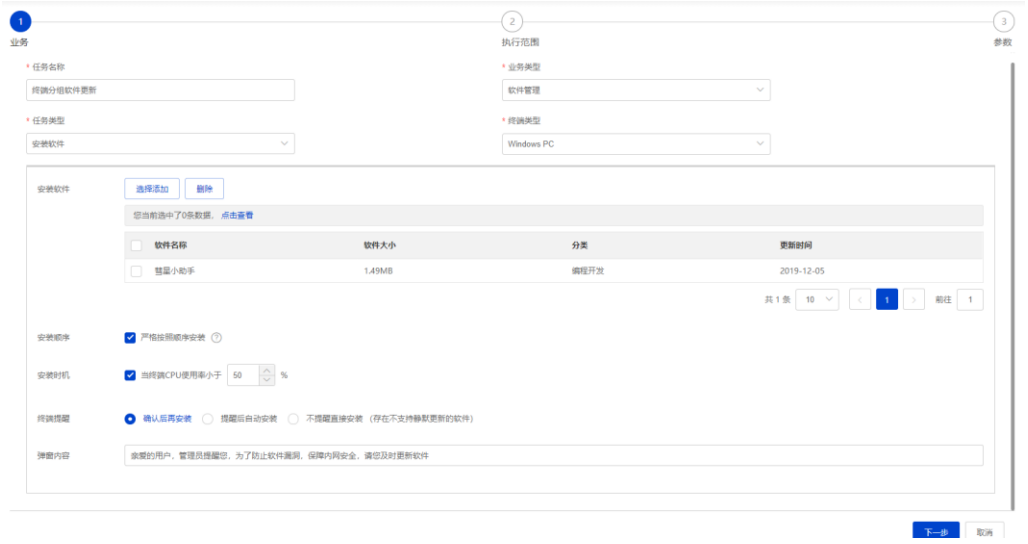


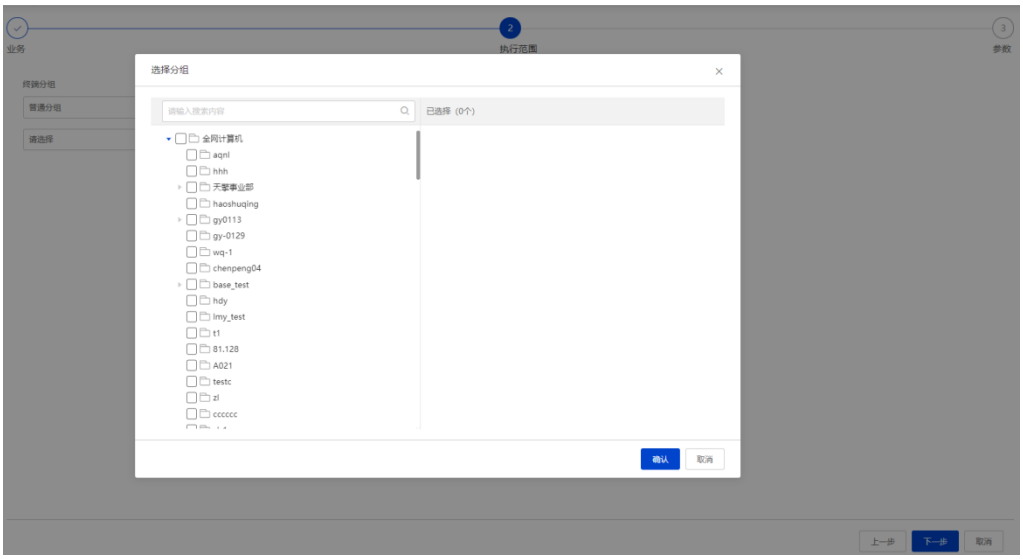
4.4. 软件终端任务

4.4.1. 分组软件任务

在终端任务业务类型中选取“软件管理”，任务类型包括安装软件，更新软件，卸载软件。终端类型包括 WindowsPC、Windows server、信创终端。在软件列表中选择需要管理的软件进行配置，能够按照软件列表中的顺序进行安装。安

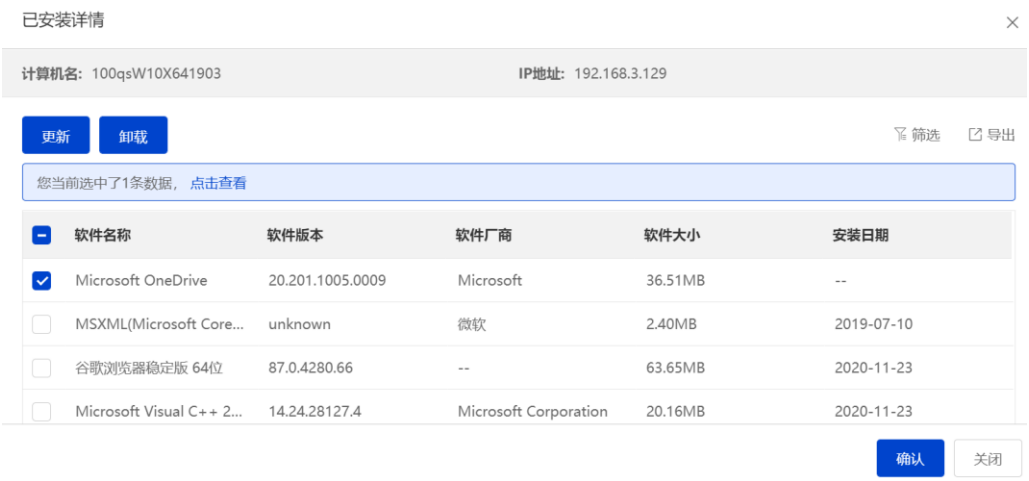
装时机是当终端的 CPU 使用率小于阀值时软件不会安装，终端提醒包括确认后再安装，提醒后自动安装，不提醒直接安装三种提醒方式。配置截图如下：



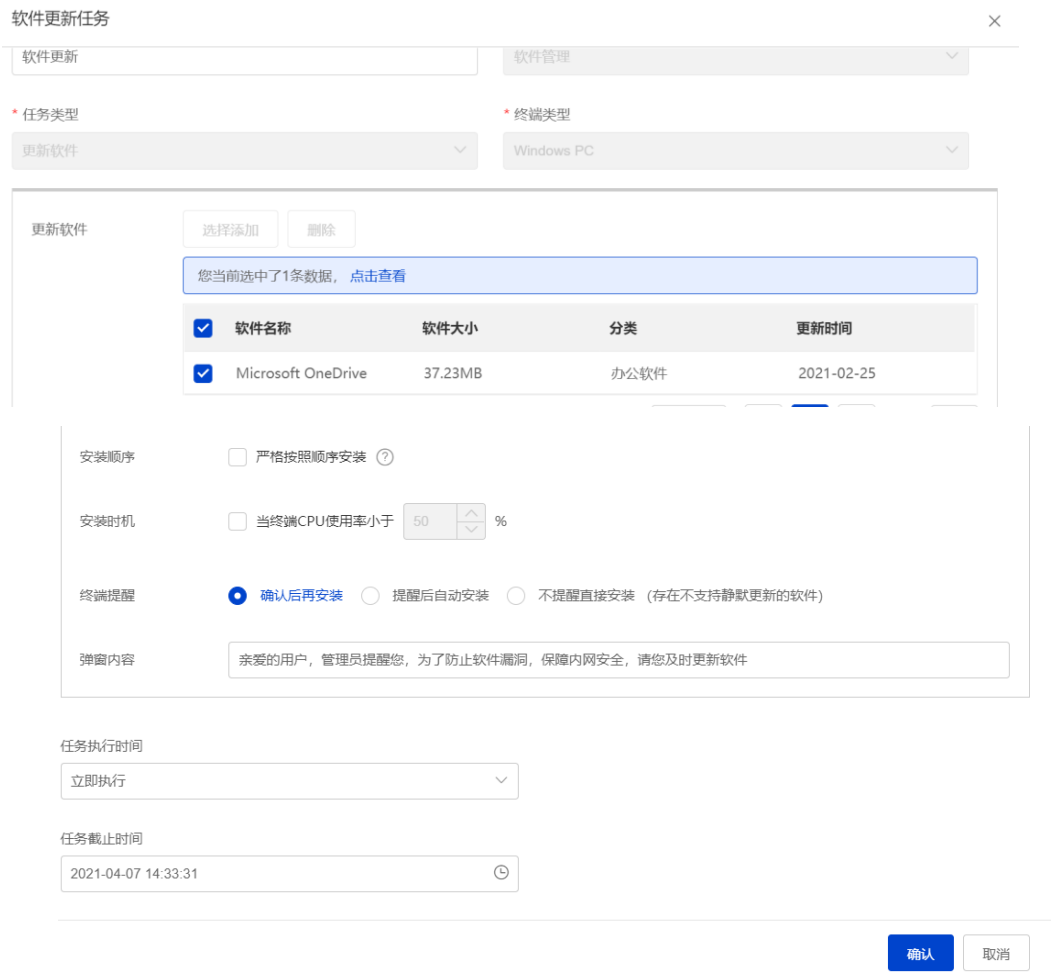


4.4.2. 终端软件任务

在终端软件概况中选取需要维护的终端分组，在已安装的列表中选择软件清单，对其进行更新或卸载。



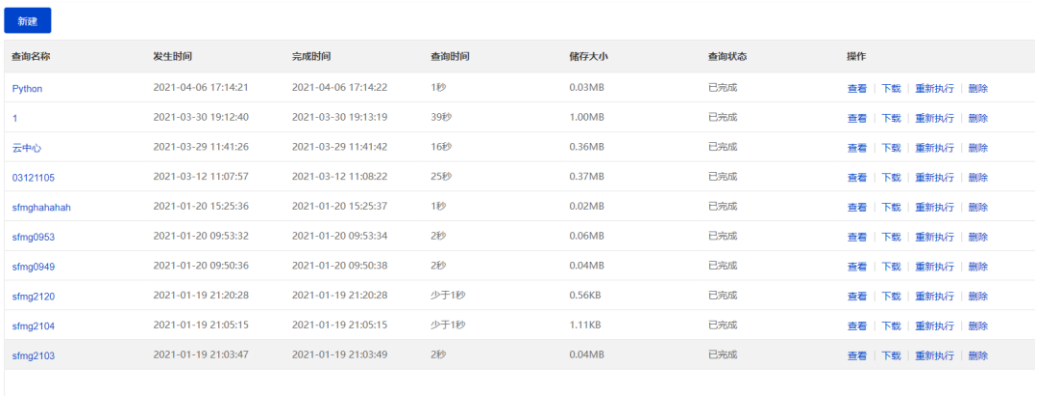
填写任务名称，选取更新软件，配置好安装顺序、安装时机、终端提醒和任务执行开始时间，完成对当前终端的软件升级。

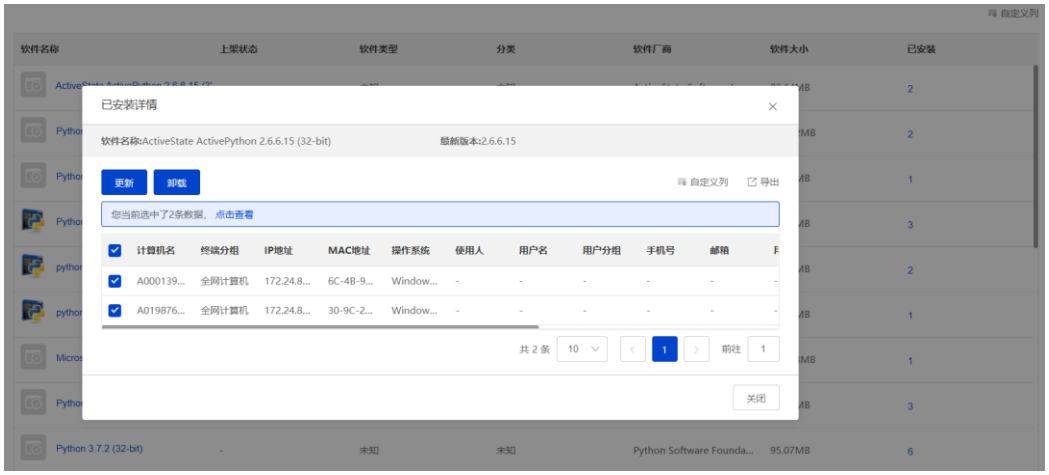


【注意】软件任务下发时如果更新文件较大或涉及终端较多，则建议进行分批下发。以防出现不可预测的问题，如：带宽打满、更新程序兼容性故障等问题。同时下发前先做好少量终端验证工作。

4.4.3. 软件查询任务

软件查询任务是对终端上已经安装的软件按照分组和软件类型进行查询，同时可对查询统计结果中的软件进行更新和卸载。

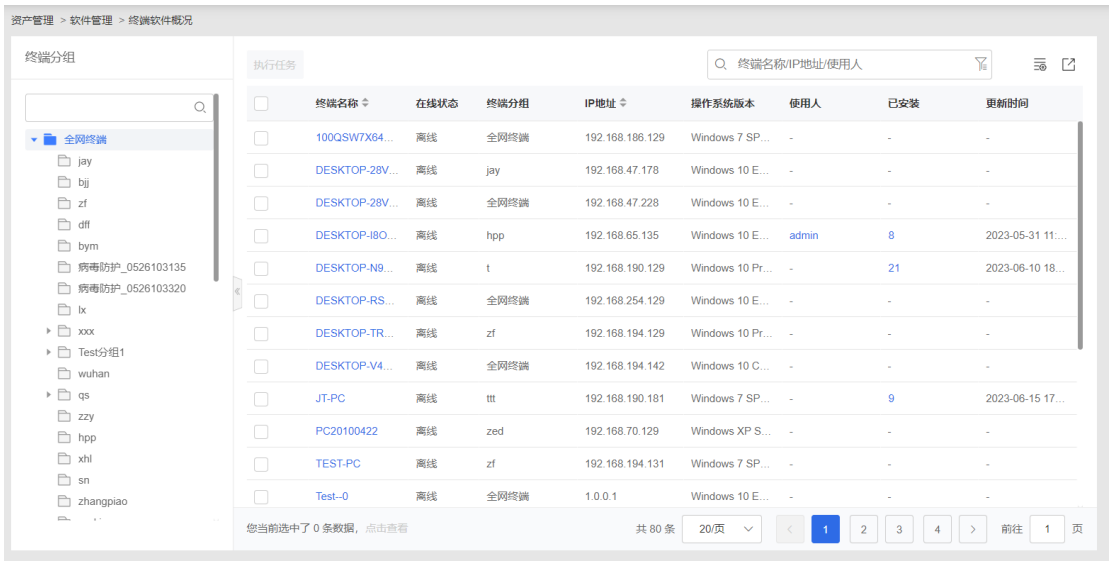




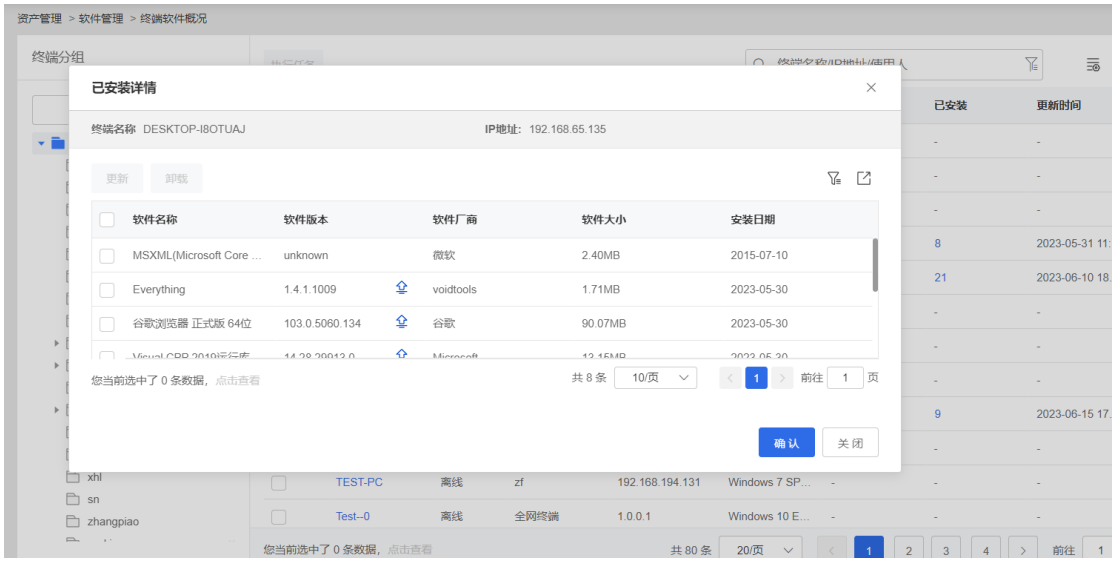
4.5. 终端软件概况

导航到“软件管理>终端软件安装”可从终端维度对软件的安装情况进行统计展示。支持按照不同的终端分组进行软件的统计。

按照终端分组、终端、已安装软件数量统计终端的软件安装情况，并可以批量导出指定范围终端的所有已安装软件列表。



也可对某一终端软件安装情况进行查看分析，详情如图所示。



4.6. 软件安装统计

导航到“软件管理>软件安装统计”可从软件维度对网内各分组的软件安装情况进行统计展示。支持按照不同的终端分组进行软件的统计查看。

按照终端分组、软件名称、是否授权等信息查看软件的安装情况，并可以批量导出指定范围软件的所有已安装终端列表。

在软件分析梳理过程中，支持选择软件并选择对应标签进行管理，标签可按管理场景需求进行自定义管理。

当发现非正版授权或其他违规软件的安装时，可直接对安装终端执行消息通知、更新或卸载等任务。

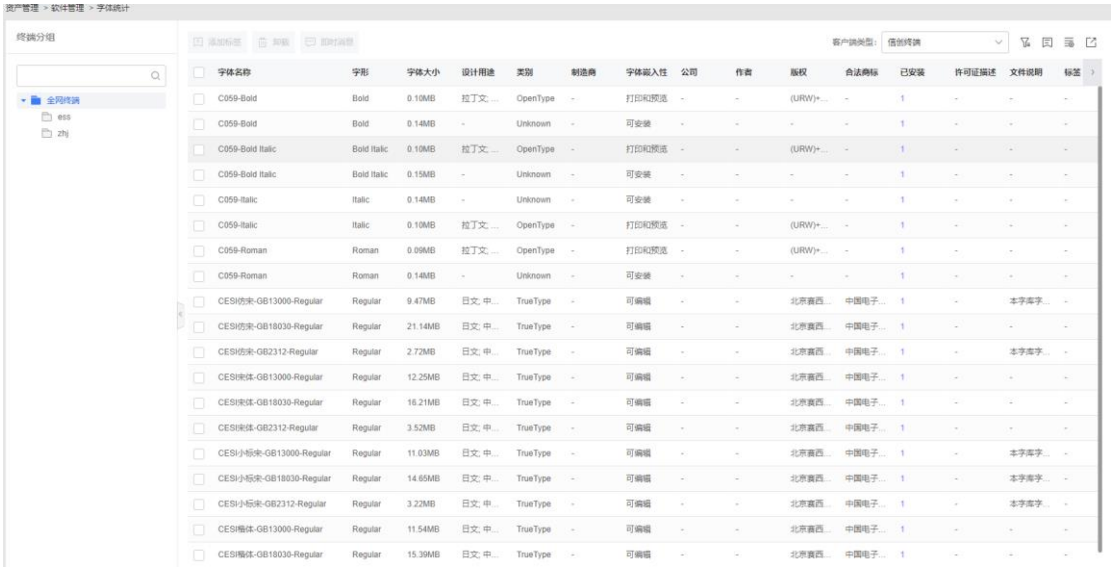
可在软件处置前，选择软件，对软件的使用进行任务统计，定期生成使用活跃度报表，可为软件的管理提供有效数据抓手。

也可对某款软件的安装版本及安装终端列表进行查看分析，详情如图所示。

4.7. 字体统计

导航到“软件管理>字体统计”可从字体维度对网内各分组的字体安装情况进行统计展示。支持按照不同的终端分组进行字体的统计查看。

按照终端分组、字体名称、大小、设计用途、公司等信息查看字体的安装情况，并可以批量导出指定范围字体的所有已安装终端列表。



当发现非正版授权或其他违规软件的安装时，可直接对安装终端执行消息通知、更新或卸载等任务。

也可对某款软件的安装版本及安装终端列表进行查看分析，详情如图所示。

4.8. 正版化管理

4.8.1. 添加统计规则

管理员可按需添加统计规则进行正版化软件的统计工作，许可证统计方式分为“安装数量”、“许可证数量”、“许可证”三种方式。

4.8.2. 正版化信息统计

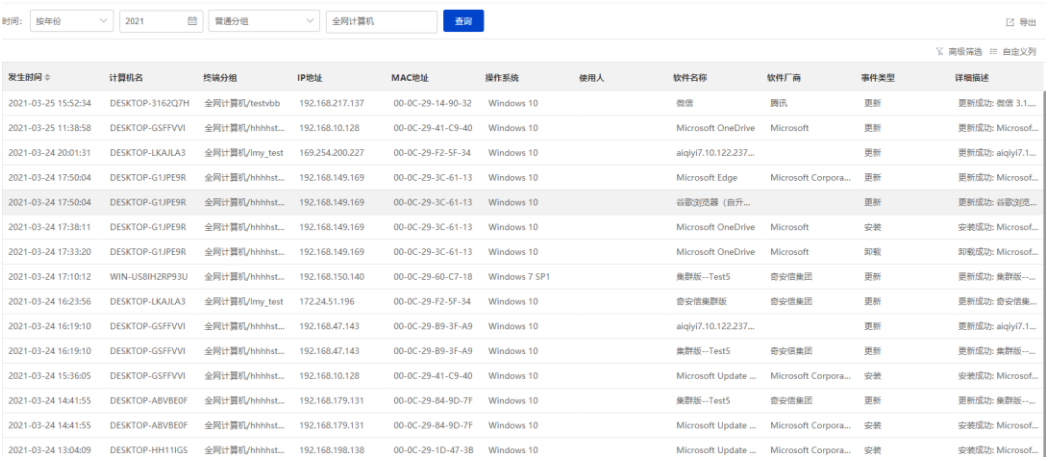
系统基于正版化统计规则定期生成统计结果，并支持管理员对统计结果进行筛选、数据下钻查看详情、导出等操作。

4.8.3. 软件活跃度统计

在正版化信息统计页面支持选择一款或多款软件进行“软件活跃度”统计。

4.9. 软件日志

软件日志可按照时间和分组两个不同的维度对终端软件的操作信息进行记录，事件类型包括，软件更新，安装，卸载。日志可以通过报表的形式导出。



4.10. 软件报表

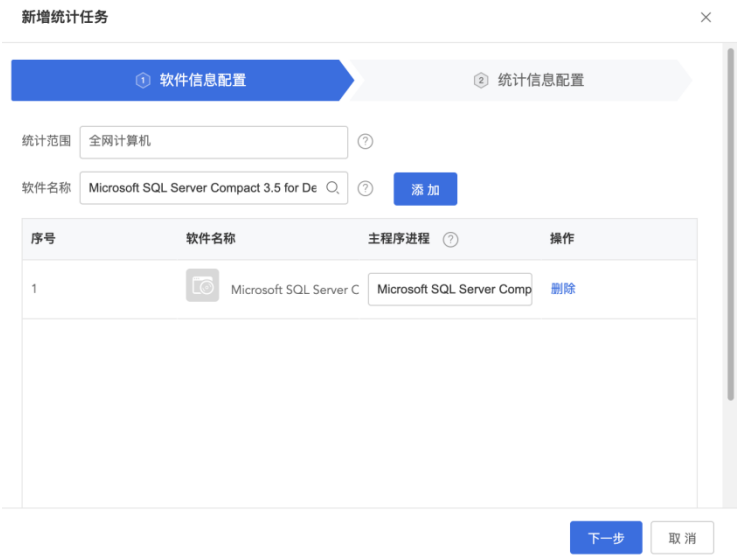
软件报表主要统计软件的变更趋势，软件安装卸载的趋势排行表。管理员可以分时间段查看报表，可按周，按月，按季度，按年来查询时间段内企业用户的软件下载情况等。

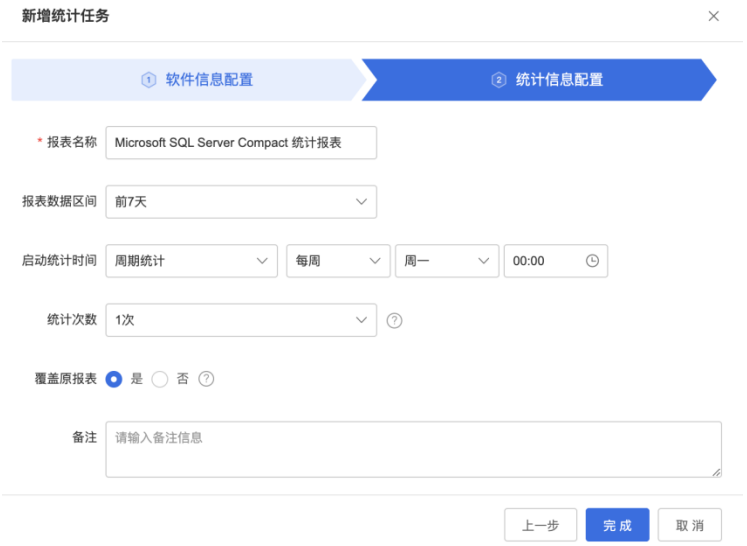
4.11. 活跃度统计

4.11.1. 添加计划报表任务

管理员按需配置报表任务，可“添加统计报表”、“删除统计报表”，“添加统计报表”分为两个步骤，在“软件信息配置”中配置统计范围和要统计的软

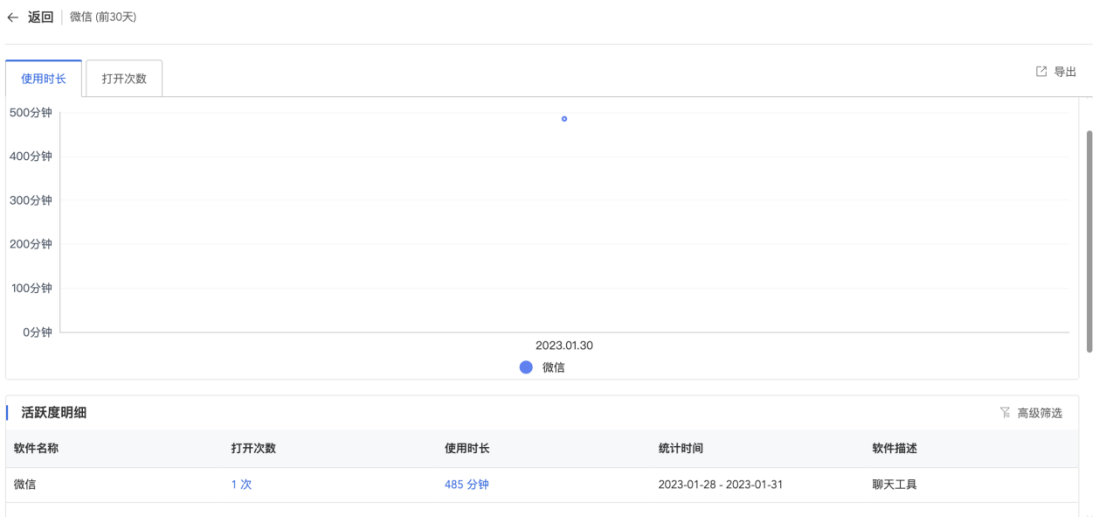
件，在“统计信息配置”中配置报表名称、报表数据区间、启动统计时间、统计次数、是否覆盖原报表等信息。配置完成后系统会按照计划任务生成对应的报表。



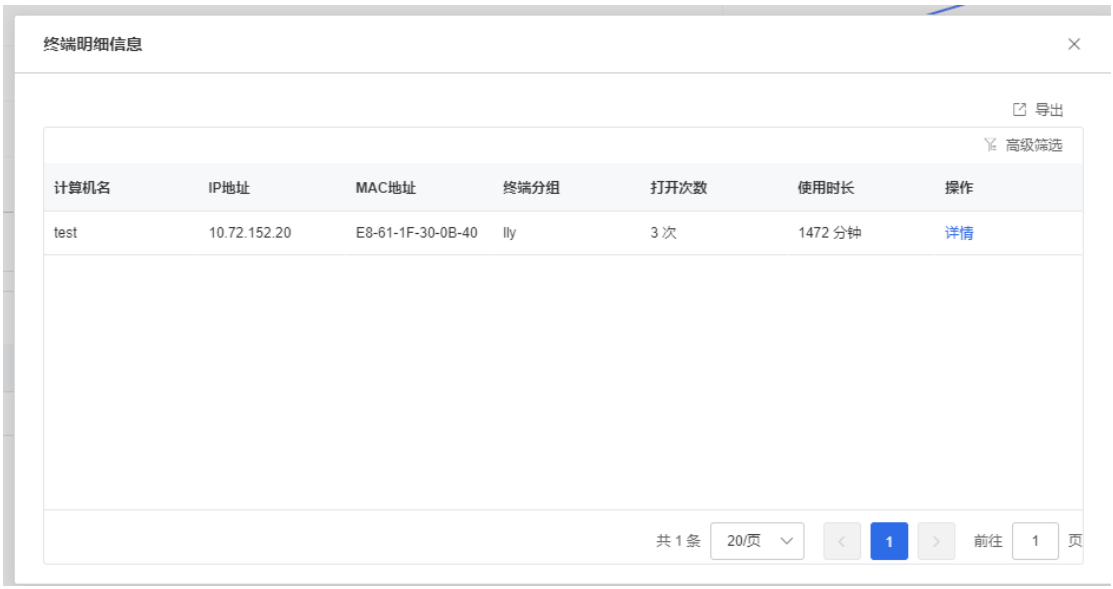


4.11.2. 统计报表

通过计划任务生成的报表在“统计报表”中体现，报表分为两部分，上半部分为“使用时长”、“打开次数”，下半部分为“活跃度明细”统计。



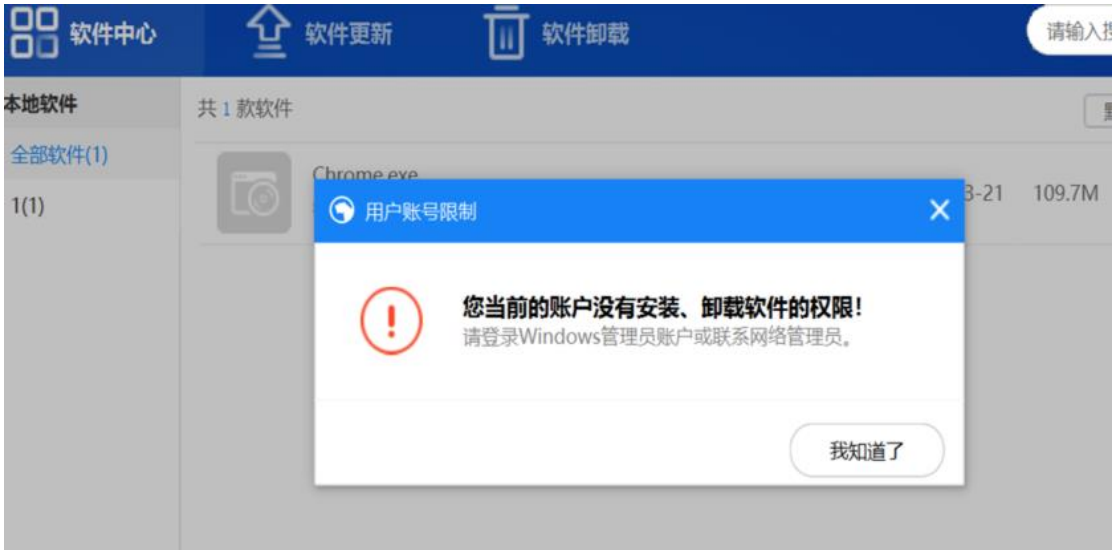
可对统计时间段内以终端维度对该款软件的使用情况进行统计及每条使用记录的详情查看分析。



4.12. 业务设置

1） 客户端软件管理

- 开启受限账户使用客户端软件管理：开启该配置，Windows 系统登录的受限账户可正常使用客户端的软件管理；如果关闭该配置，则受限账户没有权限使用客户端的软件管理。



- 开启软件管理中文输入：开启该配置，则管理员账户在客户端的软件管理-软件中心的搜索框可以使用中文输入法，否则管理员账户无法使用。

5. 病毒防护

5.1. 基本概念

5.1.1. 文件等级的定义

病毒防护功能把扫描的文件经过特征、行为分析后，其分析结果定义了不同级别，即文件等级。等级定义如下：

- 白

  本文提到的白文件、白进程都是指其等级为“白”级别，白级别是指安全无毒的等级。

- 未知

本文提到的未知文件、未知进程都是指其等级为“未知”级别，未知级别是指尚不确定是安全还是危险的等级。

- 黑

本文提到的黑文件、黑进程都是指其安全等级为“黑”级别，黑级别是指有风险的木马或病毒等级。

5.1.2. 病毒扫描

病毒扫描是终端执行病毒扫描操作，发现病毒并处理的一种防护机制。该功能主要用于当木马病毒进入系统后从未知变为已知时，可通过病毒扫描来彻底的查杀清除。病毒扫描包含快速扫描、全盘扫描、自定义扫描三种扫描方式。

- 快速扫描

扫描耗时短，有效扫描随系统自启动运行的风险文件。主要扫描系统常被利用的位置，包含启动项，顽固病毒，易感染区、系统设置、启动项、浏览器组件、系统服务、文件和内存、常用软件、系统综合、系统修复、任务计划等。

- 全盘扫描

全面扫描计算机，包含快速扫描内容以及所有硬盘文件，清理磁盘中木马病毒更彻底。

- 自定义扫描

按指定位置有选择性的扫描。

5.1.3. 信任区

信任区是终端加白的一种机制，当发现自己正常软件被误报为黑时，通过添加信任的操作避免文件被查杀。信任功能主要包括：

- 文件路径信任：按文件路径添加信任后，该路径不再被报黑。
- 文件指纹信任：按文件指纹添加信任后，则信任文件 hash 值，此 hash 的文件在任何位置都不会报黑。
- 文件扩展名信任：按文件扩展名添加信任后，符合该扩展名的所有文件都不再报黑。

5.1.4. 隔离区

隔离区是终端病毒文件被隔离后，本地备份保存的功能，此时病毒文件加密备份在系统硬盘上，可随时恢复回来。当在隔离区中执行删除操作后，该文件才彻底从硬盘上删掉。

5.1.5. 实时防护

实时防护是指终端实时地监控本地被创建/修改，文件只读等操作的文件，发现是病毒自动或手动查杀的一种防护机制。可以对文件的监控类型进行分别

设置，可以设置只监控程序和文档，也可以设置监控全部文件。同时对压缩包的实时防护也可以单独设置层数和大小。针对不同性能的终端做不同的针对性配置。

5.1.6. 主动防御

主动防御是指对进程的可疑行为进行拦截、阻止其继续操作的一种防护机制。该功能主要分为系统防护（包括：进程防护、注册表防护、驱动防护）、入口防护（包括：U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护）、系统加固（包括：勒索软件防护、Win7 加固/XP 加固）、网络防护（包括：远程登录防护、网络入侵防护、僵尸网络攻击防护、网络攻击防护、ARP 攻击防护）等。

- 进程防护

  进程防护实时监测活跃进程的各种系统行为(如进程创建、系统注入与挂钩等)，当判定为恶意行为时根据策略进行提示和拦截，实时保护系统免受各种系统恶意行为的侵害。

- 注册表防护

  注册表防护实时监测系统关键注册表的创建、修改和删除行为，当判定为恶意行为时根据策略进行提示和拦截，以阻止恶意程序试图开机启动、伴生启动或破坏系统的行为。

- 驱动防护

  驱动防护实时监测系统的驱动安装、加载、卸载等行为，当判定为恶意行为时根据策略进行提示和拦截，以阻止恶意程序试图躲避安全软件的检测、破坏安全软件或破坏系统的行为。

- 键盘记录防护

  键盘记录防护实时监测系统的键盘记录行为，当判定为恶意行为时根据策略进行提示和拦截。

- 系统账号防护

  实时检测和拦截恶意程序创建、修改系统账户的行为，发现恶意行为时进行提示和拦截。

- U 盘安全防护

  U 盘防护实时检测到系统接入 U 盘的行为，对 U 盘中关键位置的文件进行安全扫描，根据策略对发现的风险文件进行提示和清理，以保护系统免受 U 盘中恶意文件的入侵。

- 邮件防护

  恶意程序利用操作系统的漏洞，进行感染和传播而被阻断的防护。

- 下载防护

  下载防护对下载软件、浏览器下载的文件进行安全检测，根据策略对文件的风险进行提示和清理，防止从网络应用下载恶意程序。

- IM 防护

  IM 防护对即时通讯工具(IM)下载的文件进行安全检测，根据策略对文件的风险进行提示和清理，防止从 IM 下载恶意程序。

- 局域网文件防护

  局域网文件防护实时检测局域网网络共享文件的拷入、执行行为，当检测文件不安全时根据策略进行提示和拦截，防止从局域网共享目录下载恶意程序。

- 网页安全防护

  对浏览器中访问的 URL 和网页内容进行安全扫描，发现的风险进行提示和拦截。

- 勒索软件防护

  勒索软件防护实时检测未知风险程序的篡改文件和勒索病毒相关特征行为，阻止系统遭受勒索软件的加密等破坏行为。

- Win7/XP 加固

  Win7/XP 加固解决 Win7/XP 系统停服后的漏洞利用问题，为系统 RCE，浏览器、Office 应用等进行漏洞利用防护。

- 远程登录防护

  自动阻止远程登录行为，防止黑客远程爆破和拦截恶意的远程登录。

- 网络入侵防护

网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁。

- 僵尸网络攻击防护

  僵尸网络攻击防护对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。

- 网络攻击防护

  防护对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。

- ARP 攻击防护

  ARP 攻击防护根据策略检测和拦截局域网中的 ARP 欺骗攻击行为。

- DNS 防护

  检测和保护本机 DNS 的安全性，防止终端 DNS 和 HOSTS 被恶意篡改，该功能需要连公有云。

5.2. 病毒防护策略

病毒防护设置，位于管理中心>安全防护>病毒防护>策略管理，管理员根据企业自身的一些环境、业务等特点进行必要的防护策略设置。管理中心提供了通用的默认设置，但强烈建议企业管理员要根据自身的企业特点来调整策略，下面详细介绍各策略功能的意义。

5.2.1.通用设置

5.2.1.1. 检测引擎设置

该模块提供检测引擎的检出偏好、发现病毒处理方式、云查杀模式、各引擎的检出方式和适用防护范围等。

- 威胁检出偏好：通过设置检出偏好来设置对内网病毒的检出级别。默认为均衡型，同时还可以选择低误报、高检出。选择高检出的时候，能够最大化的检出病毒，但是同时可能误报的也会增加。选择低误报时候，会最大化降低误报，但是同时可能会增加漏报的可能性。建议选择均衡型。

- 云查模式：设置云查杀的连接模式，可以选择通过服务器代理云查，也可以选择直连公有云、直连私有云、隔离网不连云。在低配置服务器上（4C8G），云查模式不支持通过服务器代理云查。

通过服务器代理云查：客户端向管理中心发送云查请求；管理中心做缓存处理、转发到奇安信公有云或者私有云。这种方式节约网络出口带宽，但占用管理中心资源。

直连公有云：客户端直接向奇安信公有云发送云查请求。这种方式节约管理中心资源，但占用网络出口带宽。评估所需出口带宽请查阅管理员手册的对应章节。10.7.0.1000 开始，客户端直接发云查请求到公网；之前的版本是客户端发给管理中心，由管理中心转发到公网。

直连私有云：客户端直接向奇安信私有云管理系统发送云查请求。这种方式大幅提升隔离网中客户端的安全防护能力，需要部署奇安信私有云。

隔离网不连云：客户端关闭云查请求。这种方式仅依靠本地特征引擎拦截病毒，请管理员及时更新病毒特征库。

云查杀技术说明：

受限于电脑资源，本地病毒特征库不能无限扩大；而新病毒样本以指数级的速度增加、且快于病毒特征库的更新。为了解决杀毒软件被动处境，反病毒行业发展出云查杀技术。云查杀把电脑程序文件分为白、黑、灰（未知），任何新病毒样本会落在“未知”这个逻辑区域。云查杀结合主动防御可以有效拦截未知威胁。云查杀的优势：白的快、黑的全、灰的防得严。

- 终端无法连接管理中心设置：该选项是在云查杀模式选择“通过服务器代理云查”情况下，终端无法连接管理中心的时候，自动连接公有云鉴定中心。保障终端病毒扫描时候，安全防护能力不降低。

- 第一列：在引擎名称前面勾选该选项，表示开启该引擎。开启引擎后，左侧引擎相关设置才可以设置和启用。

- 第二、三列：属于引擎生效范围。启用引擎后，可以通过该选项对引擎的适用范围进行配置，可以配置分别对病毒扫描或实时防护及主动防御生效，也可以同时生效。
- 第四列：属于引擎误报时的应急处置。勾选后，所有该引擎的检出仅上报日志到管理中心，客户端不会对检出病毒进行处置动作。影响范围是病毒扫描、实时防护及主动防御中使用到该引擎的地方。

说明：QCE-云查杀引擎默认开启，生效范围默认是病毒扫描、实时防护及主动防御，无法修改。

【注意】仅上报不处理主要是为了初期部署通过该配置对内网终端的病毒检出情况进行“观察”。配置该模式后，所选的配置的引擎只上报日志，不处理终端的病毒。部署过程中通过该模式“观察”是否存在误报，如果无误报则可以将该配置取消勾选。防止忘记勾选导致病毒不处理的情况发生。

5.2.1.2. 未知文件鉴定

该功能可以设置开启和关闭未知文件鉴定功能。该功能的样本鉴定服务器为云查杀引擎设置鉴定服务相同。

- 功能开关：勾选“参加文件云安全计划，对未知的可执行程序进行云鉴定”代表开启该功能。
- 鉴定文件大小设置：开启功能后，可以对鉴定的文件大小进行配置，超出设置大小的文件将不进行鉴定。

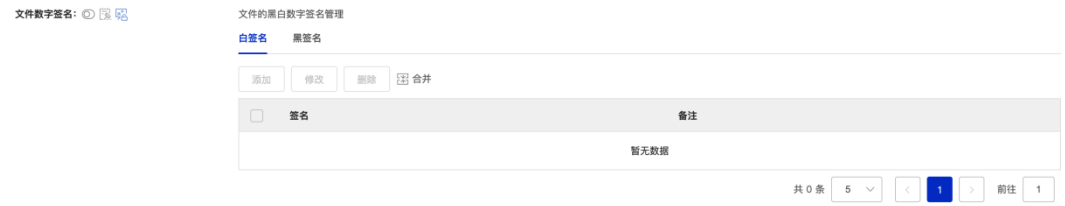
5.2.1.3. 信任区

支持添加文件、文件路径、扩展名信任。添加信任后，终端在实时防护和病毒扫描时，将忽略信任项，不进行病毒扫描。支持禁止终端添加路径/文件白名单以及扩展名白名单功能

5.2.1.4. 文件数字签名

支持将数字签名名称进行添加黑白名单。添加白签名之后，将在病毒扫描和实时防护时候忽略该数字签名的文件。添加黑签名之后，将在病毒扫描和实时防护时将该数据签名文件判为危险。

以上签名判断前提条件是签名有效，签名有效的定义是：有受信任 CA 证书机构颁发的签名证书。



【注意】黑签名检出病毒名为 Trojan.Generic.Sigature.Risk，如果通过病毒库日志发现该病毒名则表示添加签名生效。如果发现误报，则可以通过该页面进行修改。

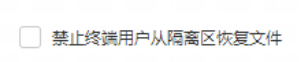
5.2.1.5. 隔离区设置

隔离区空间大小设置用来配置终端隔离区的大小。配置为“不限制”，则不限制客户端的隔离区空间大小。配置自定义大小后，终端在进行隔离区操作时，会判断当前大小和配置的大小，如果超出限制，则会将历史最早隔离的文件进行删除，以保障隔离区空间大小满足配置值。

在一些客户的环境中，终端不允许存在病毒文件，认为隔离文件也是病毒文件的一种。这种情况下，可以选择关闭隔离区，终端处理病毒文件时不再备份文件，直接删除病毒文件或者清理感染文件。

【注意】关闭隔离区后，客户端会清空隔离区中的数据，且无法恢复。请谨慎配置。

在一些客户的环境中，不允许终端从隔离区恢复、信任文件，实现统一管控白名单的效果。这种情况下，可以选择勾选：禁止终端用户从隔离区恢复文件。策略在客户端生效后，客户端的隔离区窗口左下角显示： 隔离区恢复功能被管理员禁用，恢复和恢复所选两个按钮被禁用。

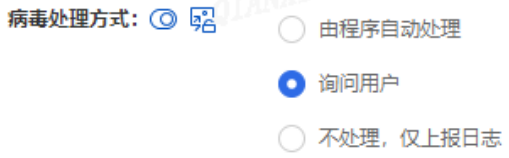


为了避免客户端上的隔离区数据一直占据磁盘空间，可以设置隔离区文件最大保留的天数。客户端每天定时检查隔离区文件，删除超期数据。

5.2.2.病毒扫描设置

5.2.2.1. 病毒处理方式

可以设置三种处理方式：由程序自动处理、询问用户和不处理仅上报日志。选择询问用户时，终端检出病毒会提示用户，由用户选择是否处理；选择程序自动处理时，终端检出病毒会自动清除；选择不处理仅上报日志，终端检出病毒后，不进行处理，直接将结果上报到管理中心。



【注意】仅上报不处理主要是为了初期部署通过该配置对内网终端的病毒检出情况进行“观察”。配置该模式后，所选的配置的功能只上报日志，不处理终端的病毒。部署过程中通过该模式“观察”是否存在误报，如果无误报则可以将该配置取消勾选。防止忘记勾选导致病毒不处理的情况发生。

5.2.2.2. 扫描对象设置

需要扫描的文件类型，支持设置扫描所有文件、仅扫描程序及文档文件。默认是仅扫描程序和文档文件。

- 程序：通常是指如 exe、dll、sys 类 Windows 系统的 PE 类文件，也包括脚本类文件，如：vbs、sh、php、js 等，同时还包括 Linux 的 elf 格式文件，macOS 中的 Mach-O，移动应用中的 apk、ipa、pxl、deb 等格式。
- 文档文件：通常是指常用办公软件的文件格式，如 doc、docx、xls、xlsx、ppt、pptx、rtf、pdf 等。以上格式判断均为根据文件的判断格式，而非根据后缀名。

扫描启动项中的网络共享路径选项为选择后，在扫描启动项时，有连接到网络共享路径的文件和地址，将进入到网络共享路径进行扫描。

全盘扫描时候扫描网络映射驱动器选项选择后，将在全盘扫描时候进入网络映射驱动器进行扫描。同时选择了终端以受限用户（没有管理员权限）登录时候不扫描网络映射驱动器（终端重启后生效），则不扫描对应区域，反之则扫描。如果不选择可能造成检测到病毒，因为权限关系无法清除的问题。

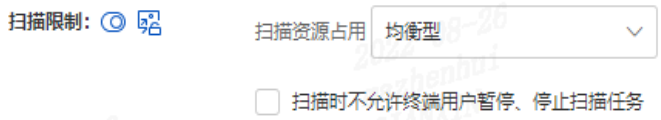
扫描压缩包设置，可以选择不扫描压缩包。如果选择了扫描压缩包，还可以设置扫描压缩包的层数和大小。压缩包的处理策略默认是扫描到病毒立即报出、不再继续扫描压缩包内的其他文件；勾选该项就是扫描完整压缩包。扫描完整压缩包受压缩包层数和大小的限制。

5.2.2.3. 扫描限制

该模块用来限制终端的某些特定功能，还支持是否允许终端暂停和停止扫描任务。扫描资源占用设置，支持设置终端病毒扫描时候的资源占用。支持配置不限制、均衡型、低资源。

- 不限制：是指终端进行病毒扫描时候，不限制 CPU 占用进行病毒扫描。实际 CPU 占用根据扫描的速度以及系统分配的可用 CPU 进行使用。
- 均衡型： 是指终端进行病毒扫描时候，终端会根据当前 CPU 的占用情况进行动态调配，以保证在 50%（平均值）以下。
- 低资源： 是指终端进行病毒扫描时候，终端会根据当前 CPU 的占用情况进行动态调配，CPU 占用保证在 30%（平均值）以下。

以上 CPU 占用值均为理想情况下的值，实际使用情况还需要根据系统可调配 CPU 资源而定。并且资源占用情况为动态值，实际扫描时的资源占用会存在一定的上下波动，跟文件的大小类型有关。



5.2.2.4. 深度查杀

终端扫描病毒发现感染型和顽固型病毒时是否自动进入深度查杀模式

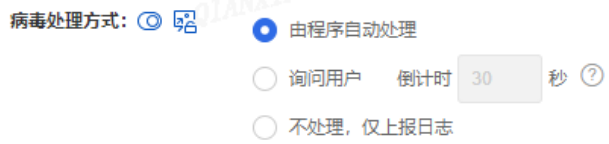
【注意】不勾选重启前弹框提示，遇到需要重启删除的病毒会直接重启而造成正在编辑未保存的用户数据丢失。建议勾选。

5.2.3. 实时防护

5.2.3.1. 病毒处理方式

可以设置三种处理方式：由程序自动处理、询问用户和不处理仅上报日志。选择询问用户时，终端检出病毒会提示用户，由用户选择是否处理；选择程序自

动处理时，终端检出病毒会自动清除；选择不处理仅上报日志，终端检出病毒后，不进行处理，直接将结果上报到管理中心。



【注意】仅上报不处理主要是为了初期部署通过该配置对内网终端的病毒检出情况进行“观察”。配置该模式后，所选的配置的功能只上报日志，不处理终端的病毒。部署过程中通过该模式“观察”是否存在误报，如果无误报则可以将该配置取消勾选。防止忘记勾选导致病毒不处理的情况发生。

5.2.3.2. 实时防护

实时防护设置可以用来开启关闭实时防护。同时考虑到不同的终端的开机速度，增加延迟开启的功能。

5.2.3.3. 防护文件类型

需要扫描的文件类型，支持设置扫描所有文件、仅扫描程序及文档文件。默认是仅扫描程序和文档文件。

扫描压缩包设置，可以选择不扫描压缩包，同时也可以选择扫描压缩包。如果选择了扫描压缩包，同时还可以设置扫描压缩包的层数和大小。

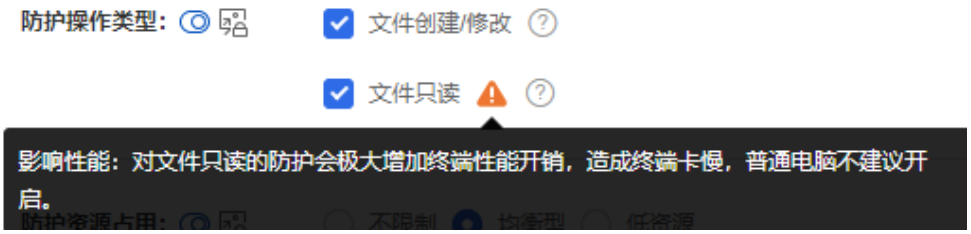
5.2.3.4. 防护操作类型

防护的操作类型包括文件的创建/修改和文件只读。

- 文件创建/修改：通常指在系统磁盘中创建和修改文件，例如保存一个新的文档称之为创建，如果修改了一个文档保存则称之为修改。
- 文件只读：是指系统中某个程序去访问系统的中的文件的行为，被称之为读取文件。例如用户打开文件目录，则是系统的资源管理器会读取该目录下的所有文件。

【注意】：勾选文件只读会极大增加性能开销，普通电脑不建议勾选；该方式仅适合经过特殊处理的终端杀毒（如适配华为 NAS 系统杀毒的服务器）。

继续勾选，会出现告警图标，如下图所示。



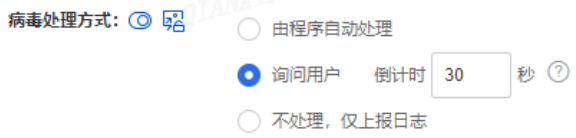
5.2.3.5. 防护资源占用

默认为均衡型。在低配置终端上，建议设置低资源。在共享文件服务器上，建议设置为不限制：当多个终端（未安装杀软）向服务器共享可写目录传播病毒文件时，可以快速查杀，不出现积压。

5.2.4.主动防御

5.2.4.1. 病毒处理方式

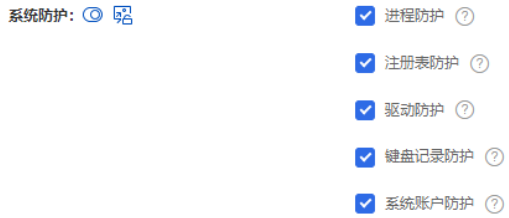
可以设置三种处理方式：由程序自动处理、询问用户和不处理仅上报日志。选择询问用户时，终端检出病毒会提示用户，由用户选择是否处理；选择程序自动处理时，终端检出病毒会自动清除；选择不处理仅上报日志，终端检出病毒后，不进行处理，直接将结果上报到管理中心。



【注意】仅上报不处理主要是为了初期部署通过该配置对内网终端的病毒检出情况进行“观察”。配置该模式后，所选的配置的功能只上报日志，不处理终端的病毒。部署过程中通过该模式“观察”是否存在误报，如果无误报则可以将该配置取消勾选。防止忘记勾选导致病毒不处理的情况发生。

5.2.4.2. 系统防护

系统防护是针对系统内的文件行为和动作进行防护。该防护下主要用来开启/关闭系统相关的防护功能和设置。系统防护功能包括：进程防护、注册表防护、驱动防护、键盘记录防护、系统账号防护。



5.2.4.3. 入口防护

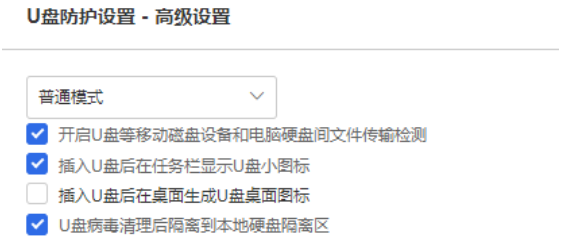
入口防护是针对终端可能从外界进入文件的环节进行防护。包括：U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护。

U 盘安全防护提供了防护模式选项，可以选择普通模式，智能模式，严格模式选项。支持 U 盘和电脑硬盘之间传输文件的检测配置以及是否在桌面或任务栏上生成图标进行配置。可以根据防护场景需求进行选择。

- U 盘：指可移动存储设备。接入终端后，可以在终端上生成可见磁盘的文件存储设备。包括 U 盘，移动硬盘，移动数码设备文件传输模式生成的磁盘等。

防护模式定义：

- 普通模式：插入 U 盘自动对 U 盘根目录进行扫描。U 盘根目录文件根据扫描策略进行全量扫描，如果根目录文件较多时，对 U 盘使用有一定的影响。
- 智能模式：根据 U 盘的内容进行分析，智能对可能出现病毒的文件进行扫描。
- 严格防护模式：插入 U 盘自动对 U 盘进行全盘扫描。该功能可能会对系统资源以及 U 盘使用效率有一定影响。



5.2.4.4. 系统加固

系统加固对系统可能被入侵的位置进行加固和拦截，从而抵挡系统被恶意入侵。系统加固包括：勒索软件防护、Win7/XP 加固。

勒索软件防护提供了增强和免疫功能设置，可以根据需要开启/关闭相关功能。勒索软件防护增强是根据勒索软件的行为特征在系统中关键位置生成诱饵文件用来监控勒索动作。勒索病毒免疫功能是针对勒索软件的行为动作进行免疫，从而达到让勒索病毒无法启动的效果。从而最大程度的拦截勒索病毒。

Win7/XP 加固是针对已经停服的微软系统进行系统增强防护的功能，增强系统的远程漏洞攻击防护、本地钓鱼攻击防护、浏览器漏洞攻击防护。同时还提供了针对该功能的拦截方式进行设置。

5.2.4.5. 网络防护

网络防护，是从网络层面对网络流量数据包进行监测，防止终端对外和对内进行攻击。网络防护包括；远程登录防护、网络入侵防护、僵尸网络攻击防护、网络攻击防护、ARP 攻击防护、DNS 防护。

远程登录防护功能为准入制防护，需要能够访问的终端双方都安装本系统终端应用。在发起请求时，通过双向验证，最大程度的保证访问请求的安全性。该功能还提供了全部禁止模式和白名单模式。白名单可以通过配置来选择需要加入

白名单的终端。考虑双向验证的机制，同时增加了逃生机制，当终端无法连接管理中心时，增加例外配置，以保障实际业务的正常。

- 全部禁止：是指禁止其他任何终端无法向该终端发起远程登录（RDP）请求。终端配置该选项后，其他任何终端向该终端发起远程登录请求均被拦截。
- 白名单模式：是指允许同管理中心策略中添加了白名单的终端、并且可以正常连接同管理中心的终端均可以向该终端发起远程登录（RDP）请求。未加入白名单和白名单中无法正常连接本管理中心的终端将无法请求。操作提示：如果希望终端 A 远程登陆到终端 B，需要把 A 添加到白名单中，且策略生效范围包含 B；同时 A 也要开启远程登录防护的功能。
- 终端脱管：是指管理中心下的终端，因为网络或其他原因无法正常访问管理中心的情况称之为脱管。

5.2.5. 定时查杀

5.2.5.1. 定时查杀

定时查杀是用来配置终端定时启动病毒查杀的功能。可以根据内网的安全防护制度来配置定时查杀任务。

为了满足不同企业或机构的安全基线需求，提供了配置按照每天、每周、每月指定时间来执行扫描动作，和配置扫描类型的功能。

部分企业会将扫描任务定在员工休息时段进行扫描，可能因为终端文件较多无法在一定的时间内完成扫描。提供了扫描时长限制以及断点续扫描功能，在规定的时间内无法完成扫描时，下次启动扫描任务继续上次任务进行扫描。统计数据显示：在非工作时间进行全盘扫描，终端用户取消扫描的比例减少 70%以上。

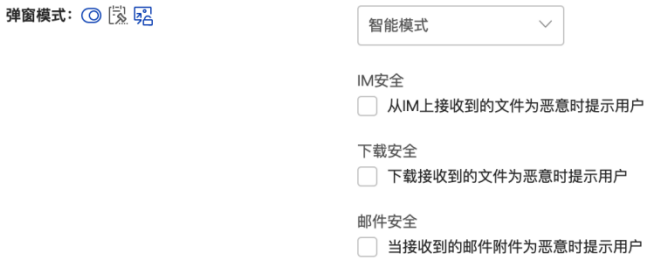
在定时任务执行时间点之后开机启动的终端，如果要求终端必须执行定时扫描任务，可以设置【错误扫描调度】中的时长，在该时间范围内，系统仍然会执行扫描计划。

【注意】全盘扫描会增加对管理中心或应用服务器的网络请求，如果内网终端较多且服务器资源相对紧张的情况下。则建议对不同的分组采取错开方式配置定时任务，防止在集中扫描时影响管理中心访问。

5.2.6.弹窗设置

5.2.6.1. 弹窗模式

弹窗设置主要对病毒防护功能的弹窗方式进行配置，另外邮件安全防护、IM安全防护、下载安全防护提示也提供单独的配置。可以根据需要进行选择。



- 智能模式：对于实时防护、主动防御的“由程序自动处理”，在处置病毒后，弹出通知窗口。。
- 免打扰模式：是在系统发现风险时候，按照默认操作进行自动操作，并记录日志。该模式的优先级高于“询问用户”这种病击处理方式。

5.2.7. 高级威胁防御

高级威胁防御 Tab 页面，包含无文件攻击防护、文档攻击防护、横移渗透攻击防护、和内存攻击防护。支持 Windows PC 和 Windows Server 两种终端类型。该功能在防御钓鱼邮件、伪装软件、爆破攻击、横向渗透等新式木马方面表现优异，但需要开通单独的授权模块。

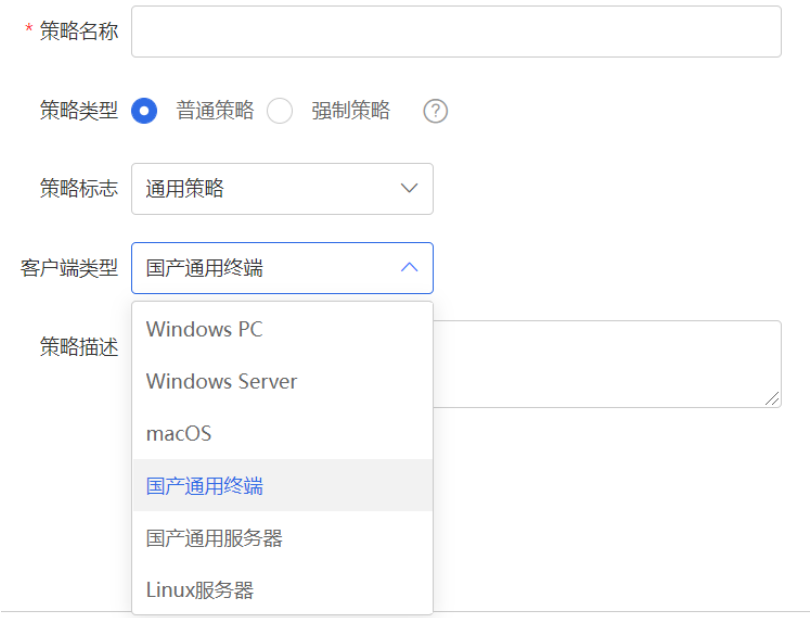
策略项	功能说明
无文件攻击防护	针对 Powershell、VBS、JS 等脚本化攻击场景，对 WMI 在内存执行行为进行监控。
文档攻击防护	针对 Office 执行 VBA 宏代码、远程模版执行、DDE、内嵌对象执行、Excel 4.0 宏等攻击行为的监测。
横移渗透攻击防护	针对内网横向移动渗透攻击进行防护，可以有效的防护阻断高危蠕虫病毒传播扩散以及减少勒索、挖矿等风险的发生。
内存攻击防护	针对可疑程序启动内存威胁攻击行为检测。

【注意】高级威胁防御不受病毒防护策略>通用设置>检测引擎设置的约束；高级威胁防御采用主动防御的病毒处理方式设置。

5.2.8.信创终端病毒防护策略

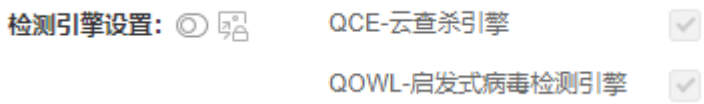
功能说明：设置Linux服务器终端、信创终端、信创服务器终端的病毒防护策略。包含：通用设置、病毒扫描、实时防护、主动防御、定时查杀。

功能入口：管理中心>安全防护>病毒防护>策略管理>客户端类型（选择Linux服务器终端、信创终端、信创服务器终端）。



1)通用设置，包含检测引擎设置（支持QCE引擎、QOWL引擎）、信任区、隔离区设置。

推荐的引擎设置如下图：



2）云查杀设置，默认云查模式为【直连公有云】

3）加信任区请参考提示信息：

4）病毒扫描，包含扫描对象、终端限制。扫描对象建议保持默认值。

5） 实时防护包含实时防护、防护文件类型。

6） 主动防御包含系统防护、入口防护、网络防护。

系统防护支持进程防护、驱动防护和系统账号防护。

入口防御的U盘防护高级设置仅有普通和严格两种模式。普通模式：仅扫描U盘根目录下的文件，不处理子目录；严格模式：对于U盘进行全盘扫描。

网络防护支持拦截爆破攻击

7） 定时查杀支持周期执行，不支持开机执行。

说明：支持断点续扫描的版本为 10.7.0.1720。

【注意】全盘扫描会增加对管理中心或应用服务器的网络请求，如果内网终端较多且服务器资源相对紧张的情况下。则建议对不同的分组采取错开方式配置定时任务，防止在集中扫描时影响管理中心访问。

5.2.9. macOS 终端病毒防护策略

功能说明：设置 macOS 终端的病毒防护策略。包含：通用设置、病毒扫描、定时查杀

功能入口：安全防护>病毒防护>策略管理>客户端类型（选择 macOS）

1）通用设置，包含检测引擎设置（支持 QCE 引擎、QOWL 引擎）、信任区、隔离区设置。推荐的引擎设置如下图：

2）添加信任区请参考提示信息：

3）隔离区-自定义，支持设置隔离区空间大小

4）病毒扫描，包含扫描对象、扫描压缩文件设置、终端限制。扫描对象建议保持默认值。

5）定时查杀，支持断点续扫描，支持周期执行，不支持开机执行。

【注意】全盘扫描会增加对管理中心或应用服务器的网络请求，如果内网终端较多且服务器资源相对紧张的情况下。则建议对不同的分组采取错开方式配置定时任务，防止在集中扫描时影响管理中心访问。

5.3. 终端任务

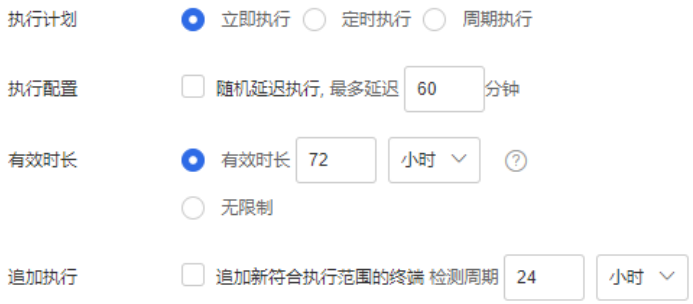
进入管理中心>终端管理>终端任务界面，通过新建任务来创建病毒防护业务任务，任务支持：全盘扫描、快速扫描、强力查杀、文件专杀、隔离区恢复等任务。并对扫描结果进行分析和处理，是保障内网安全的基础。

5.3.1. 全盘扫描

进入管理中心>终端管理>终端任务界面，创建任务，业务类型选择病毒防护，任务类型选择全盘扫描。再根据需要选择终端类型。

点击下一步选择需要下发任务的分组。

点击下一步选择开始执行的时间和结束执行的时间。



点击下一步，即完成任务的分发。终端执行时间内接收到任务后，将在任务有效期内开始扫描任务。

【注意】全盘扫描会增加对管理中心或应用服务器的网络请求，如果内网终端较多且服务器资源相对紧张的情况下。则建议对不同的分组采取错开方式配置扫描同时开启随机延时执行，防止在集中扫描时影响管理中心访问。

5.3.2.快速扫描

进入管理中心>终端管理>终端任务界面，创建任务，业务类型选择病毒防护，任务类型选择快速扫描。再根据需要选择终端类型。

5.3.3.强力查杀

强力查杀是为了解决终端可能存在病毒问题，可以通过强力查杀配置比较严格的策略来将病毒清理干净。根据售后统计，80%的无法查杀事件的根因是病毒被加入白名单、信任区。

进入管理中心-终端管理-终端任务界面，创建任务，业务类型选择病毒防护，任务类型选择强力查杀。在选择强力查杀后，会展示查杀策略，可以自定义终端扫描的策略，同时还支持忽略终端信任区进行扫描。

支持查杀 Rootkit 驱动木马。RootKit 病毒是一种高级病毒，它通过加载特殊的驱动、修改系统内核来隐藏自身。这类病毒通过奇安信的顽固木马专杀工具可以查杀，处理时会加载特殊文件进行驱动层的对抗。为了提高多台终端的查杀效率，同时保持稳定性，把该功能放到到强力查杀任务中。可以查杀 mlxg、紫狐、贪狼等带驱动保护的木马。

【注意】强力查杀会增加对管理中心或应用服务器的网络请求，如果内网终端较多且服务器资源相对紧张的情况下。则建议对不同的分组采取错开方式配置任务扫描同时开启随机延时执行，防止在集中扫描时影响管理中心访问。

【注意】扫描 Rootkit 驱动木马有蓝屏风险，建议对不同分组分批进行该项扫描，避免同时产生大面积系统故障。

5.3.4. 文件专杀

有针对性的对特定威胁进行专杀处理，支持对专杀任务的备注及任务有效期的设置。专杀工具可以从奇安信集团获取，针对特定的病毒问题，奇安信集团将发布对应的专杀工具，如有需要，参考界面提示联系售后支持。

进入管理中心-终端管理-终端任务界面，创建任务，业务类型选择病毒防护，任务类型选择文件专杀。在选择文件专杀后，会展示文件专杀上传和说明，可以根据需要填写相关信息。完成专杀工具配置后再根据需要选择终端类型。

5.3.5. 隔离区恢复

为了防止文件发生文件被误报进入隔离区的问题，提供了隔离区批量恢复的功能。可以在指定时间段下，指定的文件或路径以及病毒名进行批量恢复。

进入管理中心>终端管理>终端任务界面，创建任务，业务类型选择病毒防护，任务类型选择隔离区恢复。在选择隔离区恢复后，会展示需要恢复的时间段、文件名或路径、病毒名。完成配置后再根据需要选择终端类型。

5.3.6. 查杀未处理

快速处置终端上的未处理病毒，含未处理、处理失败、仅上报不处理（详见病毒查杀日志>处理结果）。此任务不会进行额外磁盘扫描。在部署阶段和【仅上报不处理】配合使用。

5.4. 业务管理

通过“管理中心>安全业务>病毒防护”可以查看病毒防护业务相关的概况、日志、报表、黑白名单等功能。

5.4.1. 病毒概况

病毒概况用来展示全网终端（也可指定分组）病毒发现和处理的情况以及病毒库版本、引擎启用情况。根据不同的时间和不同的分组为查询条件，以帮助管理员了解终端的安全现状。同时该页面还提供了下发病毒防护任务的快捷入口（任务使用方法详见终端任务）。如下图所示：

未处理病毒数：所选终端分组中的终端上未处理病毒个数的总和。

共发现病毒数：所选终端分组中的终端上检出的病毒次数总和。

未处理病毒是当前客户端上真实未处理的病毒文件个数（历史版本说明：在 10.3.0.5000 之前，未处理病毒数是最后一次扫描检出结果的未处理病毒数）。在客户端上，由三种处理结果会计入未处理病毒：未处理、处理失败、仅上报不处理。

未处理病毒的计算方法详细说明：假设都是相同的 200 个病毒文件，第一次扫描检出后未处理，第二次扫描后未处理，第三次扫描后全部处理。那病毒概况中第一次展示未处理是 200；第二次展示未处理仍然是 200；第三次未处理数是 0。在病毒查杀日志中，共 600 条记录；在查杀任务日志数据中，共 3 条记录，每条日志的未处理威胁依次为 200、200、0。

操作技巧：①点击未处理病毒数 ② 选择相同客户端类型的终端或者目标终端 ③点击按钮 【查杀未处理】。

未更新病毒库终端：所选终端分组中的终端上最后更新时间超过 7 天的终端数。

未开启文件防护终端：所选终端分组中的终端上未开启文件防护的终端数。文件实时防护是病毒防护的第一道防线，根据挖矿木马的统计数据，该功能贡献了 70%的拦截。

未执行全盘扫描终端：所选终端分组中的终端上在 30 天内未执行全盘扫描的终端数总和。

筛选：可以按照病毒库版本、杀毒引擎版本、最后查杀时间、最后全盘扫描时间、最后执行任务时间、最后执行计划时间来筛选目标终端。

5.4.2.病毒日志

病毒日志是全网终端（也可指定分组）病毒防护相关的日志展示，展示日志包括：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、网页安全防护日志。同时该日志支持按照指定时间、分组进行查询。同时支持高级筛选和导出等功能。

导出有五种方式 PDF、图片、CSV、EXCEL、混合导出。前两种（PDF、图片）只会导出当前页面数据，不会导出全部页面数据；CSV、EXCEL 导出的是全部数据；混合导出支持设置各个日志的导出类型。

【注意】日常运维中对文件添加了黑签名或黑名单的情况下，可以通过该页面观察是否有误报的情况，如查看文件检出目录是否有关键应用目录中的文件、或内网常用软件的文件等。

5.4.2.1. 病毒查杀日志

病毒查杀日志是指终端发现病毒事件的日志，支持展示发现终端信息、病毒文件相关信息：病毒类型、病毒名称、文件路径、文件创建时间、MD5、SHA1、发现病毒引擎、触发方式、处理结果、是否需要重启、任务名称、定时计划名称等信息。

5.4.2.2. 查杀任务日志

查杀任务日志是终端发起的扫描任务的结果的展示。展示扫描终端的信息，任务相关信息：任务触发方式、扫描类型、扫描用时、扫描引擎、扫描文件数、发现威胁数、清除威胁数、扫描结果、操作、任务名称、定时计划名称等信息。

5.4.2.3. 攻击防护日志

攻击防护日志是开启 Win7/XP 加固防护功能发现的威胁结果的展示。展示扫描终端的信息，攻击防护相关信息：事件类型、触发方式、攻击类型、攻击对象、攻击目标、攻击指令、处理结果等信息。

5.4.2.4. 系统防护日志

系统防护日志是主动防御功能（除网页安全防护、Win7/XP 加固防护以外的功能）发现威胁结果的展示。展示扫描终端的信息，系统防护相关信息：触发方式、主体、客体、风险文件、MD5、SHA1、风险描述、事件次数、行为、防护动作等信息。

5.4.2.5. 网页安全防护日志

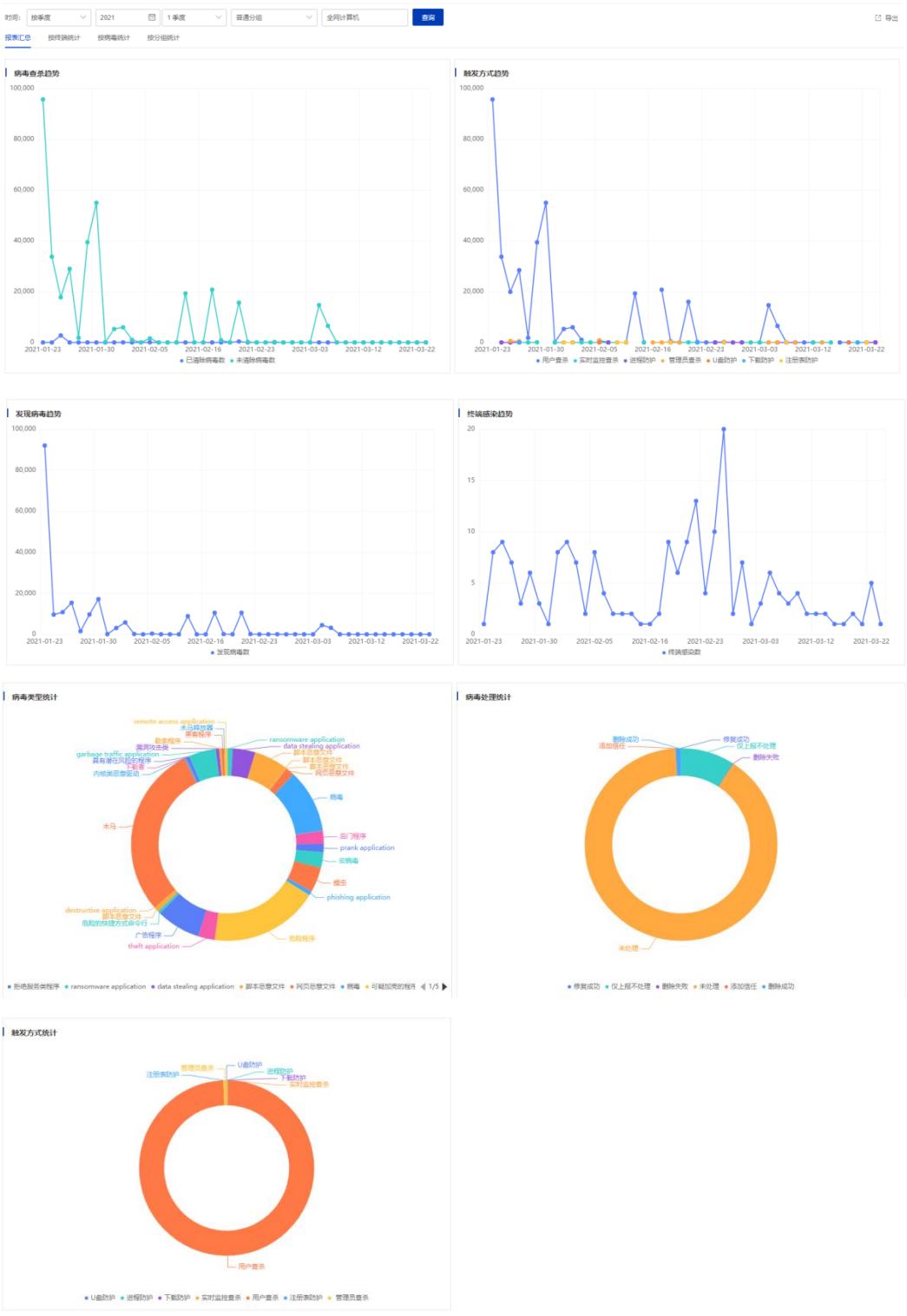
网页安全防护日志是网页安全防护功能的发现威胁结果展示。展示扫描终端的信息，网页安全防护相关信息：访问的 IP、访问的域名、防护动作、防护详情等信息。

5.4.3. 病毒报表

病毒报表是用来展示全网终端（也可指定分组）病毒防护相关的报表统计展示，展示报表包括：报表汇总、按终端统计、按病毒统计。通过分析报表中的相关趋势及时掌握内网终端的病毒风险以及威胁情况。

5.4.3.1. 报表汇总

报表汇总中提供了整体的病毒相关的统计以及趋势分析情况，包括：病毒查杀趋势、触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理统计、触发方式统计，感染病毒最多终端 TOP10 等数据，传播最多病毒库数 TOP10。


病毒查杀趋势
触发方式趋势
发现病毒趋势
终端感染趋势
病毒类型统计
病毒处理统计
触发方式统计

感染病毒最多终端TOP10

序号	计算机名	终端分组	IP地址	MAC地址	使用人	查杀次数
1		全网计算机	172.24.83.92	1C-69-7A-20-BA-BC		144531
2		全网计算机	172.24.83.28	A0-48-1C-9D-E4-AD		102644
3		全网计算机	172.24.83.93	1C-69-7A-20-BA-BC		21106
4		全网计算机	10.41.0.103	00-50-56-8E-59-4A		20756
5		全网计算机	172.24.83.96	6C-4B-90-40-9E-FB		19564
6		全网计算机	10.41.0.103	00-50-56-8E-59-4A		16039
7		全网计算机	10.41.0.103	00-50-56-8E-59-4A		13392
8		全网计算机	172.24.83.96	30-9C-23-2E-8C-0F		10547
9		全网计算机	192.168.188.132	00-0C-29-AA-7F-4A		4599
10		全网计算机	10.41.0.103	00-50-56-8E-59-4A		4015

传播最多病毒数TOP10

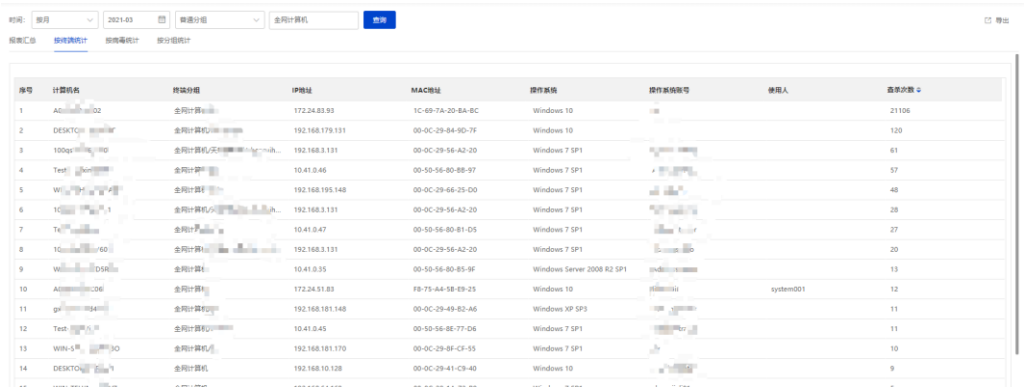
序号	病毒名	病毒类型	感染终端数
1	PUA.Signature.Risk	危险程序	20
2	Trojan.Win.Agent.d7c0fd1d	木马	20
3	Risk/CRS.Autorun.Generic	危险程序	19
4	Trojan.Generic	木马	16
5	QDE.v1.0.1LAA2CXP13.18YBZ	木马	14
6	Backdoor.Win32.Wabot.B	后门程序	14
7	Win32/Trojan.4cb	木马	14
8	Virus.Win32.Viking.Q	病毒	14
9	QDE.v1.0.SN5I94DZHQ.2HWMN	木马	13
10	QDE.v1.0.1LA9SKNMNK.8F	木马	11

受感染最多分组TOP10

序号	终端分组	感染终端数	查杀次数
2	全网计算机(本级)	24	292
3	gx	9	21212
4		5	161
5	hhhhstest	3	92

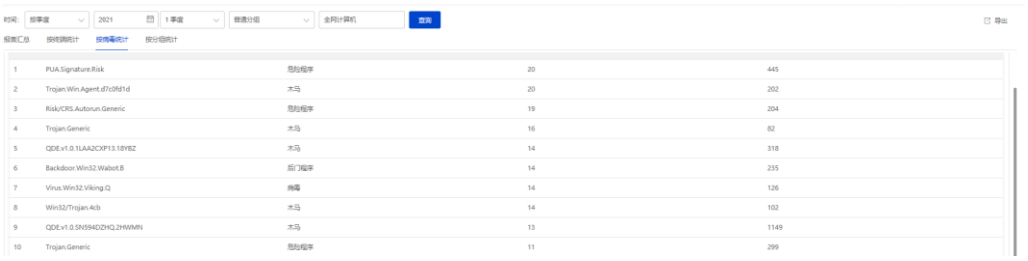
5.4.3.2. 按终端统计

该功能提供按终端统计病毒的查杀次数情况，可以通过筛选排序等方式来找出内网中风险较高的终端，进行处置。



5.4.3.3. 按病毒统计

该功能提供根据病毒统计终端感染情况和查杀次数，通过筛选排序功能，可以快速定位出内网感染病毒的范围和影响情况，通过分析做出处理决策。



5.4.4. 扫描分析

该功能对指定时间范围内发生的病毒扫描进行汇总分析，包括：管理员扫描任务，管理员定时扫描策略，用户扫描和第三方联动的扫描。默认选择最近 7 天扫描结果。

5.4.4.1. 扫描列表

按照扫描任务名称、策略中定时计划名称来展示列表。用户扫描默认置顶，是终端用户自己发起的扫描结果；周期执行的任务按照批次分开展示，任务名称末尾的序号表示执行批次；相同名称的定时扫描计划的结果会汇集在一起，即使他们不在一个策略中。

5.4.4.2. 列表详情

扫描结果详情，包含三部分：扫描概况、扫描终端分析、扫描结果分析。扫描概况展示名称、扫描来源和扫描类型，内容与扫描列表中的数据对应。

扫描终端分析，从终端的维度来评估扫描完成情况。有终端完成结果分布、检出威胁终端数、执行扫描终端数、检出威胁率（分子：检出威胁终端数；分母：执行扫描终端数）、终端扫描趋势、发现威胁终端 TOP10、扫描最快终端 TOP10、扫描最慢终端 TOP10、扫描文件最多终端 TOP10。

扫描结果分析，从十一个维度来评估病毒检出结果。有病毒检出和处置趋势、处理结果（需要关注仅上报未处理、未处理、删除失败、添加信任是否符合管理员预期）、引擎统计（需要关注云查杀引擎是否生效）、病毒类型 TOP10、终端分组 TOP10、病毒名称 TOP10、病毒文件 TOP10（点击文件，展示其检出趋势）、病毒路径 TOP10、勒索程序 TOP10、挖矿木马 TOP10、WebShell 木马 TOP10。

这些内容回答了六个病毒问题：终端是否有毒、报毒的终端主要是谁、病毒是否已妥善处理、网内主要是什么病毒、有无重点病毒、各个杀毒引擎在第三道防线是否有产出。

5.4.5. 主防分析

与扫描分析相比，主防分析是动态拦截数据的汇总，对第一道防线、第二道防线的病毒检出数据进行分析，包括：实时防护分析、主动防御分析。支持按照最近 1 天、最近 7 天、最近 30 天查看，默认选择最近 7 天。

5.4.5.1. 实时防护分析

实时防护是病毒防护的第一道防线。以 Viking 全盘感染型病毒数据为例，77%的拦截来自实时防护。

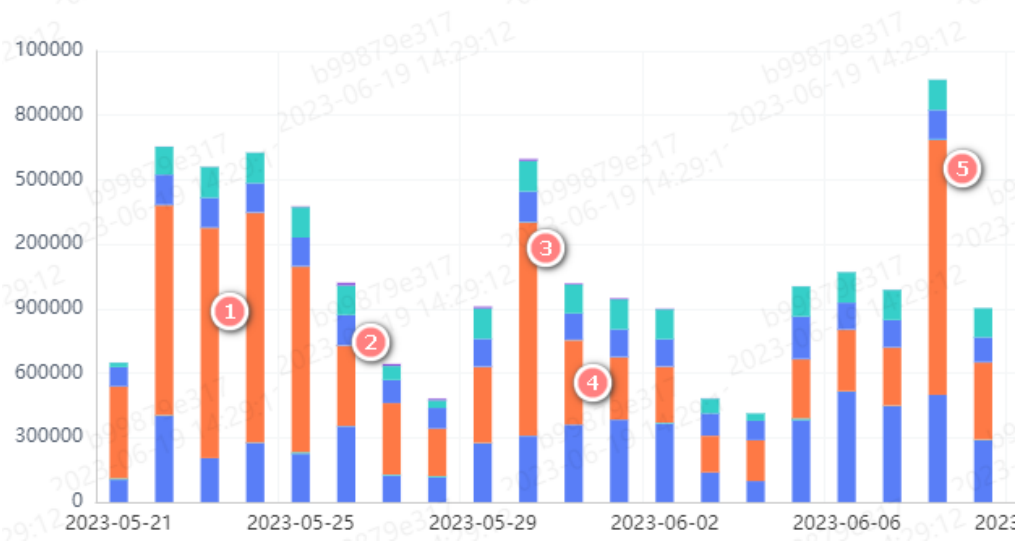
该报表包含 13 项内容：实时防护概况、实时防护趋势、处理结果分布、处理结果趋势、检出引擎分布、病毒类型 TOP10、检出终端 TOP10、病毒名称 TOP10、病毒文件 TOP10 、 病毒路径 TOP10、勒索程序 TOP10、 挖矿木马 TOP10 、 WebShell 木马 TOP10。

这些内容回答了六个病毒问题：终端是否有活跃病毒、中毒的终端主要是谁、病毒是否已妥善处理、网内主要是什么病毒、有无热点病毒、各个杀毒引擎在第一道防线是否有产出。

5.4.5.2. 主动防御分析

主动防御是病毒防护的第二道防线。主动防御趋势提供了该防线 18 种防护的拦截趋势。目前提供了五种防护类型详细报表：进程防护、驱动防护、勒索软件防护、网络入侵防护、僵尸网络攻击防护。另外，高级威胁防护的拦截结果也体现在主防防御趋势中。

主动防御趋势：用来判断增加、减少的检出来自哪个防护类型。



如上图所示，假如橙色代表网络入侵防护，可以看出几个关键信息：

①主动防御检出量持续高位位，最多是网络入侵防护， 需要管理员针对蠕虫采取措施；

②网络入侵防护检出量显著下降，说明管理员措施有效；

③网络入侵防护检出量激增，说明病毒在上次并未处理干净，需要继续治理；

④网络入侵防护检出量显著下降，说明管理员措施有效；

⑤网络入侵防护检出量再次激增，说明病毒源并未根除，需要深度治理。

五类防护深入分析说明如下：

【进程防护】通过进程防护-进程文件 TOP10 明确重点可疑程序。

【驱动防护】通过驱动防护-驱动文件 TOP10 明确重点可疑驱动。

【勒索软件防护】通过勒索软件防护-进程文件 TOP10 明确重点可疑程序。

【网络入侵防护】攻击源地址是发起攻击的 IP。通过客户端安装情况来判断应对措施：① 未安装天擎客户端-安装天擎客户端；② 已安装天擎客户端，且首次安装时间在攻击之前-排查策略设置是否有误，客户端天擎进程是否存在；③ 已安装天擎客户端，但安装时间在攻击之后-非产品问题。

【僵尸网络攻击防护】通过僵尸网络攻击-进程文件 TOP10 明确重点可疑程序。

5.4.6. 黑白名单

该功能提供运维人员在做安全运维时，需要全网添加信任或拦截的文件的功能。提供人工手动输入、名单导入、文件导入功能。该功能添加后，将对全网生效。

- 白名单：是指添加白名单后，终端对病毒扫描或者主动防御防护时，会忽略引擎的检测结果，直接将添加的名单文件直接判断为安全并放行。
- 黑名单：是指添加黑名单后，终端对病毒扫描或者主动防御防护时，会忽略引擎的检测结果，直接将添加的名单文件直接判断为危险并拦截。
- 一键鉴定：把云端检测结果反馈给管理员做对比参考。该功能针对当前页面的全部内容进行鉴定，和下方的复选框无关。
- 黑白名单会被下沉到终端，防止终端在漫游、断网或者网络异常状态时产生黑白名单失效问题。

【注意】黑白名单操作属于高风险操作，并且配置后会全局生效，如果添加错误可能导致整个内网内相关文件均被拦截。黑名单检出病毒名为：Trojan.Generic.BL 。添加黑名单后，可以通过病毒日志查看该病毒名的检出情况判断是否存在误报。为了避免出现误报事件，建议如下：

1、建议如果有添加黑名单的需求，并且非常确定为黑文件可自行添加到黑名单，涉及不确定的黑文件提交奇安信分析确认后通过奇安信病毒库下发拦截。

2、如果涉及添加黑名单文件较多的情况，则建议通过将云查杀引擎设置为仅上报不处理，然后添加黑名单之后，通过“观察”病毒日志查看病毒名为：Trojan.Generic.BL 的检出结果，是否存在误报情况，确定无误报之后，再将云查杀引擎仅上报不处理取消勾选。

5.5. 日常运维管理

5.5.1.提升和保持终端部署率

高终端部署率是企业内网安全的基本保障，如果终端没有部署客户端，一切安全策略都无法落地。可以参考终端部署章节内容，定期关注部署率相关数据并努力提高部署率。

5.5.2.通过定期扫描提升内网安全

定期对内网终端进行病毒扫描，可以提高内网的安全等级。我们推荐每周进行一次快速扫描，一个月至少进行一次全盘扫描。可以设置定时杀毒任务来自动进行病毒扫描。

5.5.3.更新病毒库

定期更新内网终端的病毒库，可以提升对新病毒的防御能力。我们在日常安全运营中，会保障每天发布病毒库，并且在病毒大规模爆发时可能会一天多

次更新病毒库。建议将病毒库更新设置为自动（或按照一定的批次自动更新）。设置方式参考更新管理相关章节。

【注意】库文件和程序文件文件在奇安信内部有严格的出厂测试检验程序，检测合格后才能发布。由于每个客户的场景有所不同，不排除可能会出现误报或兼容性问题。建议在管理中心-系统设置-更新管理中，对病毒库更新设置灰度发布版本。

5.5.4. 更新杀毒引擎

定期更新内网客户端杀毒引擎版本，我们在响应病毒处理能力时，根据需要也会通过更新客户端杀毒引擎来提升病毒防护能力，定期或及时更新客户端程序对病毒的防护能力提升有一定的帮助。建议将客户端杀毒引擎更新设置为自动（或按照一定的批次自动更新）。设置方式参考更新管理相关章节。

【注意】库文件和程序文件文件在奇安信内部有严格的出厂测试检验程序，检测合格后才能发布。由于每个客户的场景有所不同，不排除可能会出现误报或兼容性问题。建议在管理中心-系统设置-更新管理中，对杀毒引擎更新设置灰度发布版本。

5.5.5. 更新客户端程序

定期更新内网客户端程序版本，我们在响应病毒处理能力时，根据需要也会通过更新客户端程序来提升病毒防护能力，定期或及时更新客户端程序对病毒的防护能力提升有一定的帮助。建议将客户端程序更新设置为自动（或按照一定的批次自动更新）。设置方式参考更新管理相关章节。

【注意】库文件和程序文件文件在奇安信内部有严格的出厂测试检验程序，检测合格后才能发布。由于每个客户的场景有所不同，不排除可能会出现误报或兼容性问题。建议在管理中心-系统设置-更新管理中，对客户端程序更新设置灰度发布版本。

5.5.6.检修云查杀质量

云查杀是一种先进的技术架构。建议定期在客户端上采用 10 万量级以上的文件包（含白、灰、黑多类型）进行扫描，与标准的检出结果和完成时间进行对比，来检测网络通路的连通性、超时率。注意：样本少、文件单一都无法发现网络和设置上的隐患。

5.5.7. 日常运维告警

病毒防护提供了业务告警能力，可以在管理中心-系统管理-告警中心进行配置。病毒防护告警功能包括：文件监控，文件目录监控，重点病毒监控等能力。

- 文件监控：

可以监控一定时间内，全网计算机发现病毒库文件相同为相同文件达到一定数量进行告警。可以用来监控误报或大规模感染事件，

- 文件目录监控：

可以监控一定时间内，全网计算机发现病毒库包含相同目录达到一定的数量进行告警。可以用来监控内网重要的业务软件目录，及时发现可能的误报或业务软件受感染事件。

- 重点病毒监控：

可以监控一定时间内，全网计算机发现同类型病毒检出的次数达到一定数量进行告警。可以用来监控管理员关注的病毒类型的检出，及时发现关注的病毒感染的情况。

5.5.8.处理紧急问题

5.5.8.1. 误报处理

对于被终端误报的文件，可以对该文件进行加白处理，加白处理可以通过黑白名单、信任区，数字签名等手段进行处理。

5.5.8.1.1. 黑白名单

针对全网的误报处理，可以通过黑白名单功能，将被误报的文件添加白名单处理。

5.5.8.1.2. 信任区和数字签名

对于只针对单个分组终端的误报处理，可以通过策略中信任区添加文件或文件目录，还可以通过文件数字签名进行加白处理。

5.5.8.1.3. 隔离区恢复

对于已经误报并且清除的文件，可以通过隔离区备份的数据进行恢复。

5.5.8.2. 病毒快速处理

对于被终端漏报的文件，可以对该文件进行加黑处理，加黑处理可以通过黑白名单、数字签名等手段进行处理。

5.5.8.2.1. 黑名单

针对被漏报的文件加黑名单处理，可以通过黑白名单功能，将被漏报的文件添加黑名单处理。

5.5.8.2.2. 文件数字签名

针对被漏报的文件加黑处理，还可以通过文件数字签名进行加黑处理，该处理方式可以批量对所有涉及该数字签名的文件进行加黑。

5.5.8.2.3. 强力查杀

完成上述操作后，可以通过下发强力查杀任务，对指定分组终端进行强力查杀。

5.5.8.2.4. 文件专杀

如果需要文件专杀工具，也可以通过文件专杀任务功能，对指定分组终端进行文件专杀。

5.5.8.2.5. 右键扫描

在文件上点击鼠标右键进行扫描，应用额外的三项规则：

① 文件类型与扫描文件范围不一致时，正常扫描；

② 文件/路径存在信任区时，正常扫描；

③ 文件是个黑样本，但是文件/路径在信任区时，可正常检出。

5.6. 典型场景

5.6.1. 适配网络环境

5.6.1.1. 全互联网环境

全互联网环境，即管理中心、终端都能够直接连接互联网的场景。那么终端直接通过云安全中心进行云查能够保证获取到最高的病毒检测率。

建议将病毒防护策略中，检测引擎设置里面将云查杀模式调整为“直连公有云”：

仅客户端直接连接互联网、管理中心无法连互联网，建议给管理中心配置增加代理服务器。

5.6.1.2. 半隔离网

在半隔离网环境，若管理中心能够连接外网的情况下，建议终端将云查模式选择为“通过服务器代理云查”，同时针对部分终端可能会在内网和互联网环境切换的情况下，建议勾选“终端无法连接管理中心时，自动连接公有云安全鉴定中心”。以保障终端在任何网络环境下，病毒防护能力不降低。

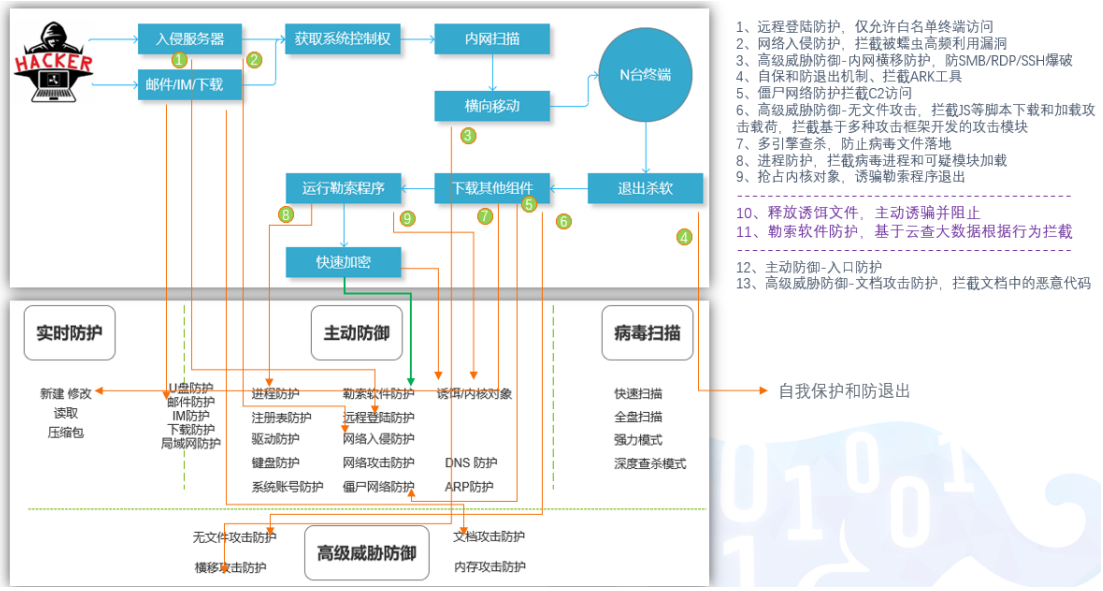
5.6.1.3. 隔离网

隔离网即所有的设备都不能与互联网进行通信，包括物理隔离或者防火墙隔离。建议终端将云查模式选择为“隔离网不连云”。

隔离网环境下，都需要定期（建议每周至少 2 次）通过离线升级工具，同步鉴定中心的未知文件等级，将管理中心或者鉴定中心的病毒库升级到最新。

5.6.2. 勒索防护专项

1）勒索防护相关功能的说明



1、远程登陆防护，仅允许白名单终端访问
2、网络入侵防护，拦截被蠕虫高频利用漏洞
3、高级威胁防御-内网横移防护，防SMB/RDP/SSH爆破
4、自保和防退出机制、拦截ARK工具
5、僵尸网络防护拦截C2访问
6、高级威胁防御-无文件攻击，拦截JS等脚本下载和加载攻击载荷，拦截基于多种攻击框架开发的攻击模块
7、多引擎查杀，防止病毒文件落地
8、进程防护，拦截病毒进程和可疑模块加载
9、抢占内核对象，诱骗勒索程序退出

10、释放诱饵文件，主动诱骗并阻止
11、勒索软件防护，基于云查大数据根据行为拦截

12、主动防御-入口防护
13、高级威胁防御-文档攻击防护，拦截文档中的恶意代码

2）勒索防护相关产品设置的说明

1、开启自我保护和防退出

2、开启高级威胁防御

3/1、管理中心连接公有云或者私有云
3/2、客户端直连公有云/直连私有云
3/3、云查质量（可用10万量级样本文件验证）

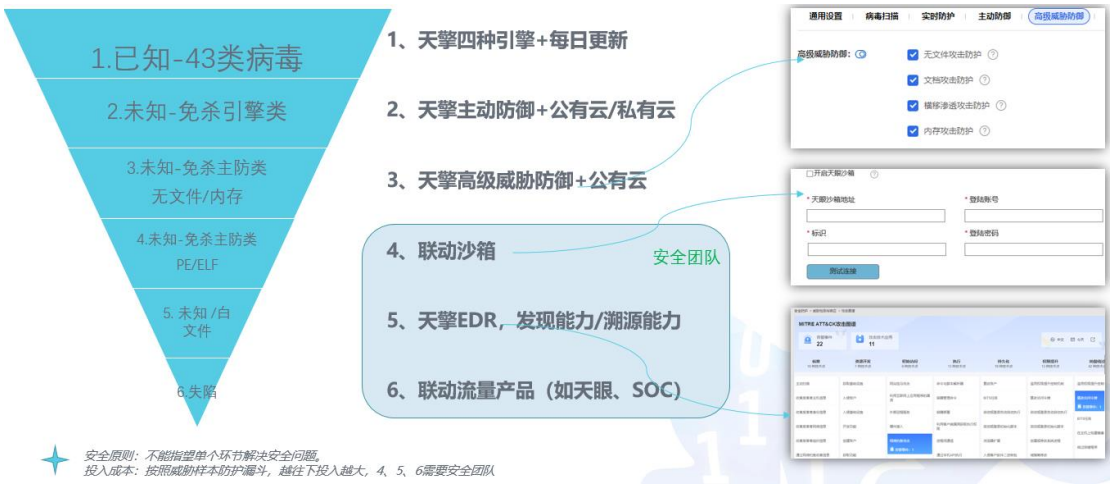
4、开启勒索防护（默认开启）

5、开启远程登陆防护

6、三道防线的病毒处理方式

7、客户端禁止添加信任

3）企业组建纵深防御的说明



6. 补丁管理

补丁管理，为企业团体提供自动化的补丁分发和漏洞修复工具和流程，及时的修复 Windows 操作系统、信创操作系统、IE、.NET Framework、Office、Adobe Reader、Adobe Acrobat 软件的已暴露的安全漏洞,解决漏洞可能被利用的安全隐患。

一些企业团体单位由于安全运营人员不足等原因并不能及时安装补丁修复漏洞，给黑客留下攻击的机会。例如“永恒之蓝”漏洞在 2017.5.12 日大规模爆发，100 多个国家和地区超过 10 万家企业和公共组织的电脑遭到了勒索病毒攻击、感染，严重影响办公甚至有的业务被迫中断，波及政府、银行、电力系统、通讯系统、能源企业、医疗、教育、机场等重要基础设施，而微软早在 2017 年 3 月发布了此漏洞的补丁，如果及时安装补丁就不会受攻击和影响。永恒之蓝事件告诉我们，不仅要安装补丁修复漏洞，而且要及时。奇安信天擎补丁管理正是为解决此痛点，为用户提供一套修复漏洞的流程和工具，自动化的分批次测试和安装补丁、逐步到全网安装补丁，如果补丁有问题则快速回退和排除补丁，既能控制其影响范围，又能及时的修复全网终端的漏洞，避免被黑客利用已暴露的漏洞攻击、破坏和造成难以估计的损失。

6.1. 基本概念

6.1.1. 漏洞

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。是受限制的计算机、组件、应用程序或其他联机资源的无意中留下的不受保护的入口点。

6.1.2. 补丁

补丁是修复漏洞、修复功能缺陷的修补程序。补丁管理是通过安装补丁来实现修复漏洞。

补丁类型

操作系统、Microsoft Office、Internet Explorer、.NET Framework、Adobe 软件。

补丁级别

安全更新：修复安全漏洞的补丁，建议立即修复。

重要补丁：修复重要功能缺陷的补丁，建议立即安装

功能补丁：修复一般功能缺陷或者优化功能的补丁，可以根据需要选择安装

可选补丁：安装后可能引起计算机或者软件不能正常使用，请谨慎安装！

热补丁：由奇安信发布的临时漏洞修补方案，等补丁官方发布后，需要卸载热补丁，安装官方补丁，目前仅支持信创终端。

【注意】策略选择时候，因为安全更新和重要补丁之间可能存在依赖关系，所以我们建议安全更新和重要补丁都勾选，并使用策略配置的方式修复。不建议针对某个特定的补丁单独安装，比如：某个安全更新被爆在野利用，这时候管理员选择这个单独的补丁对终端进行修复。这种方式很可能因为缺少某个历史前置补丁未安装从而导致无法安装的问题。

6.1.3.补丁号

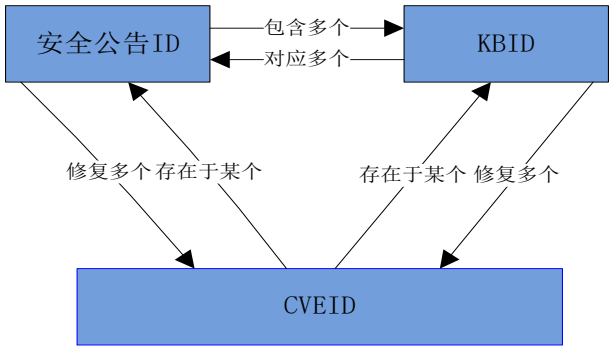
补丁号，也就是通常所说的 KBID。因为每个微软补丁都有一个唯一对应的知识库文章，所以使用知识库文章的编号作为补丁号，方便查看统计补丁的安装情况。知识库文章中描述补丁的修复了哪些漏洞、功能缺陷、补丁的已知问题等详细信息。

6.1.4.CVE 号

CVE 的英文全称是“Common Vulnerabilities & Exposures”，是国际上通用的安全漏洞的引用标准，为每个漏洞确定了唯一的名称和标准化的描述。CVE 号即国际通用的漏洞编号。例如：CVE-2017-0144 | Windows SMB Remote Code Execution Vulnerability。

管理员可以通过 CVE 号查找漏洞以及查看其修复情况，如发现有未修复的终端则可直接下发修复任务，让终端及时修复该漏洞。如有某漏洞已经被公告存在在野攻击，管理员可以针对性查看漏洞的修复情况，以便及时做相应的处置。例如永恒之蓝是多个漏洞，其编号分别是 CVE-2017-0143;CVE-2017-0144;CVE-2017-0145;CVE-2017-0146;CVE-2017-0147;CVE-2017-0148，按 CVE 号搜索查看漏洞的修复情况。

一个补丁往往修复多个漏洞，所以一个补丁号通常对应多个 CVE 号，如下图。



6.1.5. 补丁库

补丁库是补丁的特征描述，用于扫描终端的补丁安装情况。终端只有升级了新补丁库才能扫描出新补丁，为了能让终端及时扫描出新补丁修复新漏洞，需要管理中心定期更新补丁库。

【注意】在给终端进行补丁修复时，建议将终端的补丁库版本更新到最新，以确保当前终端可以扫描出需要安装的所有补丁。

6.1.6. 补丁库的发布时间

通常在每月第二个星期三（美国时间星期二）发布新版补丁库，如果发现补丁有严重问题或者微软、Adobe 公司增发了新补丁，奇安信会紧急重新发布补丁库。

信创终端补丁库的发布时间目前为一月一次，一般都是每个月的月末。如果有针对信创系统/服务器的紧急漏洞，奇安信团队会根据紧急程度判断是否需要紧急发布针对该问题的补丁库。

6.1.7. 补丁日

北京时间每月第二个星期三，美国时间星期二，奇安信同步微软在补丁日当天发布补丁库。信创终端暂不涉及。

6.1.8. 灰度分发

先让一个分组的终端先升级最新补丁库安装新补丁，观察一段时间没有问题再允许下一个分组升级安装新补丁，逐步到全网终端安装新补丁。如果在中途发现补丁有问题，则将有问题的补丁添加到策略的排除列表中。

6.1.9. 奇安信天擎补丁通告

奇安信天擎发布补丁库时会同步在微信公众号“奇安信 Cert”中发布一篇补丁通告，详述每次发布的补丁的详细情况，通常包含：

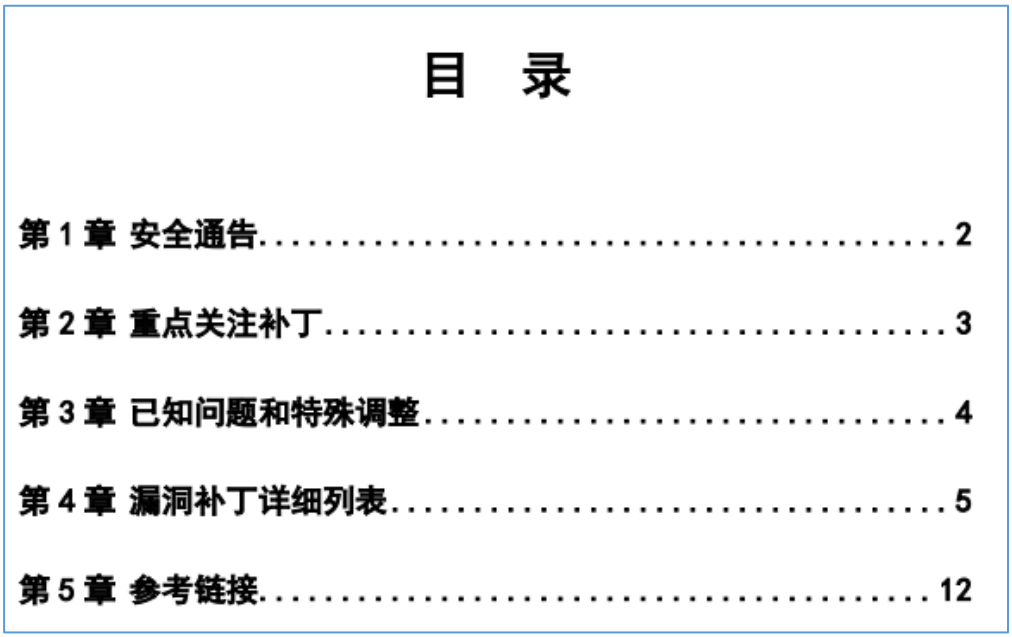
a) 修复了多少漏洞、影响哪些软件、是否有已暴露或在野攻击的漏洞（重点关注补丁）。

b) 已被公开披露或已存在在野利用攻击的漏洞，推荐需重点关注的补丁。

c) 补丁存在的已知兼容性和系统性能影响的问题。

d) 补丁号、补丁的级别、对应产品、漏洞影响、CVE-ID、是否被公开披露、是否已受攻击、漏洞被利用的概率等。

下图是样例：



目　录

第 1 章 安全通告.....2
第 2 章 重点关注补丁.....3
第 3 章 已知问题和特殊调整.....4
第 4 章 漏洞补丁详细列表.....5
第 5 章 参考链接.....12

第1章 安全通告

尊敬的客户：

最新补丁库 2018.08.15.1 版本已发布，本次发布更新了微软 2018 年 8 月最新安全公告发布的补丁。本月补丁日微软补丁修复了 36 个安全漏洞，其中 10 个评级为“严重”，25 个评级为“重要”。这些漏洞影响 Internet Explorer、Edge、.NET Framework、Windows DNSAPI、Microsoft Office 以及 Office Services 等。

本次发布同时更新了 Adobe 最新安全公告（APSB18-29）发布的 7 个安全补丁，本月 Adobe 修复了 2 个安全漏洞，这些漏洞影响 Adobe Acrobat 和 Reader。

第2章 重点关注补丁

本次修复的以下高危漏洞需要重点关注，其中 CVE-2018-8373 已被公开披露且存在在野攻击，推荐尽快安装对应补丁，详情如下：

KBID	产品	修复的漏洞	漏洞详情
4343205	Internet Explorer	CVE-2018-8373	脚本引擎内存损坏漏洞

第3章 已知问题和特殊调整

本月发布的漏洞补丁暂未发现已知问题。

第4章 漏洞补丁详细列表

本月发布的微软安全更新补丁详细列表如下：

KBID	天擎级别	产品	影响	详细信息	公开披露	已受攻击	最新软件版本	较旧软件版本	拒绝服务
4343899	高危	Windows 7 、Windows Server 2008 R2	远程执行代码	CVE-2018-8349	否	否	2	2	N/A
			远程执行代码	CVE-2018-8316	否	否	2	2	N/A
			特权提升	CVE-2018-8404	否	否	1	1	N/A
			信息泄漏	CVE-2018-8398	否	否	2	2	N/A
			信息泄漏	ADV180018	否	否	2	2	N/A
			信息泄漏	CVE-2018-8348	否	否	2	2	N/A
			信息泄漏	CVE-2018-8394	否	否	2	2	N/A
			信息泄漏	CVE-2018-8396	否	否	4	2	N/A
			远程执行代码	CVE-2018-8397	否	否	4	2	N/A
			特权提升	CVE-2018-8343	否	否	2	2	N/A
			特权提升	CVE-2018-8342	否	否	4	2	N/A
			信息泄漏	CVE-2018-8341	否	否	2	2	N/A
			特权提升	CVE-2018-8339	否	否	2	2	N/A

6.2. 补丁分发自动化运维思路

奇安信天擎补丁管理的设计理念是自动化运维，自动从奇安信云端更新补丁库、按照管理员预先设置自动的灰度发布，在保障及时修复安全漏洞的前提下尽可能的降低管理员的运维工作量。

平时 - 业务连续性优先兼顾安全性：

办公桌面、业务终端补丁管理：预先设置好灰度更新的批次和补丁管理策略（分时间段、按级别、排除有兼容性问题的补丁等），每当管理中心更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。

服务器补丁管理：业务连续性优先，安装补丁需与业务部门密切协同。根据奇安信天擎补丁通告（受影响的系统或应用，严重等级，漏洞被利用的概率，漏洞信息是否已经公开，是否有在野攻击，补丁是否有已知的兼容性和性能影响问题），决定补丁的安装策略，必要情况下可以先采取缓解措施再安装补丁。

战时 -安全优先：

已被利用漏洞（如永恒之蓝）应急响应时，安全优先，全力保证补丁的分发、安装。

6.3. 补丁更新设置

补丁更新设置，位于管理中心>系统管理>更新设置，管理员根据企业自身的一些环境、业务等特点设置适合的补丁更新方式和时间。管理中心提供了通用的默认设置，仍建议企业管理员要根据自身的企业特点来调整设置，下面详细介绍各更新功能的意义。

部署管理中心后，管理员应首先设置补丁库更新的时间和终端补丁库更新设置，推荐设置为管理中心每天 12:00-23:00 自动更新，升级源为从互联网升级（如果业务环境非常复杂，建议延迟 1-2 个月安装补丁），终端更新设置 2-3 个批次，总测试时间不宜超过 15 天，这样比较好控制补丁风险又能较及时修复漏洞。

【注意】库文件和程序文件文件在奇安信内部有严格的出厂测试检验程序，检测合格后才能发布。由于每个客户的场景有所不同，不排除可能会出现误报或兼容性问题。建议在管理中心-系统设置-更新管理中，对库文件更新设置灰度发布版本。

6.3.1. 服务器更新设置

该模块设置补丁库的更新时间，支持按月、周、天、小时周期性自动更新。如果是隔离网使用“离线工具”更新补丁库和补丁文件。

6.3.2. 终端更新设置

该模块设置全网终端的更新补丁库的时间，即新补丁的灰度分发的批次。

【注意】病毒库和程序文件文件在奇安信内部有严格的出厂测试检验程序，检测合格后才能发布。由于每个客户的场景有所不同，不排除可能会出现误报或兼容性问题。建议在管理中心-系统设置-更新管理中，对库文件更新设置灰度发布版本。

6.4. 补丁管理策略

补丁策略设置，位于管理中心>终端管理>策略管理>终端策略>补丁管理，管理员根据企业自身的一些环境、业务等特点配置适合的补丁管理策略。管理中心

提供了通用的默认设置，但强烈建议企业管理员要根据自身的企业特点来调整策略，下面详细介绍各策略功能的意义。

6.4.1.补丁安装设置

本模块提供了自动扫描补丁安装情况、自动安装、指定时间段安装补丁的功能，以及是否限定终端用户主动安装补丁。

扫描补丁（默认为关）：开启自动扫描补丁安装情况则每次开机一小时内扫描一次，如果不关机每天也会至少扫描一次，不开启则不自动扫描，需要自动安装或者管理员分发扫描任务时才扫描。

【注意】在没有配置自动扫描的情况下，为了能够统计最新的补丁库中补丁安装情况，在补丁库更新之后会触发一次自动扫描，以校准补丁统计的准确性。

自动安装补丁模式（默认为关）：开机时或者在指定的时间段内随机开始自动安装策略指定的补丁。也可以指定未关机的终端间隔 12 小时安装 1 次。通常用于可以短时中断的办公终端。

按时间段安装：在指定的时间段内安装策略指定的补丁，避免高并发挤占网络带宽。通常用于工作时间段不能中断业务的用户，建议设置为工作日下班之后到第二天上班之前修复、周六周日全天修复。在大型网络中也可以用于不同分组分时间段安装补丁，避免挤占网络带宽影响业务。

【注意】安装补丁的过程中不能强行中断安装或强制重启以及断电，一旦出现以上情况，可能导致系统出现蓝屏或无法开机等问题。请合理安排安装补丁时机。

影响到编辑 Office 文档时提醒：如果安装补丁前发现当前终端正在使用 Office，则先提醒终端用户，待终端用户确认才安装补丁。

6.4.2.补丁安装范围

本模块提供设置补丁安装范围，设置自动安装和终端用户自助安装的补丁范围，支持通过“补丁级别和补丁类型”和“补丁列表”两种模式指定安装范围。

Windows 终端

信创终端

排除列表：终端将自动排除在排除列表内的补丁，则不会再被安装，除非取消忽略。排除列表用于排除有问题的补丁。

补充列表：是对“按照补丁类型和级别安装”模式的补充，用于补充指定级别和类型不能描述的补丁。

指定列表：用于安装补丁非常谨慎的客户，只安装明确指定的补丁。

【注意】日常运行中建议安全更新和重要补丁均选择，部分安全更新安装依赖重要补丁。如果不选择重要补丁，可能导致安全补丁安装失败（绝大多数安全补丁无法安装都是这种情况）。

6.4.3. 补丁下载安装顺序

本模块设置终端补丁下载和安装的顺序。支持“逐个下载和安装”(默认)和“下载完成全部补丁后，再安装”。

6.4.4. 补丁及时生效

本模块设置为在安装补丁自动提醒终端用户重启或自动重启，默认未开启，即不提醒。以便让补丁及时生效修复漏洞。仅支持 Windows 终端

提醒重启：可设置提醒一次或多次提醒并配置提醒频率。

自动重启：可配置倒计时时间，已经指定可重启的时间段。

自动重启一般用于无人值守的重要终端和安全优先于办公的特殊场景。

6.4.5.其他设置

本模块设置一些与补丁安装相关的设置。有关闭上报排除的补丁信息、智能忽略、自定义终端保留补丁文件的时间和目录等。

不上报排除列表中或者安装列表之外补丁的安装信息（仅 Windows）：开启后，终端将不再上报排除列表或安装列表之外补丁的安装日志信息。默认未开启。

关闭 Windows Update（仅 Windows）：开启后，终端将关闭 Windows Update。支持补丁安装范围支持的 Windows 的操作系统版本。默认未开启。

开启智能忽略：补丁修复过程中如果安装失败，程序会进行多次尝试，如果累计尝试三次安装均失败（不包括下载失败）的情况下，如果开启智能忽略，则会标记为智能忽略。已经被智能忽略的补丁，后续将无法被扫描到也不能再手动安装了，需要在控制台取消忽略。如果未开启智能忽略，则后来安装失败后，后续还能被扫描出来。默认未开启。

补丁文件保存时间：开启后，可以设置终端下载的补丁文件保存的时间。默认开启，保存时间 30 天。默认未开启。

自定义补丁文件保存目录：开启后，可以设置补丁文件在终端保存的位置。如果没有实际盘符，则会在客户端安装目录下生成 hotfix 目录，用来存放补丁文件。默认未开启。

开启系统还原点功能（仅 Windows）：开启后，终端将每 24 小时创建一次系统还原点。支持补丁安装范围支持的 Windows 的操作系统版本。当电脑需要还原时，可以通过以下方式进行还原：win7：开始>程序>附件>系统工具>系统还原命令根据提示还原。win10：此电脑 >属性>系统保护>系统还原。

6.5. 终端任务

进入管理中心>终端管理>终端任务界面，通过新建任务来创建补丁管理业务任务，任务支持：扫描补丁、修复补丁、卸载补丁、取消忽略、强制停止安装、升级停服系统。（任务使用方法详见终端任务）。

扫描补丁：用于立即检查终端最新的补丁安装状态。

修复补丁：用于对指定补丁下发修复任务。

卸载补丁：用于卸载有问题的补丁。

取消忽略：用于取消曾经忽略的补丁。

强制停止安装：用于强制停止安装补丁，降低有问题的补丁的影响。

停服系统升级：用于升级已经停服的操作系统，降低因漏洞无补丁修复带来的安全风险。

【注意】任务操作时候，修复补丁如果涉及终端较多或补丁文件较多的情况下，建议配置好随机延时。同时建议考虑按照分组分批下发，并配置好限速。防止大规模补丁下载造成网络异常。

6.6. 补丁运维管理

通过“管理中心>安全防护>补丁管理”可以查看补丁相关的概况、日志、报表等功能。

6.6.1. 终端补丁概况

终端补丁概况用来展示全网终端（也可指定分组）的补丁安装情况，以帮助管理员了解终端的安全现状。

6.6.2. 补丁文件

本功能可以展示服务器上最新补丁库中的补丁信息，也可以在服务器是隔离网模式下展示补丁文件的状态，便于管理员判断终端下载补丁文件失败的原因。

6.6.3. 停服系统

本模块提供检测全网终端的操作系统的停服情况，并提供解决建议和升级系统功能。

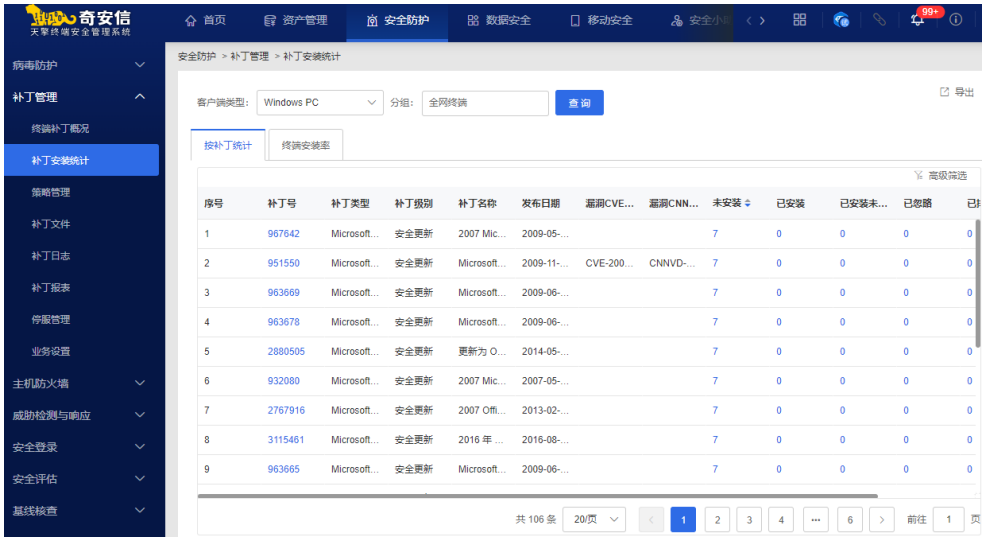
每个版本升级前先做详细的兼容策略，预防系统升级后影响业务软件正常使用。其次，升级一定要分阶段分批次进行。

a） 通过下发任务对已经停服的终端升级系统。

b） 选取少量终端做系统升级测试，待确认系统升级后不影响办公、生产后再扩大升级范围。

6.6.4. 补丁统计

用于统计全网终端(也可指定分组)的补丁安装情况。支持按照“终端分组、终端类型、补丁号、补丁级别、补丁类型、CVE 编号、CNNVD 编号”多种维度进行统计。



按照终端分组统计补丁安装率。

6.6.5. 补丁日志

补丁日志是全网终端（也可指定分组）补丁管理相关的日志展示。同时该日志支持按照指定时间、分组进行查询。同时支持高级筛选和导出等功能。

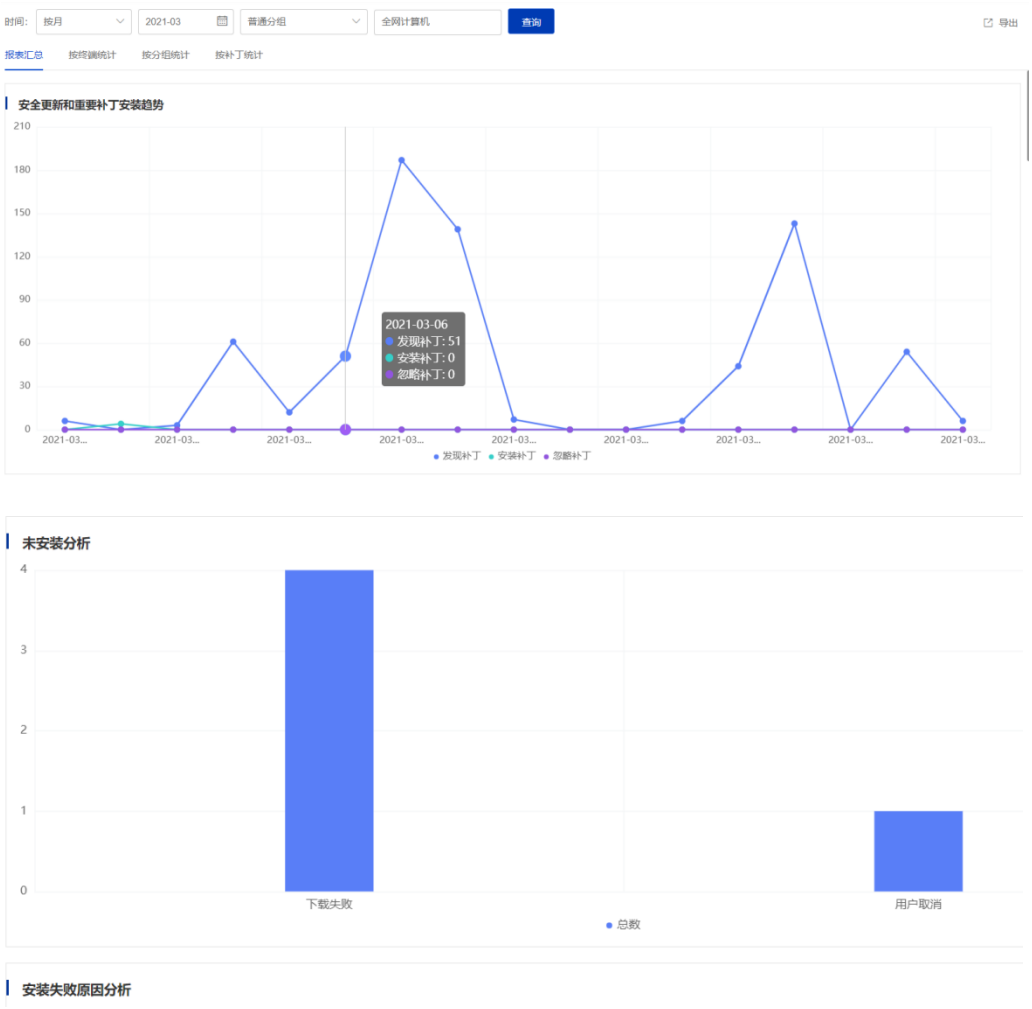
补丁日志展示扫描终端的信息，补丁日志主要信息有：补丁号、补丁级别、补丁类型、事件类型、补丁安装结果详情。

6.6.6.补丁报表

补丁报表是用来展示全网终端（也可指定分组）补丁管理相关的报表统计展示，展示报表包括：报表汇总、按终端统计。通过分析报表中的相关趋势及时掌握全网终端的补丁安装情况以及漏洞修复情况。

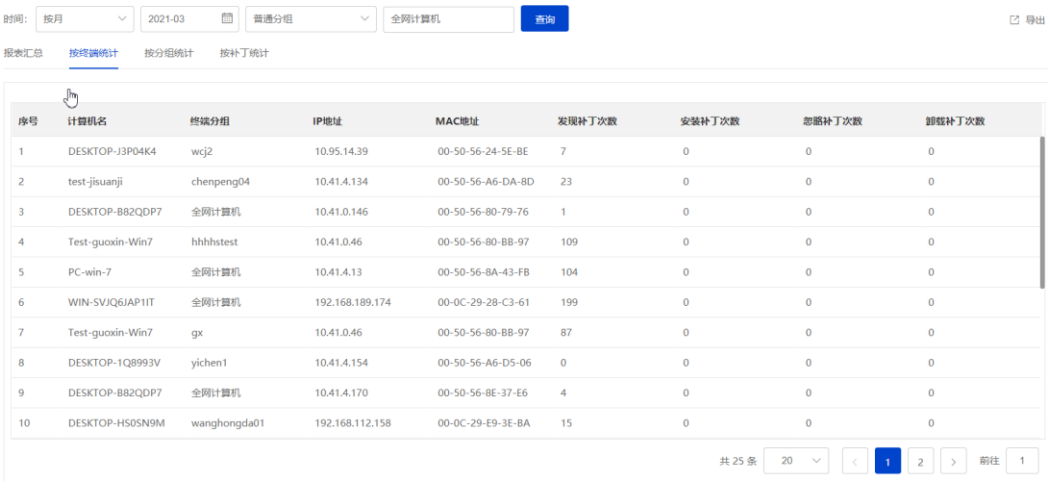
6.6.6.1. 报表汇总

报表汇总提供了补丁安装的趋势图、未安装分析以及安装失败原因、安装补丁 TOP10 的分析数据。



6.6.6.2. 按终端统计

该功能提供终端维度的统计补丁的安装情况。

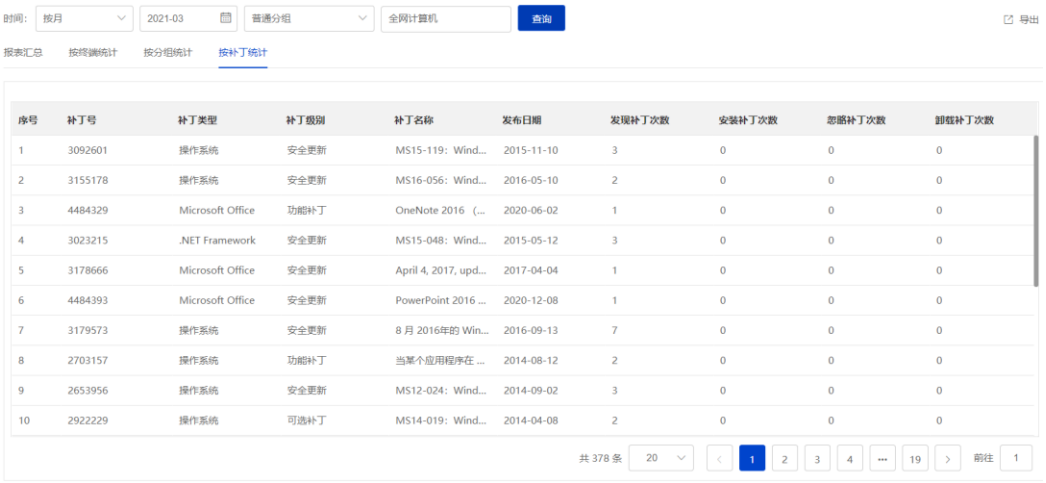


6.6.6.3. 按分组统计

该功能提供终端分组维度的统计补丁的安装情况分析。

6.6.6.4. 按补丁统计

该功能提供补丁维度的统计补丁的安装情况分析。



6.7. 终端用户自助修复

终端用户可以打开终端的“补丁管理”界面安装。终端用户是否可以安装补丁受管理员限制。

清理补丁文件：手动清理本终端已下载的补丁文件。终端会自动清理 30 天下载的补丁文件。

一般用于业务连续要求不高的终端，允许终端用户手动安装补丁。比如证券公司一般会禁止在交易时段内手动安装业务终端的补丁，影响交易。

6.8. 日常运维管理

自动化运维是尽可能降低补丁管理工作量，并不是完全不需要管理员参与，终端安全仍需管理员持续的运维。

A. 管理中心自动从云端更新补丁库。隔离网需要管理员使用离线工具同步补丁库和补丁文件。

B. 管理员查阅奇安信集团补丁通告，按需调整策略（如排除有问题补丁、修复时间）。

C. 等待优先分发的终端反馈问题，分析问题，调整修复策略（排除有问题补丁或者关闭修复功能）。

D. 管理员查看补丁安装统计结果，手动处理安装失败的补丁（根据补丁和资产重要性决定）。

E. 管理员需关注是否有新发的奇安信集团补丁通告，根据通告内容调整策略，比如已有新补丁解决了之前补丁的问题，可能需要恢复已排除的补丁，使其被安装。

【注意】库文件和程序文件文件在奇安信内部有严格的出厂测试检验程序，检测合格后才能发布。由于每个客户的场景有所不同，不排除可能会出现误报或兼容性问题。建议在管理中心-系统设置-更新管理中，对库文件更新设置灰度发布版本。

6.9. 典型场景

6.9.1. 服务器可连接互联网

推荐采用自动化运维方案，如果管理中心可以连接互联网的用户场景，建议设置为自动从奇安信云端更新补丁库、灰度分发、自动修复，在保障及时修复安全漏洞的前提下将管理员的运维工作量降到最低。

推荐设置：

A. 管理中心补丁库更新方式：每天 12:00-02:00 自动更新，升级源为从互联网升级。

   如果业务环境非常复杂，建议延迟 1-2 个月安装补丁。

B. 灰度分发：挑选终端组成优先升级分组，按批次依次开始升级补丁库测试新补丁。推荐设置 2-4 个批次，总的测试观察天数 10-20 天，再长的话就可能当月补丁库还没有升级完成，下月补丁库又发布，导致部分终端不能更新补丁库。

C. 策略设置：
   a) 终端下载补丁文件设置为内网优先（终端与管理中心网络环境）。
   b) 开启自动安装补丁模式。其余设置按需设置即可。
   c) 如果终端数量较多，全网终端按分组分批次在不同的时间段安装补丁，减小网络带宽压力。

6.9.2. 纯隔离网

纯隔离网内管理中心不能访问互联网，不能下载补丁库和补丁文件，需使用离线更新工具定期导入补丁库和文件到管理中心。

操作方法详见：《离线更新工具操作手册》

终端下载补丁文件设置为仅内网（终端与管理中心网络环境）

其余推荐设置同**错误!未找到引用源。**章节。

6.9.3. 小带宽网络下安装补丁的推荐方案

1) 分时间段、错峰安装补丁。

a) 在业务软件空闲时间段安装补丁，如中午、夜间；
b) 将全网终端划分到多个时间段依次安装补丁，避免集中下载补丁，造成网络干路拥塞。

2) 启用局域网增加 P2P 模式，减少终端去服务器或去其他网段下载补丁，从而减少占用干路带宽。

3) 限制服务器提供终端下载文件的并发数和单个连接的下载速度。

4) 级联部署或者分公司（分中心）部署升级服务器，减少区域主干网的带宽占用。

5) 如果分支机构与总部 VPN 带宽小，自己又可以上互联网，推荐让分支机构终端从互联网下载补丁文件，既能控制补丁安装节奏，又能减少占用干线带宽。

6.9.4. 补丁下载与安装网络优化

1) 为了避免大规模补丁发布时引起的“网络风暴”——即网络拥塞，我们的程序集成了智能错峰检测功能。该功能自动分散数据流量，以减少高峰期内对网络的压力。

用户可以采取以下措施进一步降低网络拥塞风险：

2) **自动安装策略：**在补丁管理界面中设置自动安装，自动安装策略可以对扫描时间进行自动错峰，以避免高峰期内的网络拥塞。

操作路径：补丁管理 > 策略管理 > 补丁策略 > 安装补丁设置

3) **指定时段安装：**在补丁管理界面中选择特定时间段进行补丁下载和安装，确保在系统使用较低的时段操作。

操作路径：补丁管理 > 策略管理 > 补丁策略 > 安装补丁设置

4) **启用 P2P 功能：**通过开启终端管理中的 P2P（点对点）功能，优化本地网络内的补丁下载流程，减少跨网段的数据传输，从而降低网络拥塞风险。

操作路径：终端管理 > 基础策略 > 通讯设置 > 下载管理

5) **配置下载限速：**对于使用内网模式的用户来说，为了防止管理中心的大量下载占用导致无法访问的问题，可以在系统管理设置中配置文件下载限速。

操作路径：系统管理 > 系统设置 > 通用设置 > 文件限速

6) 通过这些策略和设置，您可以有效地管理和减少在补丁更新过程中可能出现的网络拥塞问题。

6.10. FAQ

6.10.1. 补丁卸载后，扫描不到

属于正常情况。

因为虽然补丁卸载了，但是这个补丁可能较旧，终端的文件已经比补丁中的部分文件的版本高，所有不能再安装。举例说明：

- KB3192391 和 KB4471328 补丁都会更新 Ntoskrnl.exe 这个文件来修复操作系统漏洞。更新后 Ntoskrnl.exe 版本号分别是 6.1.7601.23564、6.1.7601.24308。
- 假设终端安装了这两个补丁，卸载补丁 KB3192391，实际上并不会回退 Ntoskrnl.exe 文件，所以下次扫描就会变成不支持。说明这个旧补丁已经不适用于终端，手动运行安装包也会提示不适用。
- 这种情况如果必须再安装这个补丁，必须要将比该补丁后发布的补丁都卸载才能可能安装成功。
- 强烈建议不要卸载旧补丁，没有实际意义，一般旧补丁的问题已经新补丁中修复了，而新补丁更容易出问题。

6.10.2. 补丁安装失败如何处理

因为不同终端有不确定的差异，补丁安装率并不能达到 100%，总有个别终端安装补丁失败。在管理中心可以查看安装失败的原因，根据失败原因做相应处理——处理安装失败的原因或者开启智能忽略策略。

若想分析补丁安装失败的详细原因，在终端手动运行补丁安装程序，通过安装结束后的错误码在网上查找原因或咨询 95015。也可以手动收集补丁安装日志（C:\Windows\Logs\CBS 目录里所有的文件）反馈给奇安信售后专家分析，分析后将新增的失败原因添加到产品中，用户下次再遇见此原因则可以直接在管理中心上查看清楚。

7. 主机防火墙

7.1. 基本概念

7.1.1. 主机防火墙

主机防火墙（Host Firewall），是针对终端上的基于网络五元组信息对主机网络流入流出进行防护的模块。通过配置和管理防火墙放行或拦截规则，来增强阻断或放行终端的异常网络请求、保障终端和内网的安全的能力，支持Windows PC/Server、macOS、信创终端。

7.1.2. 接管系统防火墙

针对 Windows 安全中心提供了一套安全防护功能，病毒防护和防火墙功能。同时微软也针对安全厂商提供和 Windows 安全中心对接的能力。微软的 MVI（Microsoft Virus Initiative）合作伙伴均可以通过微软提供的标准接口在 Windows 安全中心进行注册。当安全产品向 Windows 安全中心发起注册请求时，Windows 安全中心会响应注册请求同时也会关闭自身的功能。

针对信创系统提供了一套安全防护能力，可接管系统防火墙，统一由管理员统一管控，实现更为方便终端网络运营管理。

7.2. 主机防火墙策略

主机防火墙策略设置，位于管理中心>安全防护>主机防火墙>策略管理，管理员根据企业自身的一些环境、业务等特点进行必要的防护策略设置。管理中心提供了通用的默认设置，但强烈建议企业管理员要根据自身的企业特点来调整策略，下面详细介绍各策略功能的意义。

7.2.1. 主机防火墙设置

7.2.1.1. 主机防火墙

终端主机防火墙功能是否开启可以进行设置，开启该功能后主机防火墙的功能才能生效。同理如果关闭该功能，则主机防火墙的其他设置均失效。默认未开启。macOS 类型终端无此开关。

7.2.1.2. 防火墙规则

开启主机防火墙功能，可以通过该功能配置防火墙规则，同时还可以对已经配置的规则进行优先级排序。终端匹配规则是先匹配先生效原则。

添加防火墙规则，支持配置规则名称、规则类型（支持域名或 IP、IP 支持输入 IPV4 和 IPV6、操作（支持允许、拒绝）、方向（支持入站、出站、双向）、协议（支持 TCP、UDP、TCP+UDP、ICMP、多播和组播、任意）、本地端口（支持任意、自定义）、远程地址（支持任意、自定义）、远程端口（支持任意、自定义）等功能。

添加防火墙规则时，支持对生效时间和生效场景进行选择配置。

添加规则后，可以通过界面的上移\下移功能，对已有规则进行优先级排序，越上面优先级越高。

可以通过导入导出功能，对防火墙规则进行管理。

点击“高级设置-生效条件”，可以对生效时间和生效场景进行配置，供每条防火墙规则选择使用。

生效条件的设置可参考：3.4.策略管理。

【注意】添加拦截策略可能请注意，采取拒绝所有远程访问请求的策略可能会导致终端设备无法连接到网络。建议在配合允许特定远程访问的策略下使用此类策略，并且在需要访问远程地址（如 VPN、零信任安全架构、准入列表规则、DNS 服务器地址、打印服务器等）时，必须进行适当的白名单处理。

加白路径：资产管理 > 终端管理 > 基础策略 > 策略内容 > 白名单设置 > 网络访问白名单。

另外添加策略时，如果存在需要添加端口范围时。建议将一些常见应用访问端口设置高优先级放行后，再配置范围端口。以防关键应用网络被拦截。

7.2.1.3. 接管系统防火墙

该功能提供是否开启接管系统防火墙功能。开启接管系统防火墙功能之后，终端将会注册到 Windows 安全中心，同时关闭系统防火墙。如果关闭接管，则是取消 Windows 安全中心注册，同时开启系统防火墙。在信创终端中，开启接管会停用系统防火墙。默认不开启。

如果未开启接管功能，则 Windows 防火墙和主机防火墙同时存在的情况下，最终的效果如下：1、同时开启拦截效果为拦截范围的叠加。2、如果一个为放行，另一个为拦截。则拦截优先，最终效果为拦截。

Windows PC/Server、信创终端支持，macOS 不支持。

【注意】接管系统防火墙开启后，Windows 系统防火墙会自动关闭。如果需要开启接管系统防护墙时，建议先在防火墙规则中配置好防火墙防护策略后再开启。防止直接接管系统防火墙导致系统防火墙规则失效导致高危端口被暴露。

如果接管系统防火墙状态为开启，则取消接管或卸载主机防火墙模块卸载时，会执行取消接管动作。执行取消接管系统防火墙之后，在 Windows 系统防火墙在被接管期间新增的应用有联网动作可能会被系统防火墙拦截并提示。如果存在利用该功能放行的终端应用网络的场景的情况下请谨慎操作。

7.2.1.4. 日志上报配置

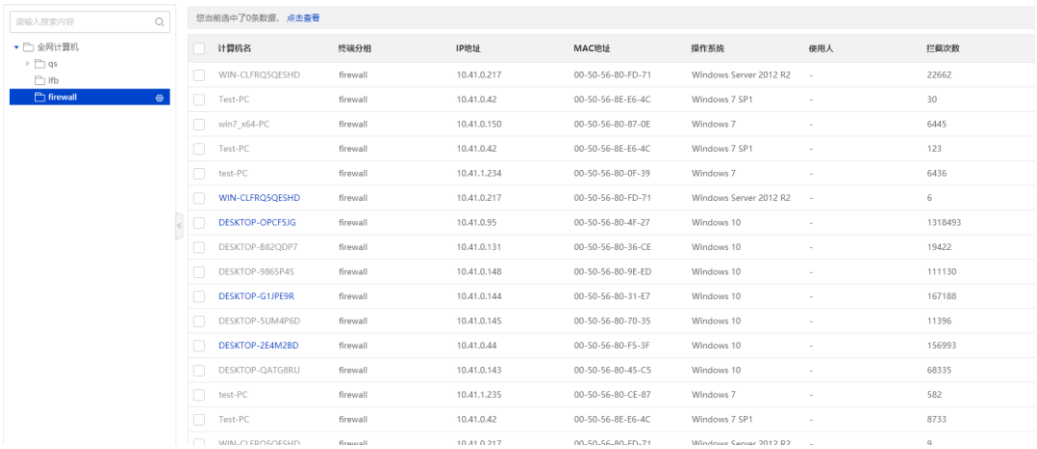
通过该功能可以配置是否上报日志，开启功能后同时可以配置日志上报的频率。**默认未开启，不上报日志。**

7.3. 业务管理

通过“管理中心>安全防护>主机防火墙”可以查看主机防火墙业务相关的概况、日志、报表等功能。

7.3.1. 防火墙概况

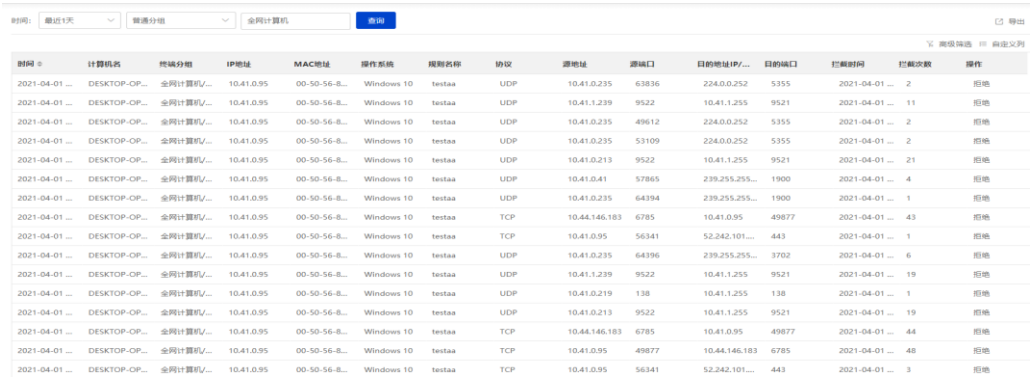
防火墙概况用来展示全网终端（也可指定分组）防火墙规则拦截的情况，根据分析拦截次数，以帮助管理员了解终端的安全现状。



7.3.2.防火墙日志

防火墙日志是全网终端（也可指定分组）防火墙防护相关的日志展示。同时该日志支持按照指定时间、分组进行查询。同时支持高级筛选和导出等功能。

防火墙日志展示拦截终端的信息，防火墙防护相关信息：规则名称、协议、源地址、源端口、目的 IP/URL、目的端口、拦截时间、拦截次数、操作等信息。



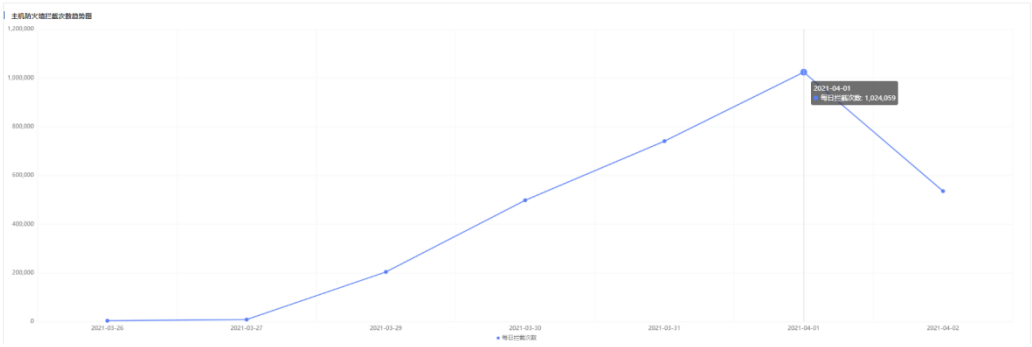
【注意】如果防火墙规则添加较多或范围较大的情况下，可能会出现日志非常多的情况。为了防止日志过多或日志未上报导致无法运维的情况，建议在开启日志上报的时候合理配置。

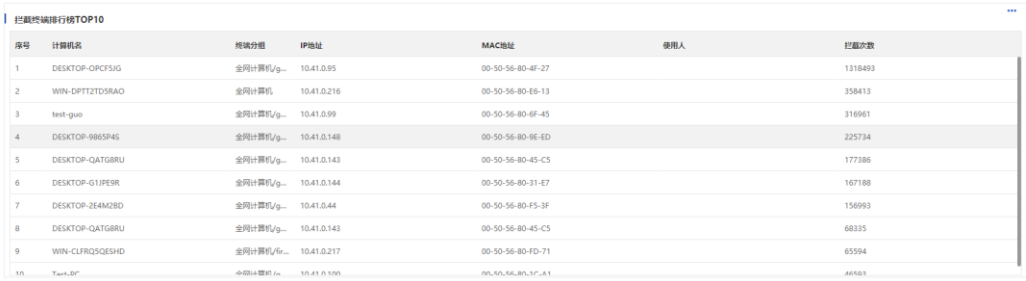
7.3.3.防火墙报表

防火墙报表是用来展示全网终端（也可指定分组）防火墙防护相关的报表统计情况，展示报表包括：报表汇总、按终端统计。通过分析报表中的相关趋势及时掌握内网终端的拦截情况。

7.3.3.1. 报表汇总

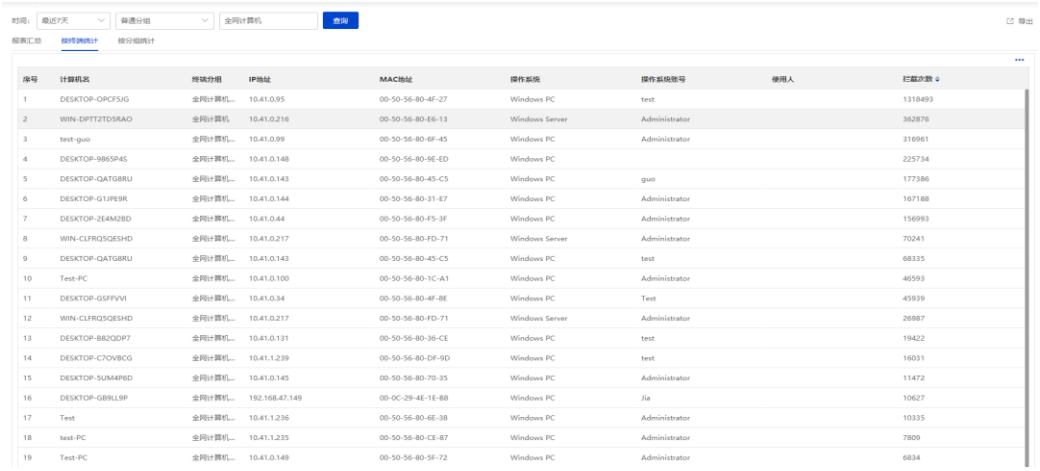
报表汇总提供了针对主机防火墙拦截的趋势图、拦截终端排行榜 TOP10 展示。





7.3.3.2. 按终端统计

该功能提供根据终端统计防火墙拦截的情况，通过筛选排序功能，可以快速定位出内网安全风险的范围和影响情况，通过分析做出处理决策。



7.3.3.3. 按分组统计

该功能提供按分组统计防火墙拦截的情况，方便管理员按分组进行统计分析。

8. 威胁检测与响应（EDR）

8.1. 基本概念

8.1.1. EDR

EDR（Endpoint Detection and Respons）即“终端检测与响应系统”。

在企业终端安全领域，企业用户不但能接触到面向企业个人的安全威胁，同时还有可能接触到面向企业资产的安全威胁。由于企业资产的价值是远高于企业个人的，所以攻击者愿意付出更多的攻击成本来实施安全威胁。这些成本往往包括一个团队，使用鱼叉攻击、社会工程学攻击等定向攻击的方式，甚至还有可能使用 0day 漏洞来提升攻击的强度，确保最终威胁实施的成功和隐蔽。同时，由于企业的安全大数据相对封闭，导致安全厂商无法第一时间帮助企业用户处理安全威胁。而企业的安全运维能力往往不足，最终导致面向企业资产的安全威胁的响应速度严重不足，甚至在企业内潜伏多年，无法发现。

通过 EDR，奇安信能够把自身云端终端安全大数据处理能力，前置到企业用户中。这些处理能力不光包括大数据存储，查询的能力，还包括大数据分析的思路和方法。通过奇安信云端威胁情报的向企业用户推送，企业用户在威胁情报中知识的引导下，学习企业内发现的已知威胁，积累威胁分析的经验。EDR 系统在威胁情报中知识的引导下，可以发现新的潜在未知威胁，供管理员分析与调查。最终，通过一套标准的未知威胁响应的业务流程，能够让对未知威胁的单次响应，快速落地为对已知威胁的持续拦截，最终成功缩短未知威胁的响应时间。

8.1.2. 威胁情报

威胁情报是关于 IT 或信息资产所面临的现有或潜在威胁的循证知识，包括情境、机制、指标、推论与可行建议，这些知识可为威胁响应提供决策依据。这

里特指奇安信威胁情报中心根据云端收集到的攻击情报信息，经过数据处理加工确认后，推送到 EDR 的情报。通过云端威胁情报与 EDR 的终端信息进行匹配，形成企业内部的威胁告警，根据告警进行威胁溯源，进而去做出响应。

8.1.3. IOC

IOC（Indicator of Compromise）以 xml 文档类型描述捕获多种威胁的事件响应信息，包括病毒文件的属性，注册表改变的特征，虚拟内存等。能帮助管理员直观的去了解威胁以及影响范围。

8.1.4. 进程树

进程树是一系列关联的进程的表达方式，通常至少包含一个父进程和一个子进程。一个程序进程运行后，会调用其他的一些进程来一起完成某项具体的功能与任务。通过进程树的展示，可以清楚的了解一个威胁行为的源头，进而对威胁进行溯源。

8.1.5. 数据字典

数据字典是将 EDR 数据采集获取到的数据进行规范化，模块化。这包括涉及样本投递的迹象追踪，样本在内存活动的迹象追踪，以及样本对系统造成变更的迹象追踪。形成一个列表，帮助管理员通过列表对每一种数据的意义、查询方式进行了解。

8.1.6. 威胁响应

产生威胁告警后，通常需要管理员或者安全分析人员对告警终端进行调查分析，经核实后，确认告警是一个确切的威胁，这时管理员或者安全分析人员可以通过 EDR 对每一个威胁进行处置，包括进程终止、进程隔离等；若分析后发现告警并没有产生实际影响或者不需要处置，可以对告警进行“不处理”。通过对威胁地及时响应，能够保证内网终端的安全。

8.1.7. 筛选

数据通过终端采集上报到管理中心，通过威胁追踪的搜索界面，管理员可以按照数据字典去构建任意条件的搜索数据，符合搜索条件的数据就会全部展现在管理中心界面上。而这些数据是没有经过任何维度的聚合分类的，所以数据量会比较多，并且种类繁多，可能包含终端进程信息、网络请求信息等。根据数据类型进行分类筛选，可以让管理员或者安全分析人员聚焦到一类数据中，进行进一步的分析。EDR 将数据分成了文件传输、账户变更、文件操作、终端进程信息、DNS 访问、IP 访问等大类，每一个大类里还提供了细分数据过滤筛选的条件。同

时 EDR 也支持自定义过滤筛选条件设置，把多个筛选条件以与或非的方式进行编排，满足多种筛选方式。

8.1.8. 版本

基础版 EDR 为轻量级版本，通过终端本地行为分析引擎对终端的行为数据进行异常检测，无需配合终端大数据分析平台即可使用，安装部署简单，功能使用方便，适用于中小型企业。而高级版 EDR 则包含 EDR 基础版全部功能，增加终端数据采集、监测和大数据关联分析能力，可以显著提升发现高级威胁的能力，在对抗内网渗透、零日漏洞利用等攻击场景中获得更好的检测和响应效果，由于需部署大数据分析平台，高级版 EDR 更适用于中大型企业。

8.2. 基础版基本功能

8.2.1. 威胁概况

全网终端安全态势可视化展示，实时展示威胁告警、热门威胁事件和威胁处置情况，自动分析全局风险等级，帮助客户掌握全网终端安全态势，提升安全管理能力。

支持点击告警数、待处理数，跳转至威胁告警页面查看详情。

支持点击热门威胁事件数，跳转至威胁事件评估页面查看详情。

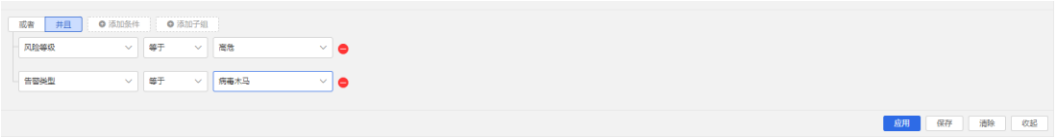
8.2.2.EDR 策略

EDR 基础版是通过终端本地行为分析引擎对终端的行为数据进行异常检测，因此威胁的检测和溯源会依赖于病毒防护业务的底层能力，管理员需在病毒防护策略中开启主动防御和实时防护功能设置。

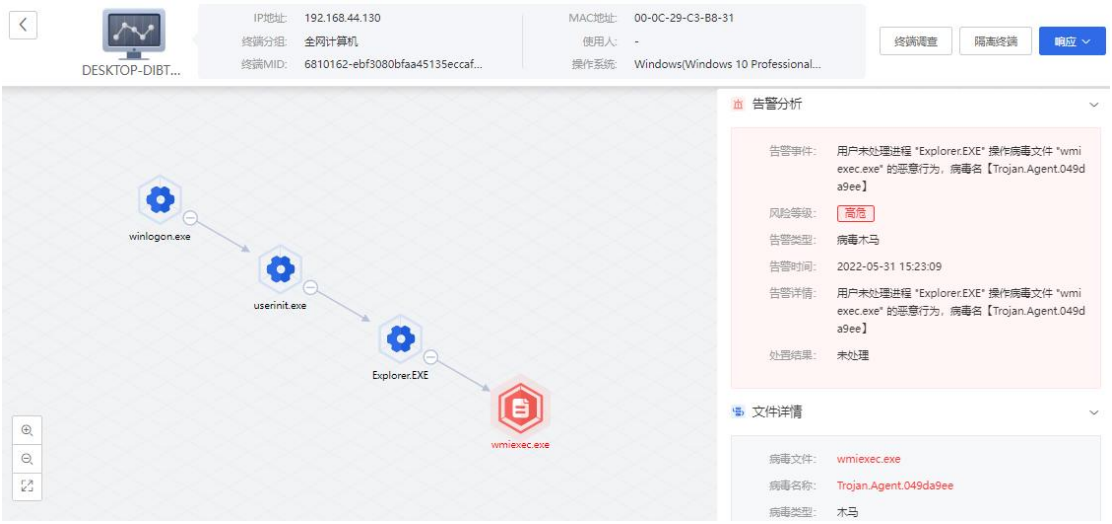
8.2.3.威胁告警

通过终端本地行为分析引擎对终端的行为数据进行异常检测，发现威胁行为后将在威胁告警页面产生告警进行提示，通过此告警方式反馈给安全管理人员。告警列表展示的信息包括风险等级、告警类型、告警详情等，点击查看详情后，能够展示具体告警的进程，及进程的上下父子进程信息，并通过进程树的可视化帮助分析人员对威胁进行追踪溯源，确认问题的根源。

对于威胁告警列表中的告警，产品也提供了丰富的筛选条件，同时关联筛选条件可以更加灵活，帮助安全人员快速找到自己关注的告警内容。



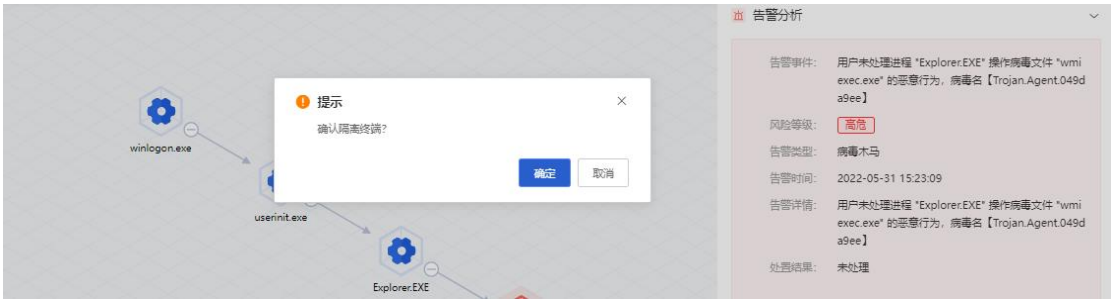
点击查看详情，能够展示具体告警的进程，及进程的上下父子进程信息。通过进程树的可视化帮助分析人员对威胁进行追踪溯源，确认问题根源以及该恶意行为带来的影响。



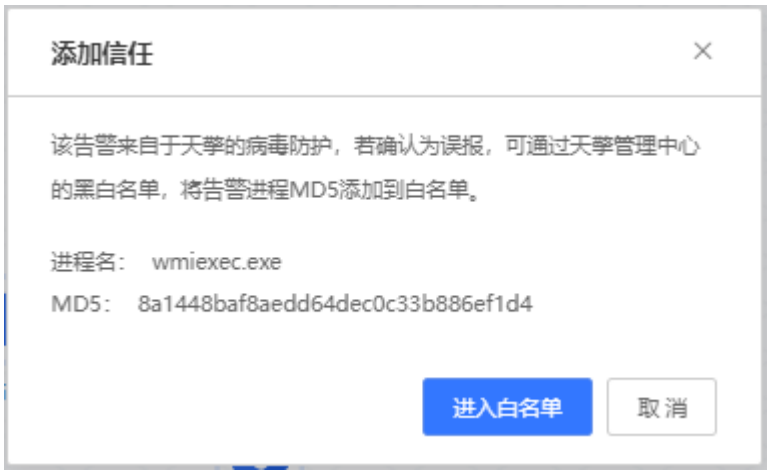
同时可通过快捷按钮对异常终端进行远程调查、威胁处置及对当前异常告警处理状态进行标记。

点击“终端调查”按钮可跳转到终端调查页面快速下发调查任务，帮助分析人员远程即可对异常终端进行问题排查及定位，减少远程安全运维成本。

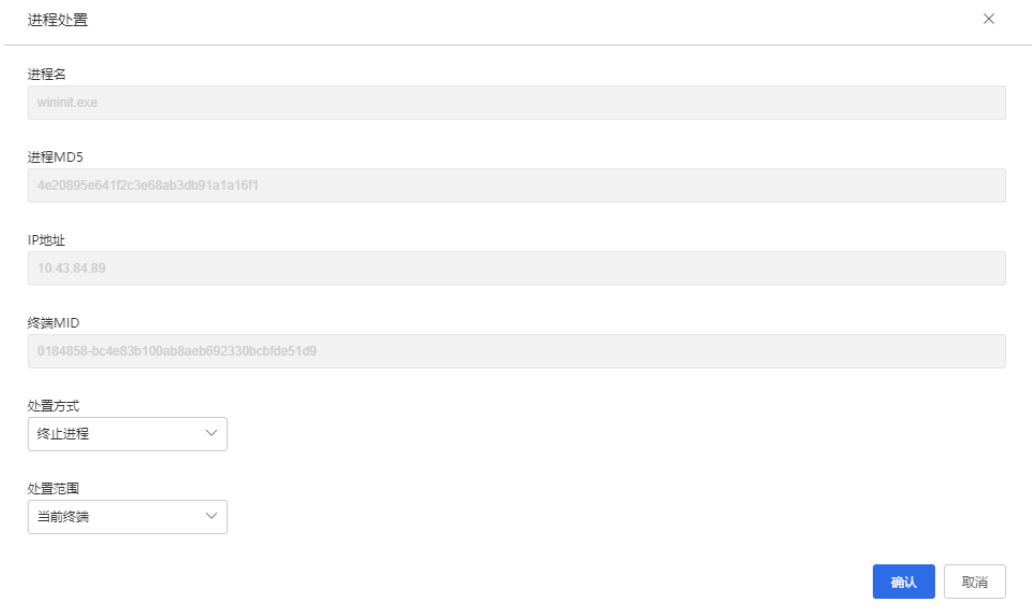
点击“终端隔离”按钮可对终端进行断网操作，只允许与管理中心进行通讯，以避免影响其他终端，进而扩大安全事件影响范围。



点击“响应”按钮可标记当前告警的处理状态，状态包含跟进中、确认威胁、添加信任。如需对告警文件进行信任，需跳转到病毒防护业务中的白名单页面添加文件 MD5 进行信任。



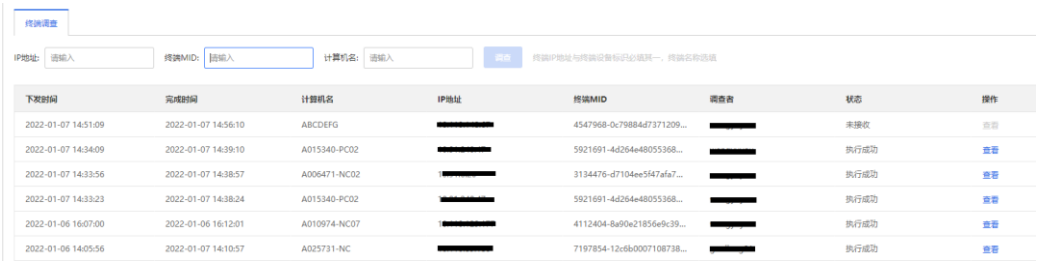
点击“进程处置”按钮可对单台终端或全网终端的进程进行处置，处置动作包含终止进程、终止进程并隔离、终止进程删除、恢复隔离进程文件。



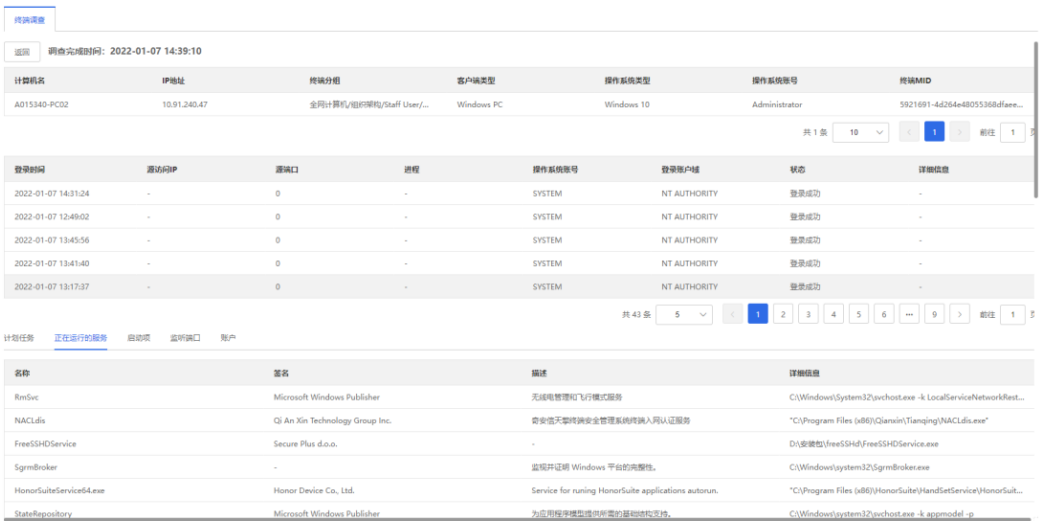
8.2.4. 终端调查

调查，这里专门指对指定终端当下的状态进行深入调查，获取最新的安全状况，包括终端登录日志、启动项、计划任务、正在运行的服务等，帮助分析人员远程即可对异常终端进行问题排查及定位，减少远程安全运维成本。

管理员可输入终端 IP 地址或终端设备标识下发终端调查任务。



当终端调查完成后，点击查看详情，能查看具体详细信息。



8.2.5. 威胁处置

当发现终端有异常行为存在安全风险时，安全人员需要通过处置进程或隔离终端的方式对该终端存在的威胁进行处置。

终端隔离：需要对该终端进行断网操作，只允许与管理中心进行通讯，以避免影响其他终端，进而扩大安全事件影响范围。

【注意】终端隔离会中断该用户所有需要联网的业务，建议仅在明确终端隔离原因的前提下再对指定终端下发该任务，必要时请提前联系该用户说明情况和原因。并且，若对

安装了天擎客户端的关键网络设备和天擎服务器下发终端隔离任务，可能导致全网天擎能力失效或全网通信故障，建议仔细审核终端隔离对象后再下发。

处置进程：终止进程、终止进程并隔离、终止进程删除、恢复隔离进程文件、禁止进程运行、取消进程拦截。

【注意】进程处置可按选定的处置方式对指定正在运行的进程执行处置，若处置了关键系统进程，可能造成系统崩溃或无法开机，建议仔细审核进程对象，谨慎选择批量和全网下发。

网络阻断：对访问恶意 IP 的网络连接行为进行阻断。

【注意】网络阻断将下发策略持续中断终端与指定 IP、端口和协议的通信，若该 IP 为关键网络设备或天擎服务器，可能导致与天擎失联、故障或网络无法访问，建议仔细审核网络地址对象后再下发。

8.3. 高级版基本功能

8.3.1. 威胁概况

全网终端安全态势可视化展示，实时展示威胁告警、热门威胁事件和威胁处置情况，自动分析全局风险等级，帮助客户掌握全网终端安全态势，提升安全管理能力。

支持点击告警数、待处理数，跳转至威胁告警页面查看详情。

支持点击热门威胁事件数，跳转至威胁事件评估页面查看详情。

8.3.2. 攻击图谱

可视化展示威胁告警在 MITRE ATT&CK 攻击模型中的覆盖情况，方便用户直观了解攻击者所应用攻击战术点和技术点，进而评估出攻击所处阶段和影响范围。

点击攻击技术点可查看技术编号，同时支持跳转至威胁告警页面查看告警事件详情。

8.3.3.EDR 策略

8.3.3.1. 终端数据采集

Windows 终端、Windows Server：开启终端数据采集策略，EDR 会对终端进程行为进行采集，并上报到终端大数据分析平台。采集的终端进程行为数据类型包括进程事件、IP 访问、DNS 访问、进程注入、注册表变更、文件操作、账户变更、邮件附件传输、U 盘文件传输、IM 文件传输、下载工具文件传输、浏览器文件传输、PowerShell 命令执行、命名管道事件、进程权限信息、WMI 事件、驱动文件加载、映像文件加载、无文件脚本执行、内网横向渗透、内存执行事件、账户登录登出、病毒防护事件。

管理员可通过在威胁检测与响应策略>数据采集配置页面自定义选择 EDR 在终端采集的数据类型。

Linux 服务器、信创终端和信创服务器：开启终端数据采集策略，EDR 会对终端进程行为进行采集，并上报到终端大数据分析平台。采集的终端进程行为数据类型包括进程事件、IP 访问、DNS 访问、U 盘文件传输、U 盘挂载/卸载、浏览器文件传输、文件操作、账户信息变更、账户操作、驱动加载/卸载、映像文件加载。

管理员可通过在威胁检测与响应策略>数据采集配置页面自定义选择 EDR 在终端采集的数据类型。

8.3.3.2. 采集排除设置

针对符合特定条件的数据，管理员可通过在威胁检测与响应策略>采集排除设置页面中进行管理，命中的终端日志数据将会被过滤，不会上报到管理中心。目前支持对全部类型数据的进程路径进行采集排除。

支持分别对各类型的终端行为数据，通过配置排除的条件进行采集排除。

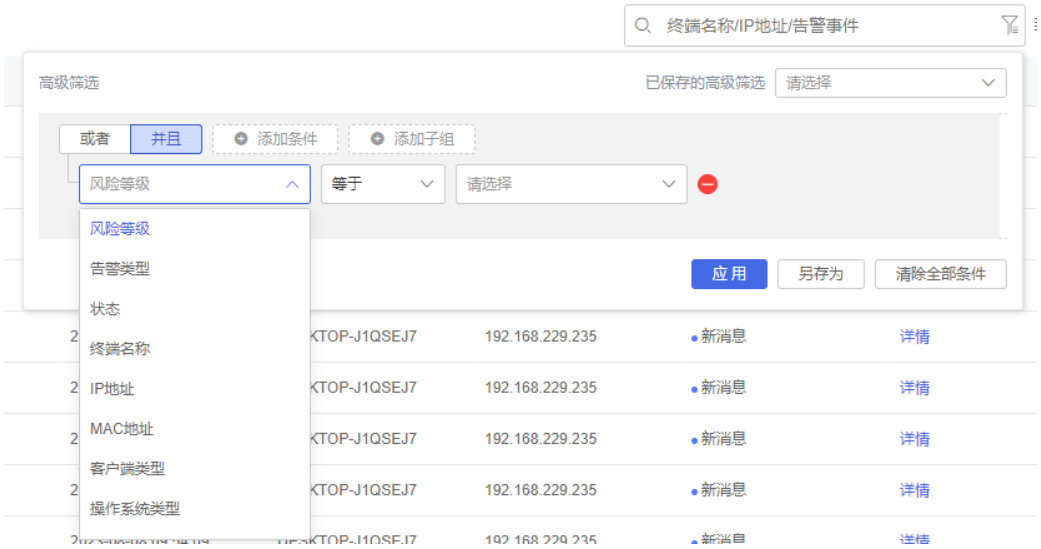
8.3.4. 威胁告警

通过分布式关联分析检测引擎 Sabre 自动对终端采集到的进程行为数据进行异常检测，发现威胁行为后将在威胁告警页面产生告警进行提示，通过此告警方式反馈给安全管理人员。告警列表展示的信息包括风险等级、告警类型、告警详情、技术点、战术点等，点击查看详情后，能够展示具体告警的进程，及进程的上下父子进程信息，并通过进程树的可视化帮助分析人员对威胁进行追踪溯源，确认问题的根源。

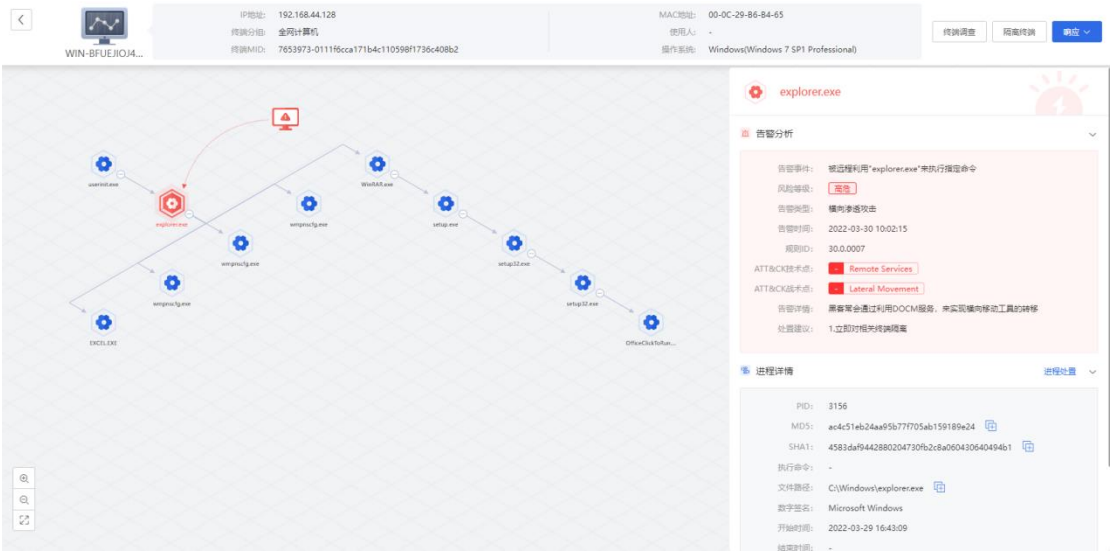
对于威胁告警列表中的告警，产品也提供了丰富的筛选条件，同时关联筛选条件可以更加灵活，帮助安全人员快速找到自己关注的告警内容。

可以对风险等级、状态、客户端类型进行快捷筛选。

可以对更多条件进行高级筛选。



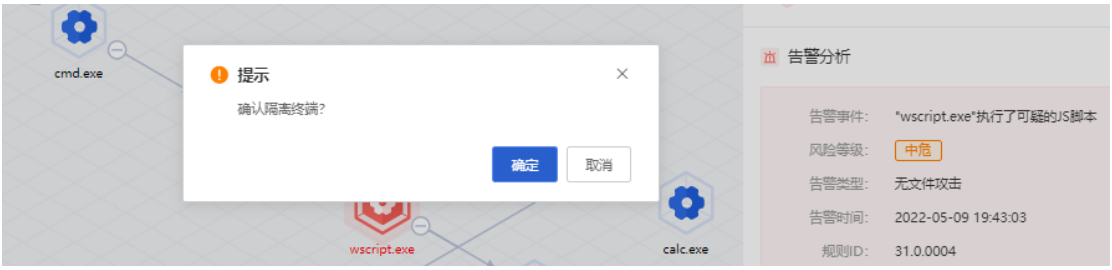
点击查看详情，能够展示具体告警的进程，及进程的上下父子进程信息。通过进程树的可视化帮助分析人员对威胁进行追踪溯源，确认问题根源以及该恶意行为带来的影响。



同时可通过快捷按钮对异常终端进行远程调查、威胁处置及对当前异常告警处理状态进行标记。

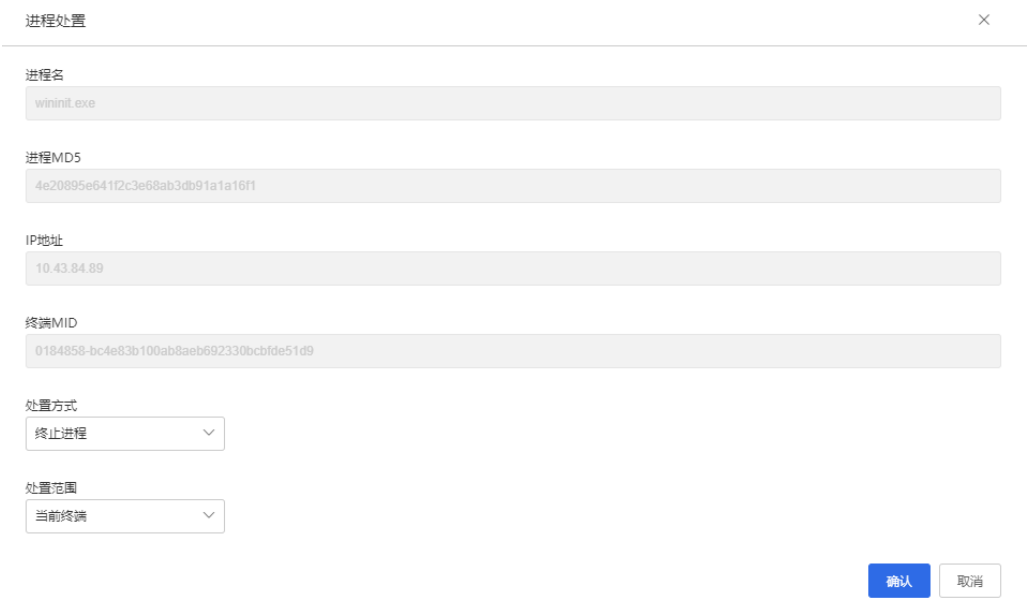
点击“终端调查”按钮可跳转到终端调查页面快速下发调查任务，帮助分析人员远程即可对异常终端进行问题排查及定位，减少远程安全运维成本。

点击“终端隔离”按钮可对终端进行断网操作，只允许与管理中心进行通讯，以避免影响其他终端，进而扩大安全事件影响范围。



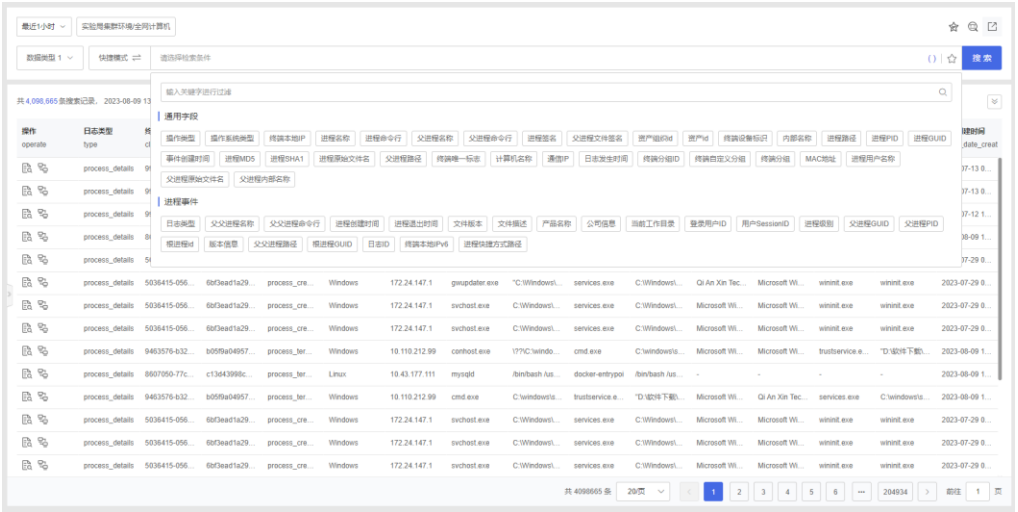
点击“响应”按钮可标记当前告警的处理状态，状态包含跟进中、确认威胁、添加信任。

点击“进程处置”按钮可对单台终端或全网终端的进程进行处置，处置动作包含终止进程、终止进程并隔离、终止进程删除、恢复隔离进程文件。



8.3.5. 威胁追踪

基于对终端数据不断采集、监测，并结合成熟的大数据运营经验，管理员可以通过威胁追踪的数据聚合筛选、日志检索等方式，在特定的时间范围、特定的数据范围内，模糊或精确的检索自身所关心的上下文，主动发现威胁活动线索并进行追踪，最终核实安全威胁。

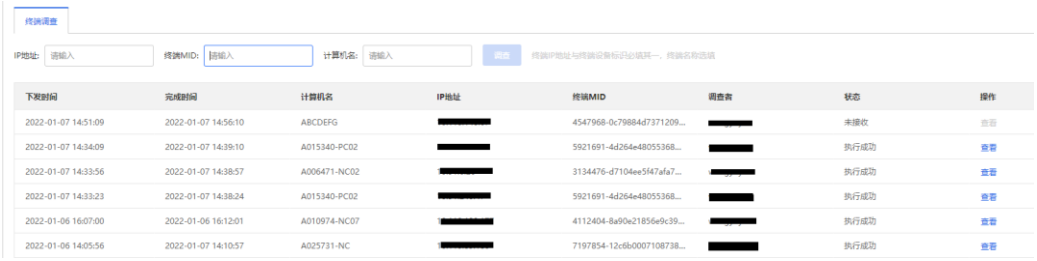


可以点击每个数据的左侧溯源按钮，对每条日志的进程链进行溯源。

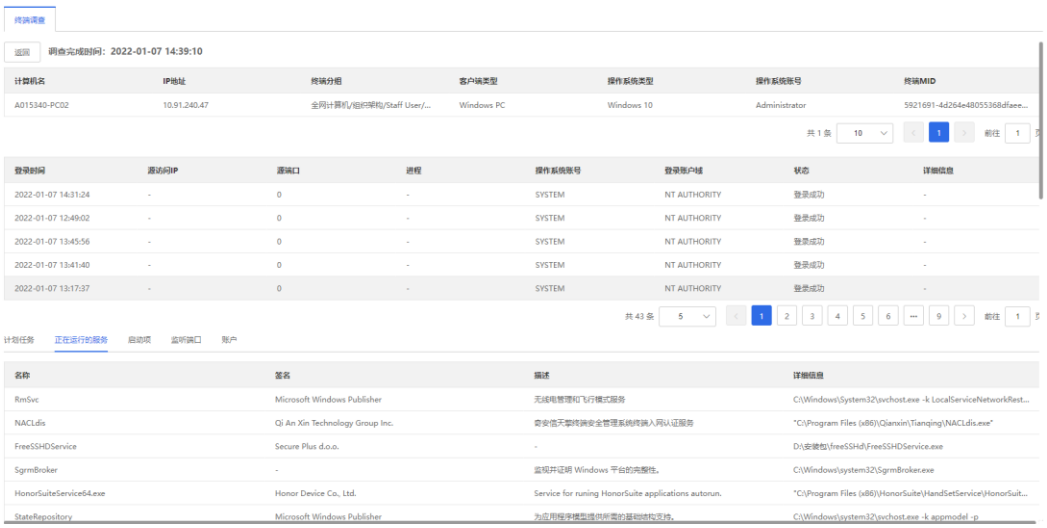
8.3.6. 终端调查

调查，这里专门指对指定终端当下的状态进行深入调查，获取最新的安全状况，包括终端登录日志、启动项、计划任务、正在运行的服务等，帮助分析人员远程即可对异常终端进行问题排查及定位，减少远程安全运维成本。

管理员可输入终端 IP 地址或终端设备标识下发终端调查任务。



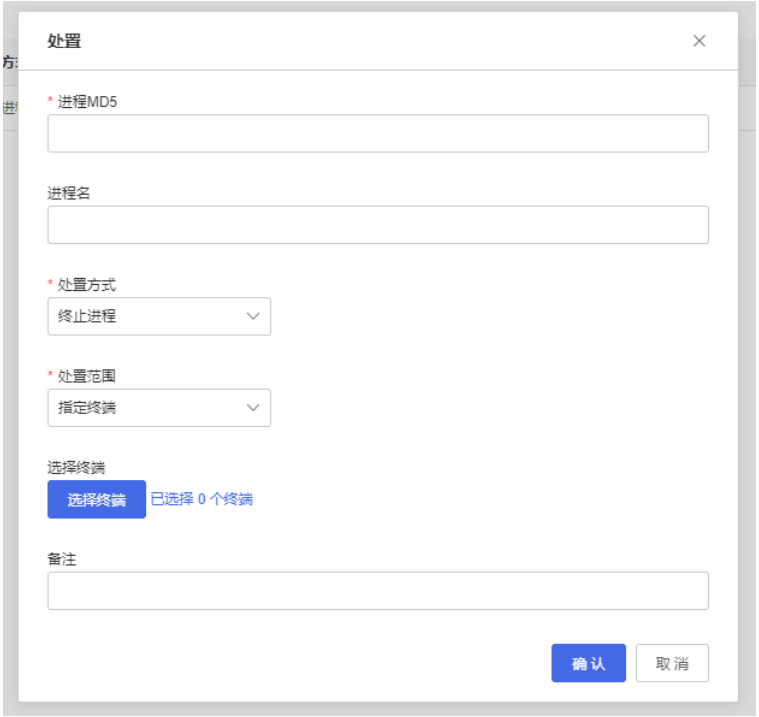
当终端调查完成后，点击查看详情，能查看具体详细信息。



8.3.7.威胁处置

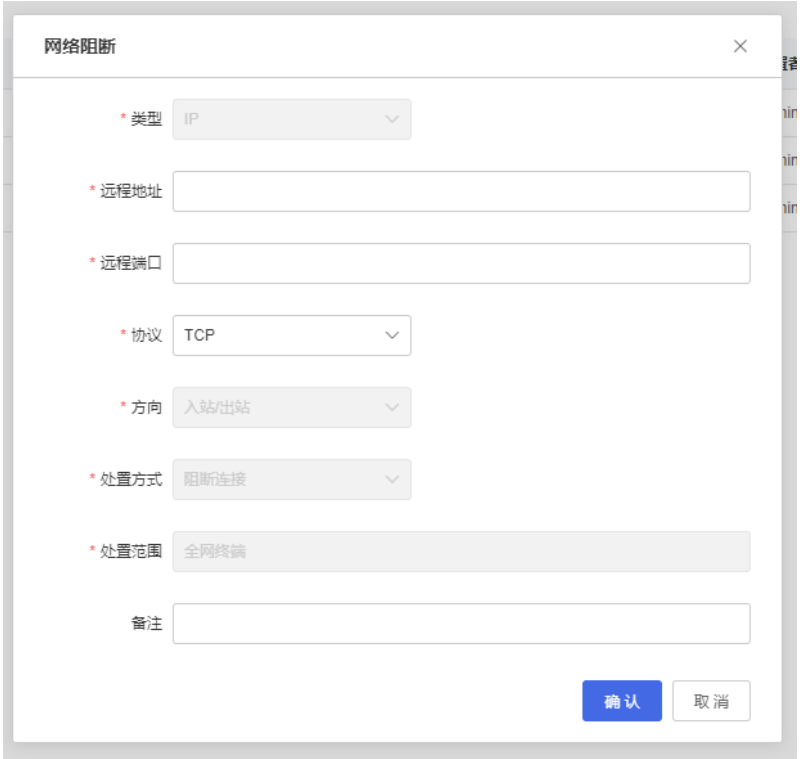
当发现终端有异常行为存在安全风险时，安全人员需要通过处置进程或隔离终端的方式对该终端存在的威胁进行处置。

进程文件：需要对文件或进程进行处置的时候，可以通过该功能添加处置规则。通过该功能增加。通过添加进程或文件 MD5、进程名、添加处置方式（处置方式包括：终止进程、终止进程并隔离、终止进程并删除、恢复隔离进程文件、禁止进程运行、取消进程拦截）、处置范围（可以选择指定终端、全网终端）。



【注意】进程处置可按选定的处置方式对指定正在运行的进程执行处置，若处置了关键系统进程，可能造成系统崩溃或无法开机，建议仔细审核进程对象，谨慎选择批量和全网下发。

网络阻断：该功能可以添加网络地址，通过添加的网络地址实现阻断相关网络地址。可以在发现恶意网络访问的情况下，快速阻断相关恶意地址的访问。



【注意】网络阻断将下发策略持续中断终端与指定 IP、端口和协议的通信，若该 IP 为关键网络设备或天擎服务器，可能导致与天擎失联、故障或网络无法访问，建议仔细审核网络地址对象后再下发。

终端隔离：需要对该终端进行断网操作，只允许与管理中心进行通讯，以避免影响其他终端，进而扩大安全事件影响范围。

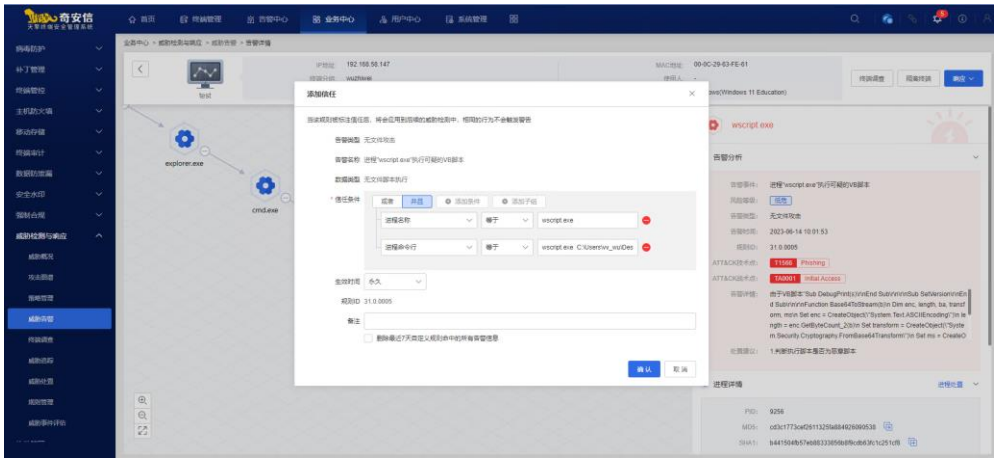
【注意】终端隔离会中断该用户所有需要联网的业务，建议仅在明确终端隔离原因的前提下再对指定终端下发该任务，必要时请提前联系该用户说明情况和原因。并且，若对

安装了天擎客户端的关键网络设备和天擎服务器下发终端隔离任务，可能导致全网天擎能力失效或全网通信故障，建议仔细审核终端隔离对象后再下发。

8.3.8. 告警规则信任

当安全分析人员对威胁告警详情进行分析后，确认威胁告警存在误报的情况，可通过威胁告警>告警详情>响应>添加信任快速对产生误报的威胁告警规则进行添加信任处理。

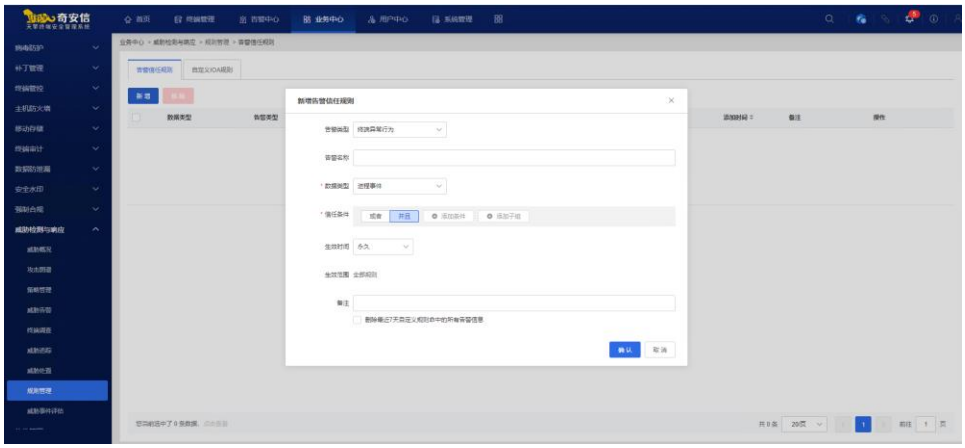
添加规则成功后，将会应用到后续的威胁检测中，相同的行为将不会再次触发告警。添加时，可对信任条件进行自定义。



在告警中添加信任时，也支持用户进行自定义编辑条件，满足运营人员对误报告警的多场景处理。

对告警规则添加信任后，可通过信任规则>规则管理列表查看当前处于信任的规则，同时支持对已添加信任的规则进行编辑、查看详情、删除操作。

支持信任规则自定义。支持用户自定义编辑信任规则，可灵活配置规则条件，支持通配符匹配及 AND、OR、NOT 的逻辑操作，有效解决误报告警问题，应用规则后不会再产生误报告警。



信任告警规则后，当出现相同告警类型、相同数据类型、相同信任条件、相同规则 ID 的行为时，将不再告警。

8.3.9. 自定义规则

安全运营人员可通过规则管理>自定义规则可视化页面自定义创建规则、编辑规则、发布规则、删除规则，同时支持以进程事件、IP 访问、DNS 访问、进程注入、注册表变更、文件操作、账户变更、邮件附件传输等行为作为检测特征编写规则实体，对内置规则未覆盖的场景进行补充检测。

创建规则需填写规则属性和告警属性。

规则属性：需选择数据源，并添加规则条件；规则编写支持通配符匹配；规则编写字符串值支持中文；规则编写支持 AND、OR、NOT 的逻辑操作。

告警属性：需填写风险等级、告警类型、告警名称、告警详情，当关联分析引擎基于自定义规则检测到告警后在威胁告警页面进行展示。

8.3.10. 威胁事件评估

奇安信威胁情报中心根据云端收集到的攻击情报信息，构建安全事件知识库，对新爆发的热点安全事件快速响应，并通过云端对奇安信天擎客户推送威胁事件库。

通过定期推送热点安全事件，主动帮助管理员对全网终端进行风险扫描评估，评估出受安全事件影响的终端范围，并可对风险终端进行快速处置。

点击威胁事件列表中的威胁事件名称，可展示威胁事件详情，帮助管理员对该威胁事件有基本的认知。

支持批量对风险终端下发处置任务，一键自动清除威胁，并将处置结果告知管理员。

9. 安全登录

本章介绍安全登录产品模块的使用方法，该产品的使用需要购买相应授权。

9.1. 基本概念

安全登录，是用户向系统以一种安全的方式提交自己的身份信息，然后由系统确认用户的身份是否属实的过程，而“安全”的含义就是对登录的用户进行更为复杂的身份鉴别，这种复杂性不仅是加强密码的长度与复杂度，而是增加了硬件 UKEY，并把 UKEY 与用户身份信息绑定，在登录系统时强制插入 UKEY，通过校验 UKEY 签名来完成安全登录。

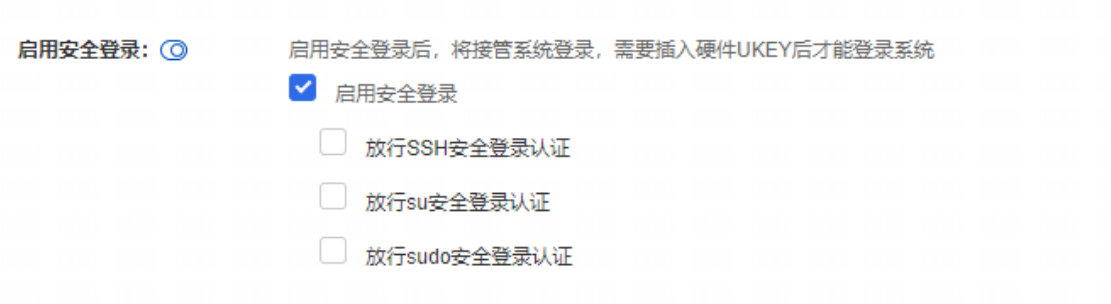
9.2. 安全登录的设置项

- 启用安全登录

默认不启用，管理员启用后，且管理员执行了用户与终端设备的绑定操作，终端才启用安全登录。

终端安全登录接管系统登录，前提条件是：

1）管理员下发了启用安全登录策略；
2）终端接收到控制中心的绑定信息。



启用安全登录后，管理员可根据实际使用场景，是否放行 SSH 安全登录认证、是否放行 su 安全登录认证、是否放行 sudo 安全登录认证。

注意：启用安全登录后，终端必须使用 UKEY+PIN 码的方式才可登录终端，只使用 PIN 码或者原有的操作系统登录密码无法登录系统。

- 拔 UKEY 响应设置：

终端根据策略设置执行相应的操作，支持拔 UKEY 锁屏、拔 UKEY 注销系统、拔 UKEY 重启系统。

➢ UKEY 密码设置

管理员可以设置 PIN 码的有效期，以及 PIN 码的复杂度，PIN 码的强度。

➢ 屏幕超时设置

管理员可以设置屏幕超时时间，超时后，自动锁屏。需注意的是调整超时时间后，终端需要注销或重启系统，调整后的时间才能生效。

➢ UKEY 锁定设置

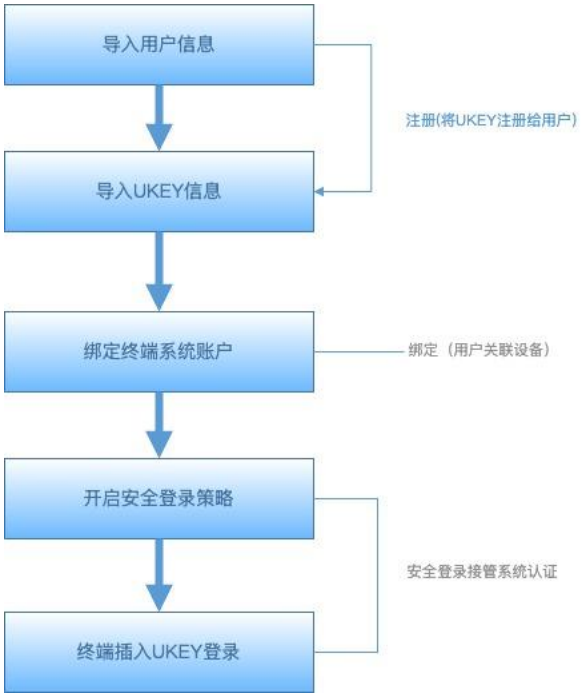
管理员可以设置 UKEY 登录的验证次数，当超过设置次数后，该 UKEY 被锁定，锁定后的 UKEY 必须解锁才能使用**（此功能受限于 UKEY，部分厂商 UKEY 无法解锁，需要使用 UKEY 厂商提供的解锁工具解锁）**

➢ 临时口令设置

管理员可以设置临时口令的有效期和口令允许的错误次数。

9.3. 安全登录使用流程

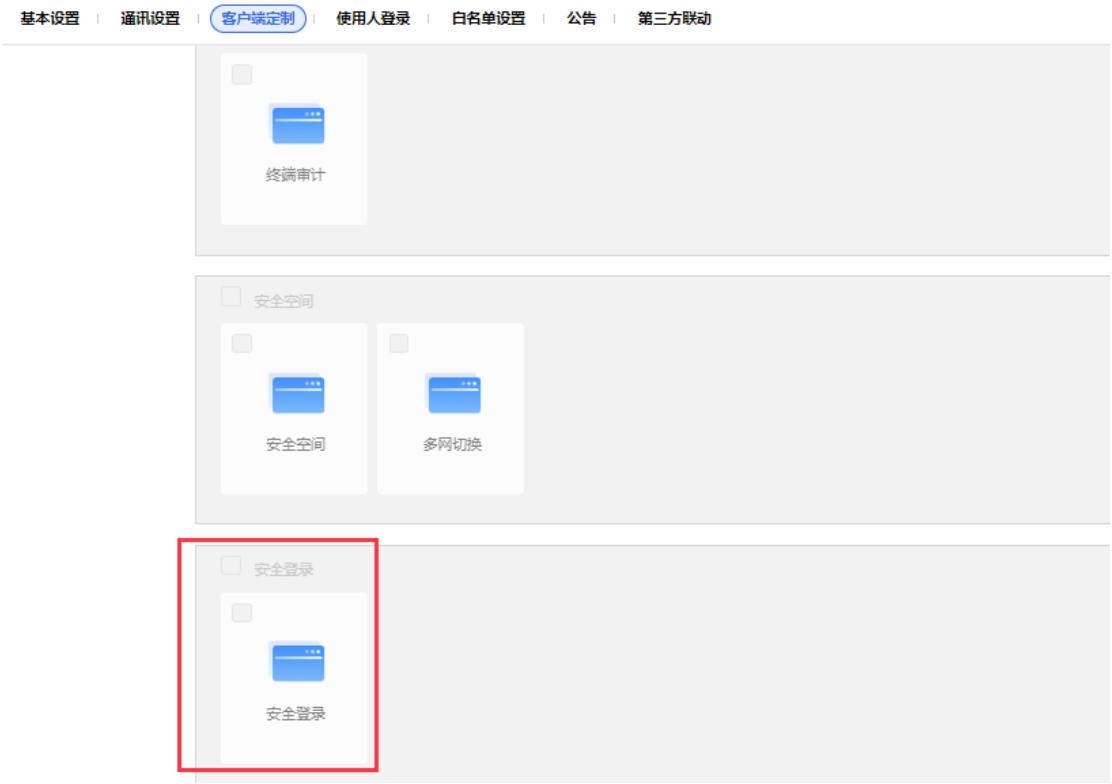
下面是安全登录模块默认支持的龙脉厂商 UKEY（型号：GM3000）的使用流程：



如果是证书认证的 UKEY，且有对应的用户系统使用流程稍有差异，因证书中已经带有用户信息，则省去了上述流程的注册操作。

➢ 准备工作

配置策略：资产管理 >终端管理 >基础策略 >客户端定制>安全登录，勾选安全登录模块。



➢ 新建/导入用户信息

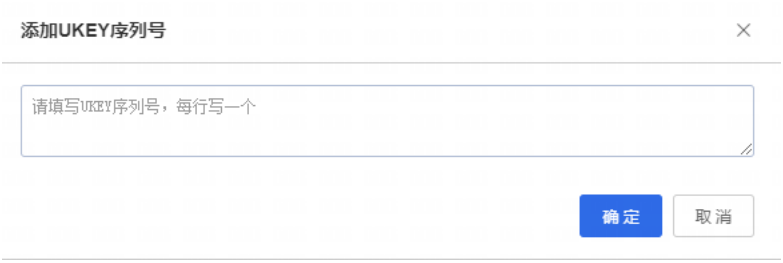
登录控制中心管理员账户，在用户中心>用户页面，点击[导入]按钮。

点击[下载模板]，可以按照模板准备需要导入的信息，然后将准备好的文件导入进控制中心。也可以通过点击添加按钮，按照要求填写相应的信息，添加用户。

➢ 导入 UKEY 信息

在数据安全>安全登录>UKEY 管理页面中点击[添加]按钮。

弹出如下对话框：

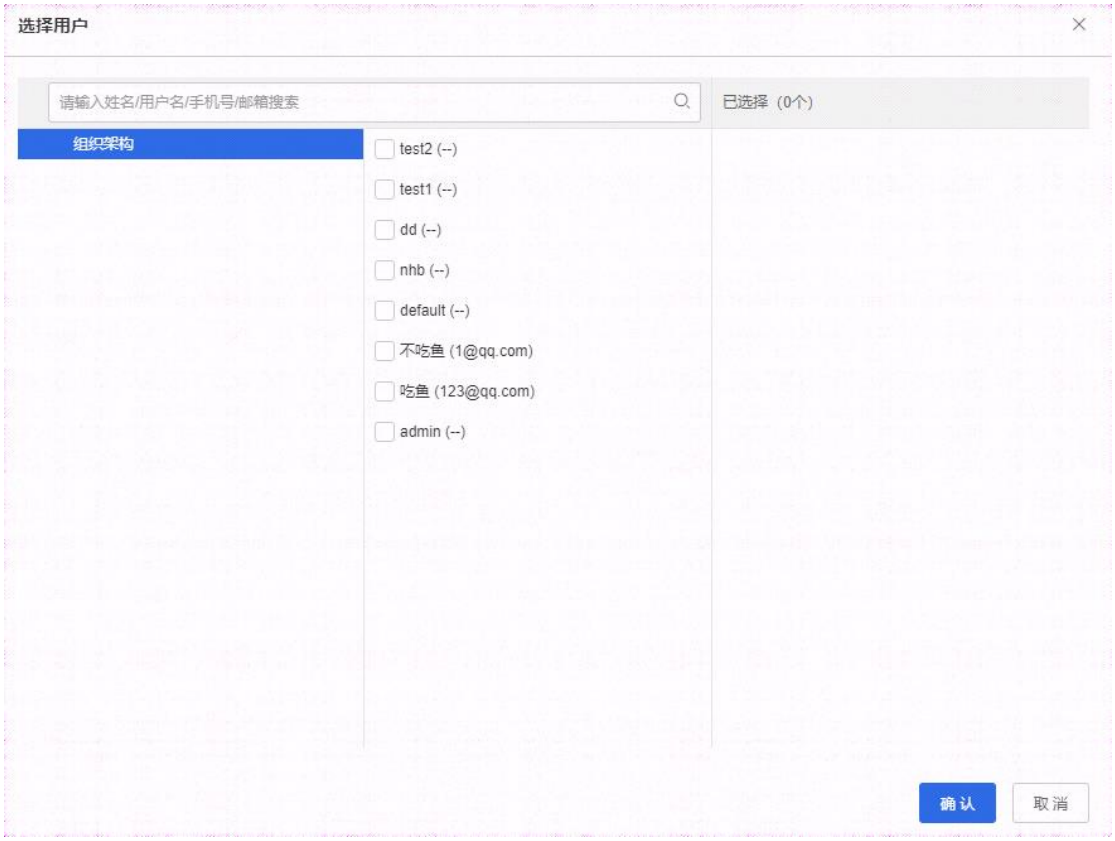


填写正确的 UKEY 序列号（UKEY 外面的数字就是 UKEY 的序列号），支持多行填写，一行视为一个 UKEY 序列号。

➢ UKEY 注册

进入业务管理>安全登录>UKEY 管理，选择未注册的 UKEY 序列号，点击[注册]按钮，弹出如下对话框：

点击[请选择用户]后：

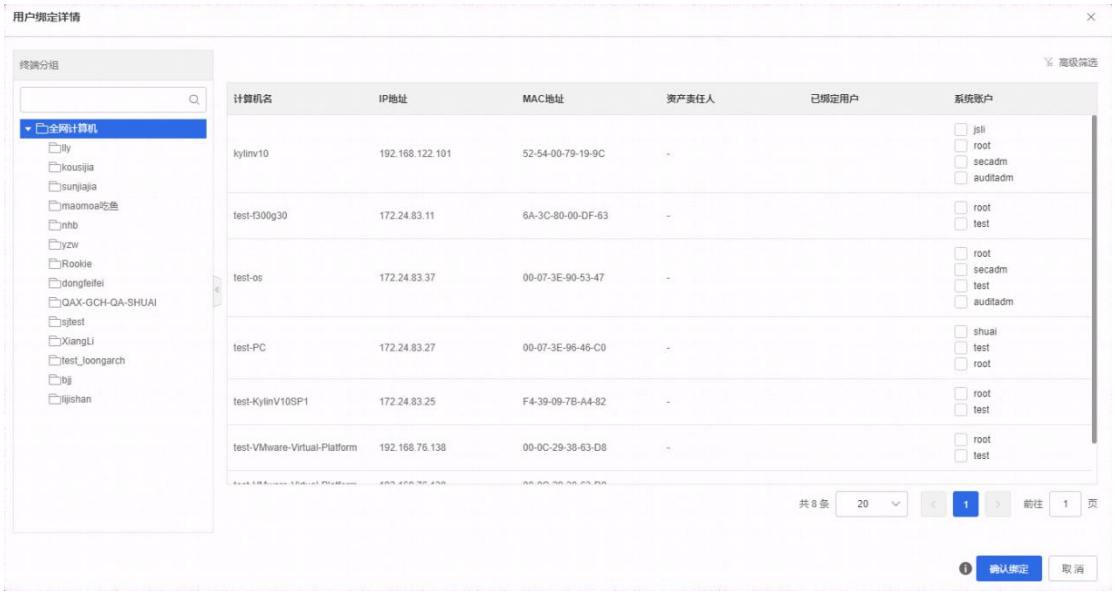


选择完用户后，完成 UKEY 的注册。

- 绑定终端系统账户

路径：业务管理>安全登录>终端绑定，点击[绑定终端]按钮。

弹出如下页面，选择想要绑定的系统账户即可完成绑定。



完成绑定后，保证系统的安全登录策略是开启的，即可实现在终端登录使用UKEY 认证的方式登录系统。

9.4. 典型场景

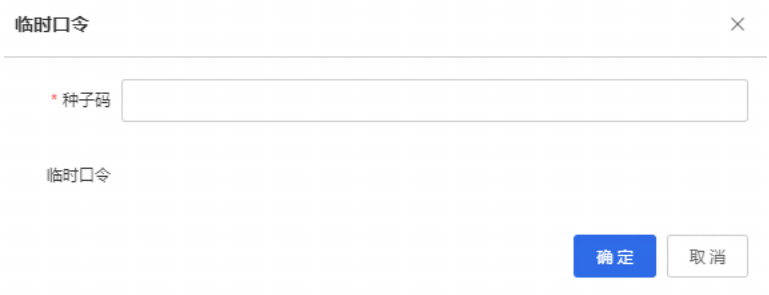
9.4.1.UKEY 损坏、网络不通如何应急登录

逃生手段：临时口令

当 UKEY 因丢失、损坏无法使用时，而 UKEY 的补发需要个时间过程，应具备临时登录手段，来处理应急事情。操作方法如下：

在登录页面输入：zhimakaimen，界面会提示种子码，把这个种子码发送给管理员。

管理管登录控制中心后，进入业务管理-安全登录-终端绑定-生成临时口令，管理员再把临时口令下发给用户，终端即可用临时口令登录设备。需注意临时口令再策略中是可以进行有效期及尝试次数的策略设置。



9.4.2. 非龙脉厂商 UKEY 能使用安全登录吗？

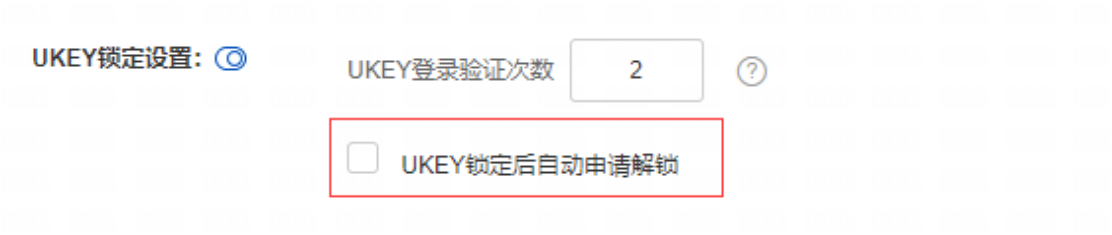
目前安全登录模块具备完善的技术架构来根据用户需要快速适配不同厂商的 UKEY，如渔翁、飞天、吉大正元、意源、海泰等。

9.4.3. UKEY 被锁定了如何处理?

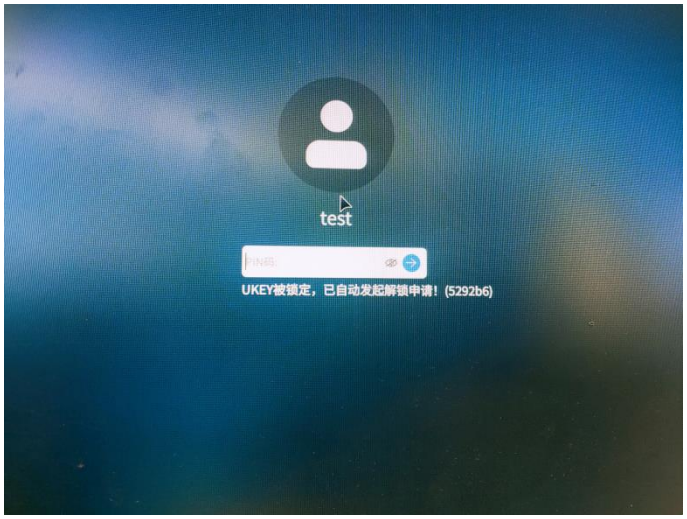
安全登录的 UKEY 在输入错误的 PIN 码达到一定的次数后会被锁定，UKEY 被锁定后，需要管理员配合将 UKEY 进行解锁，可选择两种方式进行解锁，分别是：

1. 由用户在终端发起申请或者在策略中设置了自动发起解锁申请，管理员在控制中心进行审批；
2. 由分级管理员操作在终端侧进行解锁；

如果用户选择方式一，由控制中心管理员审批解锁，在管理员在业务管理-安全登录-UKEY 审批页面下进行审批，审批通过后，即可完成 UKEY 的解锁，管理审批解锁的过程中，需要 UKEY 插入在机器上；如果想要设置自动发起解锁申请，可通过在安全登录的策略中设置中勾选自动发起解锁申请。界面如下：



当设置了自动发起解锁申请后，当终端 UKEY 被锁定后，会自动发起解锁申请。



终端自动发起解锁申请后，管理员在业务管理-安全登录-UKEY 审批页面下可对 UKEY 解锁申请进行审批通过/审批拒绝。审批通过 UKEY 解锁申请或者重置 PIN 码的申请后，则 UKEY 的 PIN 码会被重置为 12345678，使用新的 PIN 码后，可登录终端，对于初始的 PIN 码可通过修改 PIN 码的功能进行修改。

UKEY序列号	申请类型	申请人	联系电话	计算机名	终端账户名	终端分组	IP地址	申请提交日期	审批状态	审批完成时间	操作
200815630	重置PIN码	test01	222	-	test	-	-	2022-10-19 17:48:15	已拒绝	2022-10-19 17:48:24	同意 | 拒绝
200815630	解除锁定	test01	-	-	test	-	-	2022-10-19 17:44:15	已通过	2022-10-19 17:47:03	同意 | 拒绝
200815630	重置PIN码	test01	788989	-	test	-	-	2022-10-19 17:36:38	已通过	2022-10-19 17:36:45	同意 | 拒绝
200815630	重置PIN码	test01	333	-	test	-	-	2022-10-19 17:31:18	已通过	2022-10-19 17:31:43	同意 | 拒绝
200815630	重置PIN码	test01	12222	-	test	-	-	2022-10-19 17:30:06	已通过	2022-10-19 17:30:17	同意 | 拒绝
57447B50C8AC0F...	解除锁定	maomao	asa	-	test	-	-	2022-10-14 14:32:20	已通过	2022-10-14 14:55:30	同意 | 拒绝
57447B50C8AC0F...	重置PIN码	maomao	5475787	-	test	-	-	2022-10-14 10:48:38	已通过	2022-10-14 10:51:02	同意 | 拒绝
57447B50C8AC0F...	重置PIN码	maomao	55555	-	test	-	-	2022-10-14 10:48:32	已通过	2022-10-14 10:51:02	同意 | 拒绝
57447B50C8AC0F...	重置PIN码	maomao	787787	-	test	-	-	2022-10-14 10:48:28	已通过	2022-10-14 10:51:02	同意 | 拒绝
57447B50C8AC0F...	重置PIN码	maomao	312321	-	test	-	-	2022-10-14 10:48:22	已通过	2022-10-14 10:51:02	同意 | 拒绝

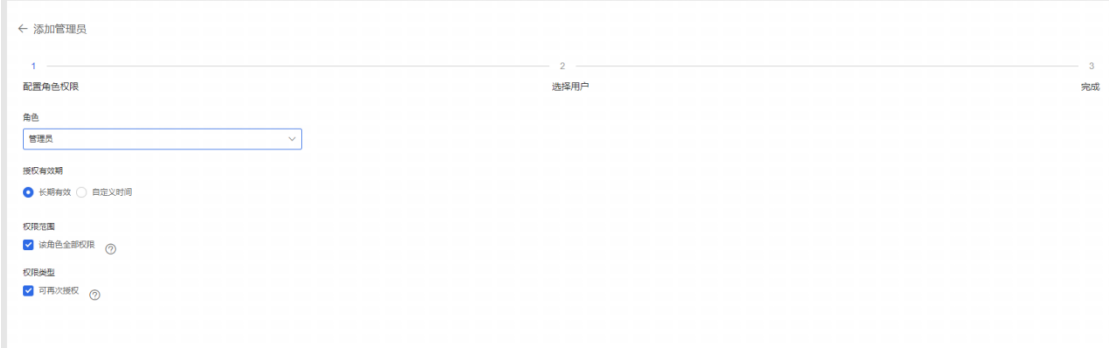
9.4.4.用户如果忘记了 UKEY 的 PIN 码如何处理？

用户忘记 UKEY PIN 码的处理流程和 UKEY 锁定的处理流程一致，管理员的具体的操作步骤可详见 UKEY 解锁的处理流程。

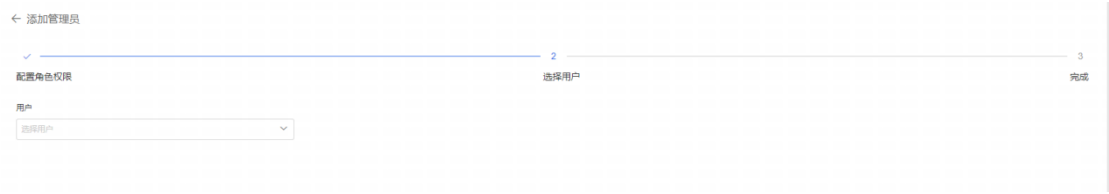
9.4.5.如何制作一把管理员 UKEY

进入用户中心>角色，点击[添加管理员]：

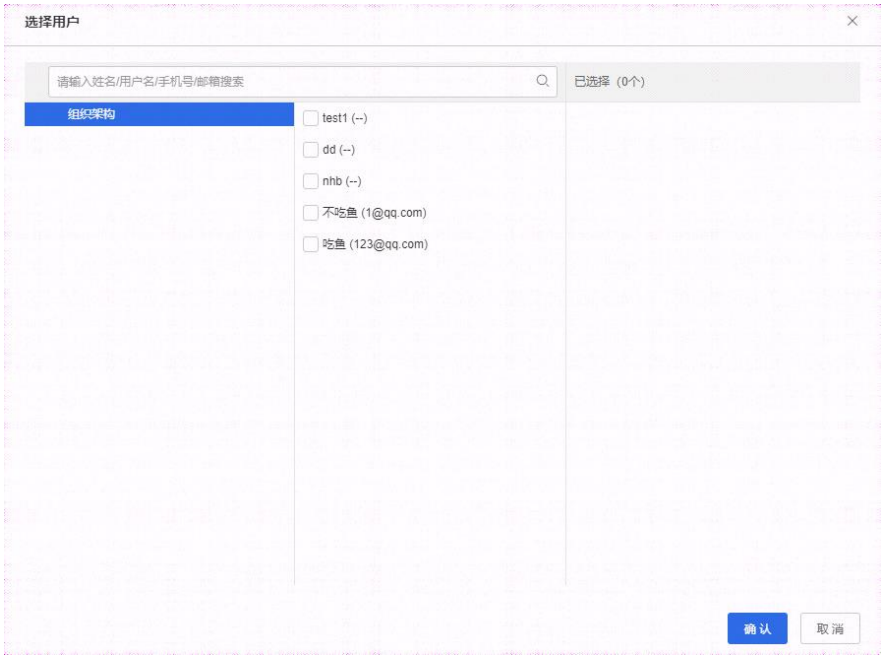
选择设置好的管理员角色，需注意，设置管理员角色的时候，通过设置管理员角色终端分组的权限实现不同管理员管理不同分组终端的功能。



点击[下一步]：



进入选择用户界面，选择用户后，则实现将该用户设置成管理员用户的功能。



管理员分组权限的设置：进入用户中心>权限>角色，配置子角色页面，对管理员的终端分组进行设置，实现管理员管理不同终端分组的功能。

在数据安全>安全登录>UKEY 管理页面，添加 UKEY，将新添加的 UKEY 注册给刚刚新建的管理员，则可以使用该管理员 UKEY 登录刚刚所设置的分组权限下的所有终端的所有账户。

10. 安全评估

10.1. 基本概念

10.1.1. 得分

得分：得分是基于每个评估项开启并配置的扣分标准后，经过策略或任务下发到终端逐项检查后，对不满足项按照配置的扣分标准和权重从 100 分进行扣分后，计算的最终得分，反映该终端的安全情况。

10.1.2. 评估类别

安全评估评估标准分为三大类，分别是：系统配置安全评估、系统状态安全评估、系统环境感知评估。每个评估大类下有多个检查项，比如 Window PC

下的登录失败限制、登录交互约束、本地身份防盗用等。每个检查项下由多个评估项组成。

10.1.3. 否决项

设置某一评估项为否决项，若终端针对该评估项评估不通过，则此评估项所在评估大类为 0 分。

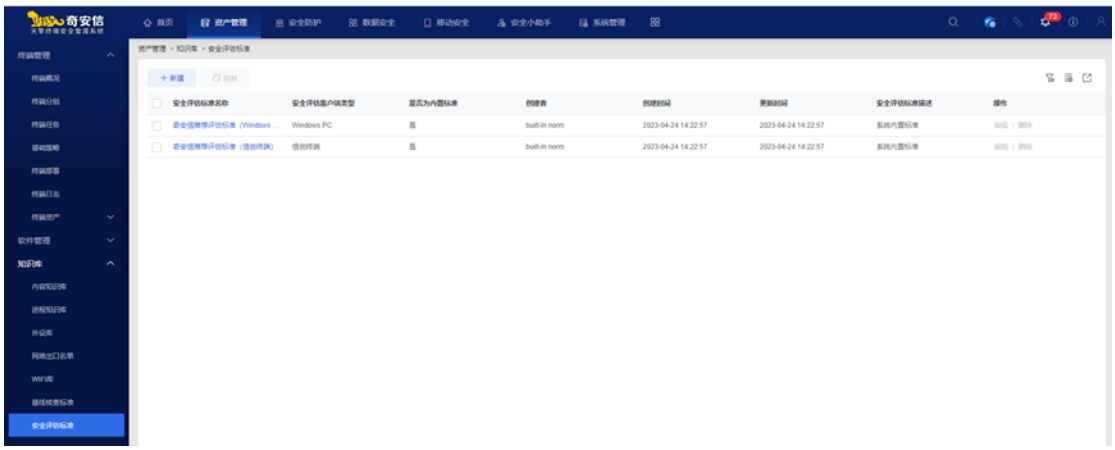
10.1.4. 定性标准

定性标准：基于评估项检查后上报的最终得分为终端的安全情况定性，支持按得分情况划分安全等级，在安全防护>安全评估 >业务设置进行定义。

安全级别：对终端评估的最终得分进行安全级别定义，目前为百分制，并分为 4 个级别：高危、中危、低危、安全。

10.1.5. 评估标准

什么是安全评估标准：收集等级保护 2.0、等级保护 3.0 等，形成评估项集合，在使用时根据实际情况按需定制评估模板。如下图：



10.2. 基本功能

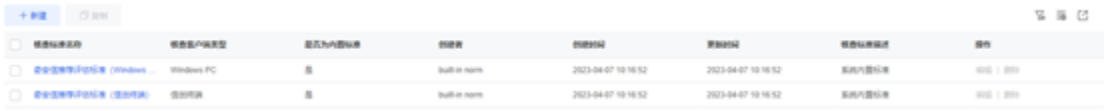
10.2.1. 安全评估业务设置

在安全防护>安全评估 >业务设置页面，可以基于得分配置终端的安全级别，如下图：

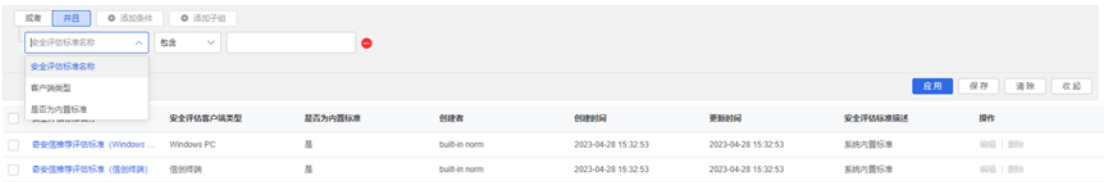
10.2.2. 安全评估标准

目前知识库内置有奇安信推荐评估标准（Windows PC）和奇安信推荐评估标准（信创终端），用户可以根据企业自身或行业要求自定义评估模板。在资产管理-知识库-安全评估标准页面，可以查看内置标准，并可以新建标准和复制标准；对于非内置的标准可以进行删除和编辑。

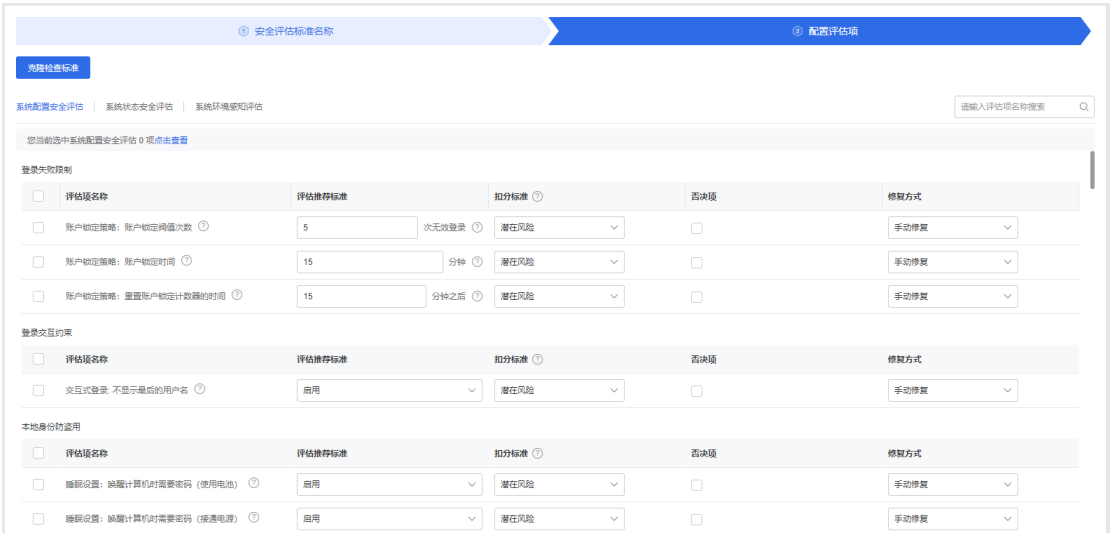
入口：资产管理-知识库-安全评估标准。



同时，支持通过名称、终端类型等不同条件筛选标准，支持导出标准列表。



通过新建/编辑可自定义安全评估的详细评估向项。



注意：当修复方式设置为自动修复后，会将终端按照设置的评估标准进行修改。如果评估标准设置的不合理，会对终端造成不可预知的问题。请谨慎设置。以下列出部分高频出现问题评估项：账户：重命名来宾账户、账户：重命名管理员账户、应禁用账户评估。

10.2.3. 安全评估概况

安全评估概况从终端视角展示全网终端（也可指定分组）当前的评估情况和评估项视角展示不同评估项的终端评估情况。

10.2.3.1. 终端视角

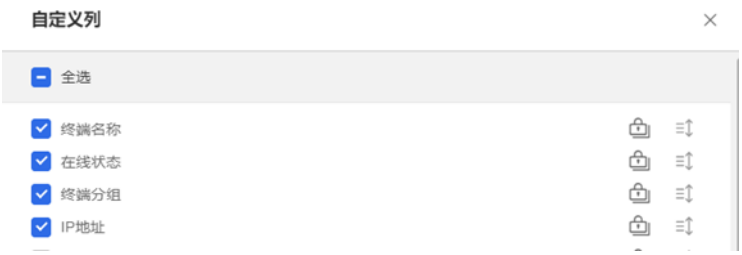
终端视角下展示通过项数、未通过项数、未评估项数、最新得分、是否设定授权人、最新评估时间等情况。根据终端名称/IP 地址/在线状态/终端类型和不同的分组等为查询条件，以帮助管理员快速找到对应的终端信息。

选中一个/多个终端可下发重新检查任务和即时消息。

入口：安全防护>安全评估>安全评估概况。

导出：可以选择导出安全评估概况信息安全评估详情信息：

自定义列：设置安全评估概况的自定义列情况：

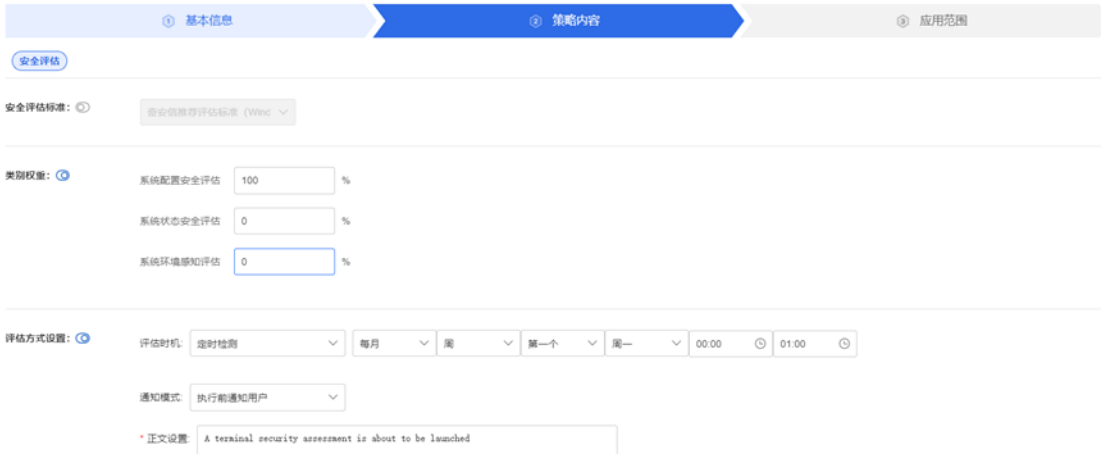


10.2.3.2. 评估项视角

评估项视角下展示不同的评估项的通过终端数/不通过终端数/未评估项数/更新时间。

10.3. 安全评估策略

在安全防护>安全评估>策略管理>编辑策略页面，可以安全评估评估标准、类别权重、评估方式设置、其他设置进行设置；配置完成后，点击“下一步”然后配置应用范围后点击“应用”，可以下发策略到对应分组终端。如下图：



10.4. 安全评估任务

在资产管理 >终端管理 >终端任务 >创建任务里下发安全评估任务，可以配置安全评估的评估标准/类别权重；配置完成后，下一步选择执行范围后下发终端执行。如下图：

10.5. 安全评估日志

安全评估日志是对指终端上报的安全评估结果日志的记录，支持展示上报的终端基础信息、检查时间、得分、通过项数、不通过项数、未评估项、安全等级等信息，并支持多种导出方式。

入口：安全防护 >安全评估 >安全评估日志。

10.6. 典型场景

10.6.1. 如何快速完成对终端的安全性及合规性标准检查？

使用内置的国家标准，或者提前定义好行业或者企业级标准评估模板，在需要及时检查时克隆检查标准并通过任务下发给终端快速完成检查。

10.6.2. 进程对应的软件升级后进程也发生变化，如何减少调整保证设置的黑白名单依然有效？

在软件使用过程中无法避免软件的更新可能导致我们配置的进程检查列表失效，因此在管理中心提供了基于不同维度的规则对检查进程进行归类；在终端管理-知识库-进程知识库可以对进程检查通过按产品名称、公司名称、启动路径、签名等来设置规则，或者基于某些规则对进程进行分组归类，在下发制定评估项的时开启了进程检查则选择对应规则或者进程组即可，当终端进程有变化时可以基于规则自动调整，或者基于分组手动调整后再下发即可。

10.6.3. 评估后发现问题后如何修复

管理中心提供了安全配置类的检查项和对应修复帮助文档；终端用户在安全评估的主界面可以打开查看。

10.6.4. 如何计算评估得分

如果管理员设置了如下的评估标准：

评估大类	检查项	评估项	扣分标准	是否否决项	评估结果
系统配置安全评估	登录失败显示	账户锁定策略：账户锁定阀值次数	潜在风险	否	通过
		账户锁定策略：账户锁定时间	一般风险	否	通过
		账户锁定策略：重置账户锁定计数器的时间	严重风险	是	不通过
	登录交互约束	交互式登录：不显示最后的用户名	潜在风险	否	不通过
系统状态安全评估	外设管控	蓝牙开启评估	严重风险	否	通过
	违规外联	互联网连接评估	一般风险	否	不通过

设置的权重比例是：系统配置安全评估 50%，系统状态安全评估：50%，那么终端的最终得分计算逻辑是：

系统配置安全评估大类得分为 0 分，因为否决项【账户锁定策略：重置账户锁定计数器的时间】评估不通过，则该评估项所在在大类不得分。

系统状态安全评估评估大类得分=50-（（2/（3+2））*50%*100）=30 分。

11. 基线核查

11.1. 基本概念

11.1.1. 得分

得分：得分是基于每个核查项开启并配置的扣分标准，经过策略或任务下发到终端逐项检查后计算的最终得分，反映该终端的安全及合规情况。

11.1.2. 定性标准

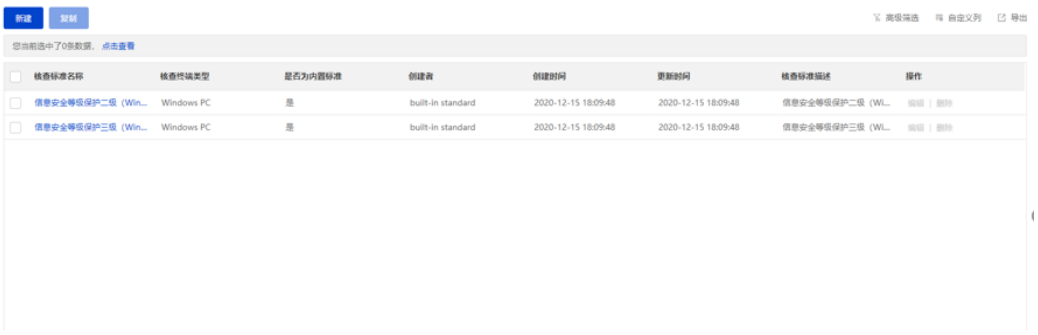
定性标准：基于检查项检查后上报的最终得分和否决项检查结果为终端的安全情况定性，支持按得分情况划分安全等级，也支持按得分情况和否决项通过情况划分检查结果，在安全防护>基线核查>业务设置页面进行定义。

安全级别：对终端检查的最终得分进行安全级别定义，目前为百分制，并分为 4 个级别：高危、中危、低危、安全。

检查结果：对终端的最终得分和否决项检查情况进行检查结果定义，并分为 2 种情况：通过、不通过。

11.1.3. 检查标准

什么是检查标准：针对国家标准、行业标准、自定义检查模板用来评估当前网内终端是否符合对应标准；目前产品内置有信息安全等级保护二级和三级检查模板（在资产管理>知识库>基线核查标准处查看和管理）。如下图：



11.2. 基本功能

11.2.1. 基线核查终端定性设置

在安全防护>基线核查>业务设置页面，可以基于得分配置终端的安全级别，也可以基于否决项和得分配置检查结果，完成配置后在基线核查概况、基线核查日志以及详情中均能实时查看终端的安全级别或检查结果（自定义列中勾选）。如下图：

标准配置：

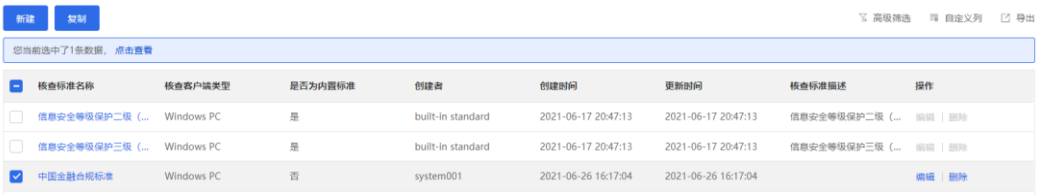
检查结果：

安全级别：

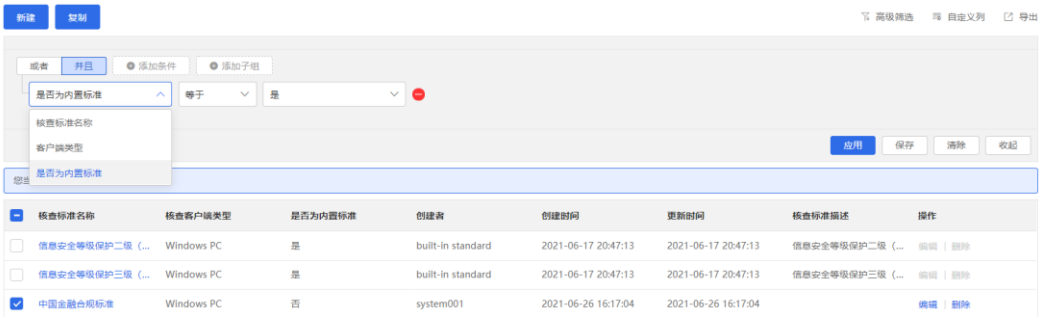
11.2.2. 基线核查标准

目前知识库内置有国家等保二级和等保三级核查标准，同时用户可以根据企业自身或行业要求自定义核查模板。在资产管理>知识库>基线核查标准页面，可以查看内置标准，并可以新建标准和复制标准；对于非内置的标准可以进行删除和编辑。

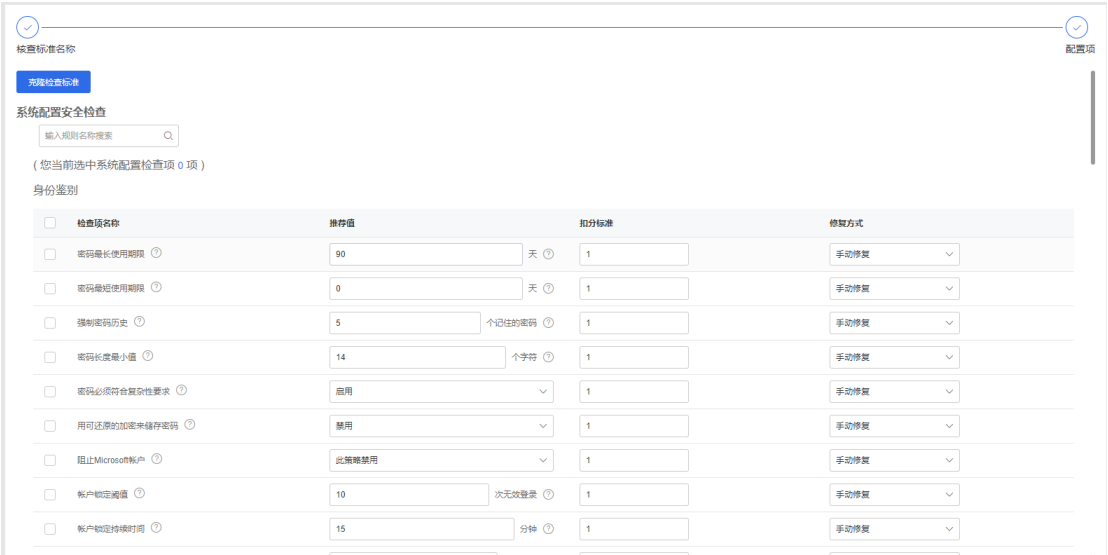
入口：资产管理>知识库>基线核查标准。



同时，支持通过名称、终端类型等不同条件筛选标准，支持导出标准列表。



通过新建/编辑知识库可自定义检查项。



11.2.3. 基线核查概况

基线核查概况用来展示全网终端（也可指定分组）当前的核查情况，包括检查项、检查通过项、检查不通过项、得分等等情况。根据在线状态和不同的分组等为查询条件，以帮助管理员快速找到对应的终端信息。

入口：安全防护>基线核查>基线核查概况。

导出：可以选择导出概况信息，可以导出终端的核查详情信息

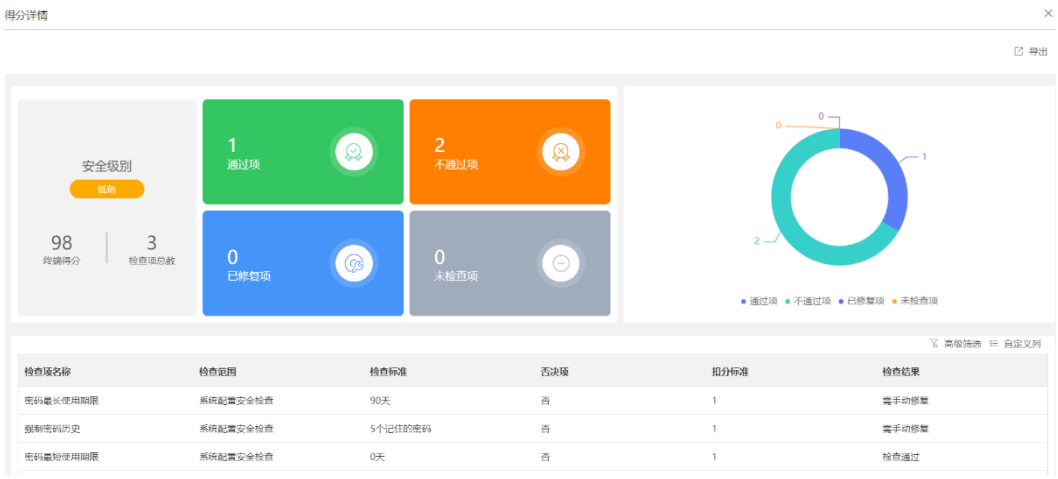
11.2.4. 基线核查详情

基线核查详情详细记录终端当时配置的检查项、扣分标准、检查结果，帮助管理员了解终端的详细检查情况，同时支持高级筛选、自定义列和导出。

入口：基线核查概况，以及基线核查日志>详情。

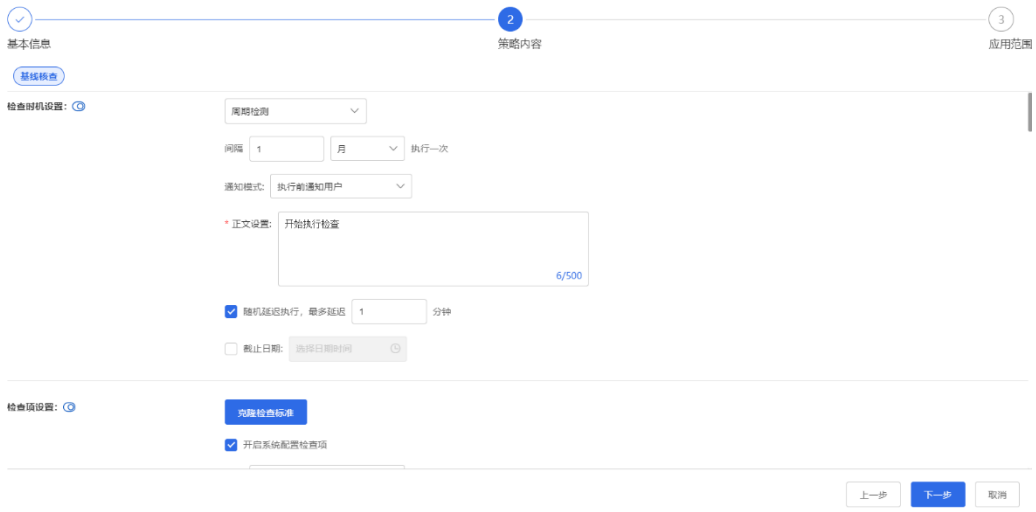
1、基于检查结果展示：

2、基于安全级别展示（在安全防护>基线核查>业务设置中切换定性标准）



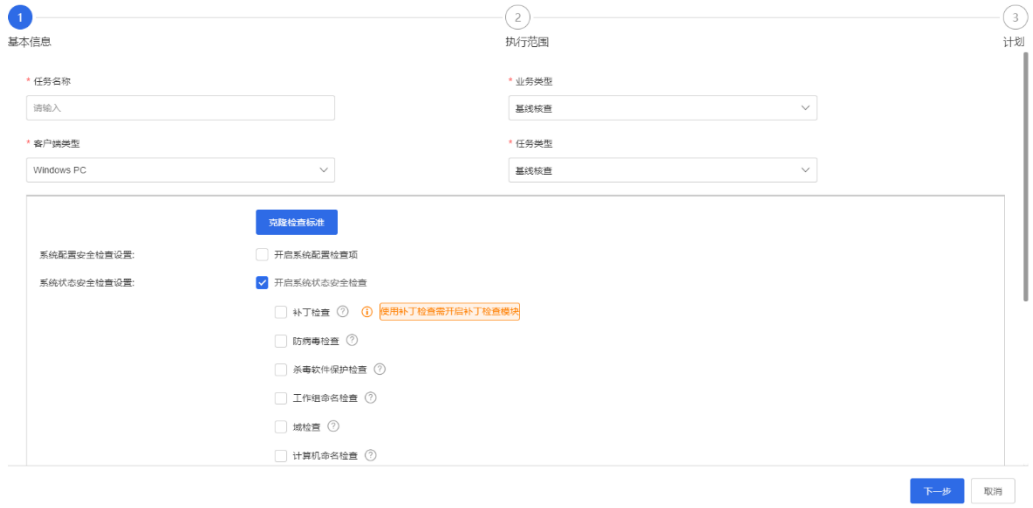
11.3. 基线核查策略

在安全防护>基线核查>策略管理的基线核查页面，可以对系统配置安全检查设置、系统状态安全检查设置、系统运行安全检查设置三个大项下面的几十项内容进行配置，并且可以对检查的时机进行设置；配置完成后，点击“下一步”然后配置应用范围后点击“应用”，可以下发策略到对应分组终端。如下图：



11.4. 基线核查任务

在资产管理>终端管理>终端任务里下发基线核查任务，可以对系统配置安全检查设置、系统状态安全检查设置、系统运行安全检查设置三个大项下面的 59 项内容进行配置；配置完成后，下一步选择影响范围后下发终端执行。如下图：

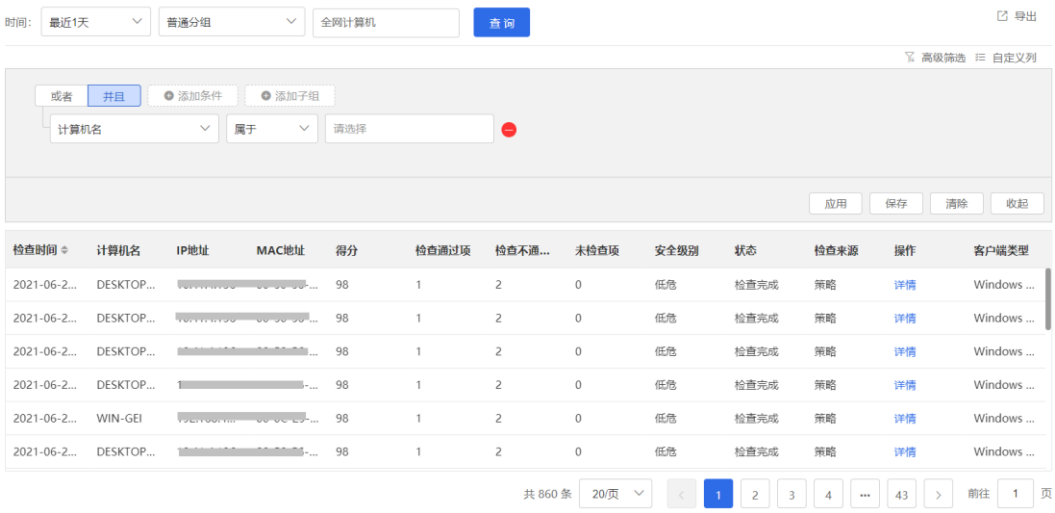


注意：在基线核查的知识库、策略和任务中，均可定制基线核查的检查项和修复方式。当修复方式设置为自动修复后，会将终端按照设置的核查标准进行修改。如果核查标准设置的不合理，会对终端造成不可预知的问题。请谨慎设置。以下列出部分高频出现问题评估项：账户：重命名来宾账户、账户：重命名管理员账户。

11.5. 基线核查日志

基线核查日志是对指终端上报的基线核查结果日志的记录，支持展示上报的终端基础信息、检查时间、得分、检查通过项、检查不通过项、未检查项、安全级别、检查来源、状态、操作（详情）等信息，并支持多种导出方式。

入口：安全防护>基线核查>基线核查日志。



11.6. 基线核查情况统计

基线核查情况可以按分组进行统计，统计当前分组范围内的终端检查情况，按照终端定性标准进行统计，新建统计任务后可以进行查看、重新执行和删除。

入口：安全防护>基线核查>基线核查统计。

统计详情按安全级别展示，包括待检查终端、安全终端、低危终端、中危终端和高危终端，具体如下：

统计详情按检查结果展示，包括待检查终端、检查未通过终端、检查通过终端，具体如下：

11.7. 典型场景

11.7.1. 如何快速完成对终端的安全性及合规性标准检查？

使用内置的国家标准，或者提前定义好行业或者企业级标准检查模板，在需要及时检查时克隆检查标准并通过任务下发给终端快速完成检查。

11.7.2. 进程对应的软件升级后进程也发生变化，如何减少调整保证设置的黑白名单依然有效？

在软件使用过程中无法避免软件的更新可能导致我们配置的进程检查列表失效，因此在管理中心提供了基于不同维度的规则对检查进程进行归类；在终端管理-知识库-进程知识库可以对进程检查通过按产品名称、公司名称、启动路径、签名等来设置规则，或者基于某些规则对进程进行分组归类，在下发基线核查时开启了进程检查则选择对应规则或者进程组即可，当终端进程有变化时可以基于规则自动调整，或者基于分组手动调整后再下发即可。

11.7.3. 检查发现问题后如何修复

管理中心提供了安全配置类的检查项和对应修复帮助文档；终端用户在基线核查的主界面可以打开查看。

12. 数据防泄漏

随着计算机系统在各行各业的普遍应用，办公文件、财务报表等各类数据都以电子文件的形态，在不同的设备（终端、服务器、网络、移动端、云端）上存储、传输、应用，数据安全已经成为政府、军队、企业及个人最为关注的问题。

12.1. 基本概念

奇安信天擎数据防泄漏以深度内容分析为基础，覆盖终端网络、邮件、设备、应用等数据通道，洞察敏感数据的分布、传输与应用，对数据进行即时的识别、监控和保护。

12.2. 内容知识库

12.2.1. 业务说明

内容知识库可以将敏感内容规则进行预先定义，进一步提供给数据安全相关业务配置内容安全策略。

12.2.2. 内容识别元素

关键字：由单个或多个字符构成的特征集，来定义某个敏感类别的特征。关键字作为用户理解最为直观的敏感内容配置方式，在实际生产环境中运用十分广泛。为了提高命中率，系统采用字符集（词典）的方式，按业务类别进行词典展示和维护。

近邻关键字：由两组关键字（词）组成，通过定义他们之间的间隔来实现敏感信息定义。

正则表达式：一种用于识别文本字符串（如特定字符、单词或字符模式）的机制，可以匹配一系列符合某个句法规则的信息。

数据标识符：具有一定数据正确性校验能力的数据特征集，与正则表达式类似，但在同样类型的数据配置中，数据标识符比正则更有效。

文件内容指纹：将文件内容按一定颗粒度换算成数字指纹数据进行特征匹配。

数据库内容指纹：对运行中的数据库库表字段数据进行数字指纹转换提取，作为特征检测匹配的依据。

智能分类：对分类样本做智能语义特征分析和提取，并根据分类语义特征进行数据分类判断的一种内容特征识别方式。

脚本：在普通的正则、关键字不能满足内容定义的一些场景下，支持用户通过系统提供的 Lua 脚本模板自定义扩展检测能力。例如：定义文档第 1001 个字符为 0 时，文件为敏感文件。

文件类型：可以通过文件特征识别到的文件类型，不代表可以识别到这些类型文件的内容。

12.2.3. 内容添加/维护

关键字

权重：当前关键字的相对重要程度，可以理解为权重值越大，越能代表该关键字在当前分类中的重要程度。

全字匹配：当前关键字在内容扫描时，前后为非中英文字符或非数字时才能被命中。

启用通配符：通配符包括半角的“*”和“?”，如果启用了通配符，当前关键字中的“*”代表任意字符串，“?”代表单个字符。

同时启用繁体：在点击[添加]按钮时，如果当前关键字中含简体中文字符，则自动追加一条翻译成中文繁体的关键字。在同一个词典内，需要对相同的关键字去重处理。

近邻关键字

定义：近邻关键字由两组关键字（词）组成，当两组关键字同时出现，其间隔又固定在一定范围内时记作命中。

示例：将关键字“中”和“国”设为近邻关键字，间隔为 3 字符，“中心之国”符合匹配规则，“中华人民共和国”则不符合匹配规则。

近邻关键字添加

正则表达式

场景：对于格式化特征比较明显的数据分类，使用正则表达式进行抽象化是目前业内的普遍做法。

为保证添加正则表达式时的语法正确性，添加正则时页面提供表达式本身数据正确性的测试功能：

数据标识符

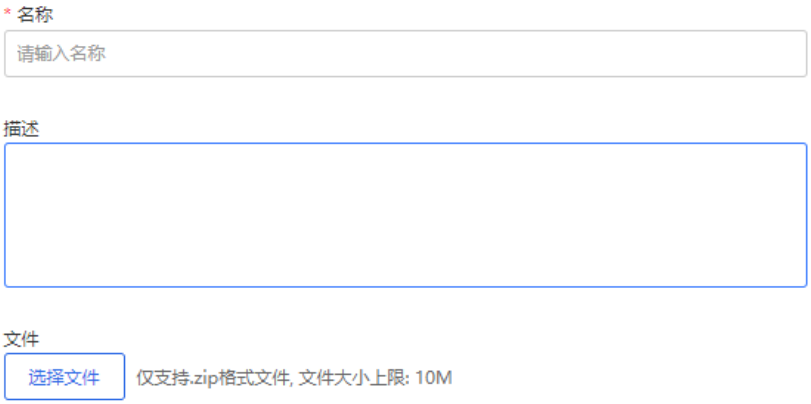
数据标识符通常情况下内置了一些数据校验的算法，内容都为系统内置：

文件内容指纹

使用场景：对于某些少量且重要的文件内容，将其内容按颗粒度转换为数字指纹后，可准确追踪到文件原内容的扩散泄漏。

前提条件：在制作文件内容指纹策略时，需提前使用指纹提取工具将文件内容转换为指纹文件（ZIP）。

指纹文件上传



数据库内容指纹

使用场景：针对数据库表中的敏感字段，进行数字化指纹转换，当终端外发含有这些字段的内容时进行准确匹配命中。

前提条件：在制作文件内容指纹策略时，需提前使用指纹提取工具将数据库字段内容转换为指纹文件（ZIP）。

数据库指纹上传

智能分类

使用场景：在不做任何内容定义的前提下，通过收集某些分类的文件样本，通过工具直接学习这些样本的分类特征，并把分类特征制作为策略内容，以自动将未知样本进行归类匹配。

前提条件：在制作文件内容指纹策略时，需提前使用指纹提取工具将数据库字段内容转换为指纹文件（ZIP）。

分类特征集上传

文件类型

定义：该页面展示的内容为可以通过文件特征识别到的文件类型，不代表可以识别到这些类型文件的内容。

脚本

LUA 脚本作为检测内容

导入脚本

内容工具下载

下载特征提取工具，特征提取工具为独立离线工具，可用于文件内容指纹、数据库内容指纹和智能分类特征的提取。

12.3. 基本功能

12.3.1. 数据安全运维基本思路

奇安信天擎数据防泄漏的设计理念是对通过通过网络、设备、应用等方式外发的数据进行内容的敏感度分析，对外发数据中含有的敏感信息进行审计、警告、阻断以及原文备份留证等，对数据泄漏行为形成有效监管和控制。

12.3.2. 发送者/接收者

系统策略定义后，默认对当前生效终端的所有符合定义的外发数据进行内容检测。系统支持从发送者/接收者维度复加定义符合检测条件的身份规则。

- 数据发送者：对数据发送者的身份进行定义，定义后系统只针对发送者外发的数据进行内容检测。
- 数据接收者：对数据发送者的身份进行定义，定义后系统只针对发送者外发的数据进行内容检测。
- 数据发送者例外：对数据发送者的身份进行例外处理，定义后符合例外规则的数据发送者在外发数据时免受内容检测。
- 数据接收者例外：对数据接收者的身份进行例外过滤，定义后在外发数据给符合例外规则身份的目标时免受内容检测。

逻辑关系：数据发送者和数据接收者之间为“与”的关系，数据发送者例外和数据接收者例外之间为“或”的关系。

12.3.3. Windows 终端数据防泄漏策略设置

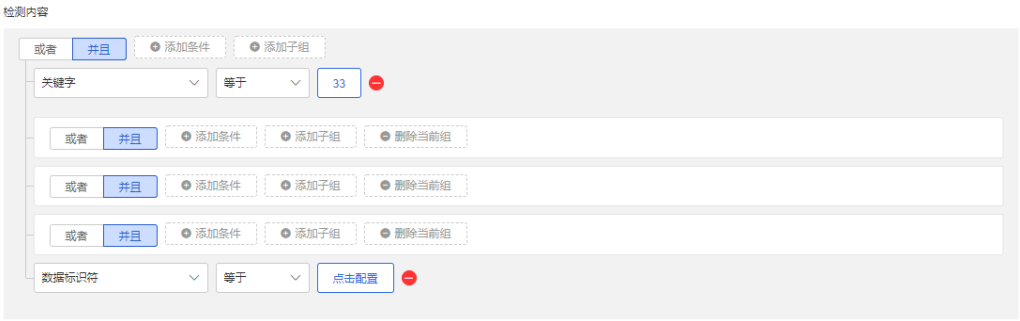
12.3.3.1. 外发数据实时检测

数据防泄漏的主体策略，定义外发数据通道所要检测的主要内容和保护动作。

内容规则：外发数据检测的最小闭环策略单位，可定所要检测的外发通道、检测内容以及执行动作。多个内容规则之间为“或”的关系。

匹配规则与例外规则：一次数据外发事件发生时，会先用例外规则进行匹配，如果符合例外规则的内容定义，则该次数据外发会被直接认定为不含敏感信息；如果不符合例外规则，会进一步检测是否符合匹配规则的内容定义，如果符合，会被认定为含有敏感信息。

检测内容：定义所要检测的敏感内容，支持将多种内容元素按照“与”、“或”、“非”以及逻辑子组合的方式进行混合定义：

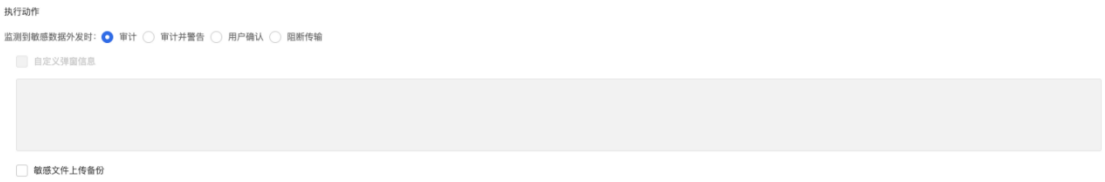


内容级别：定义内容规则的内容级别，系统内置 4 个内容级别，直接自定义添加和重命名。

适用通道：定义内容规则的开启通道范围，被开启的通道在检测到数据外发时，会自动使用策略配置的检测内容进行敏感性检测。对于 HTTPS、SMTPS、FTPS 加密网络协议，需要配置数据外发所使用的软件，否则不会解析加密协议外发数据。

执行动作：定义外发数据在符合敏感内容的定义时的响应动作。

- 审计：对于外发的敏感数据进行事件的详细审计。
- 阻断传输：对于外发的敏感数据进行事件的详细审计基础上，对外发的数据本身进行传输阻止并弹窗告警。
- 审计并警告：对于外发的敏感数据进行事件的详细审计基础上，系统弹窗告警。
- 上传文件：当外发的文件符合策略定义的敏感内容时，将原文件上传到文件服务器进行备份，并在日志中提供下载链接。
- 用户确认：外发的数据被检测到含有敏感信息时，系统弹框提醒用户外发的数据中含有敏感信息，由用户自行选择是否继续外发或主动阻断。无论最终结果是外发放行还是阻断，都会对外发进行事件的详细审计。



12.3.3.2. 功能配置

数据防泄漏策略的复加功能配置项，用来补充完善数据安全策略的细分需求。

通道白名单：开启某个通道的白名单后，终端对该通道外发数据不再启用内容检测。

文件加白申请：文件外发被阻断后，可针对文件本身进行外发加白，加白后的文件将不再进行内容检测。勾选“允许申请文件外发加白”后，终端在对一个文件进行右键操作时，自动出现“申请文件外发”菜单。

业务联动：可配置对奇安信加密 U 盘的对应分区进行加白，加白后往加密 U 盘对应分区的文件拷贝不再进行内容检测。

扫描模式：完整扫描模式下，系统默认对多个内容规则按从上到下顺序依次扫描，事件结果体现多个内容结果的命中情况；快速扫描模式下，系统对多个内容规则按从上到下的顺序依次扫描，当按策略命中一个内容规则时，不再继续扫描剩余的内容规则。

SMTP 传输阻断：开启后可对通过 SMTP 外发的邮件进行阻断，当“数据接收者”配置了相应的 Email 地址时，系统默认对这些地址的外发邮件内容进行敏感性检测后执行动作，而不是直接阻断。

12.3.4. 信创终端数据防泄漏策略设置

12.3.4.1. 外发数据实时检测

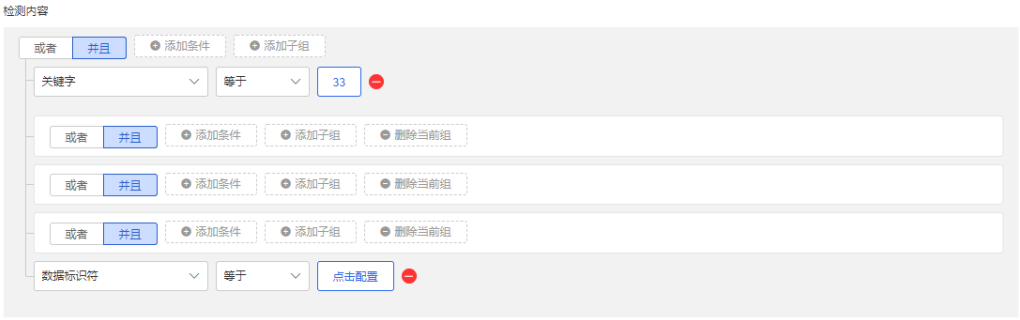
数据防泄漏的主体策略，定义外发数据通道所要检测的主要内容和保护动作。

内容规则：外发数据检测的最小闭环策略单位，可定所要检测的外发通道、检测内容以及执行动作。多个内容规则之间为“或”的关系。

匹配规则与例外规则：一次数据外发事件发生时，会先用例外规则进行匹配，如果符合例外规则的内容定义，则该次数据外发会被直接认定为不含敏感

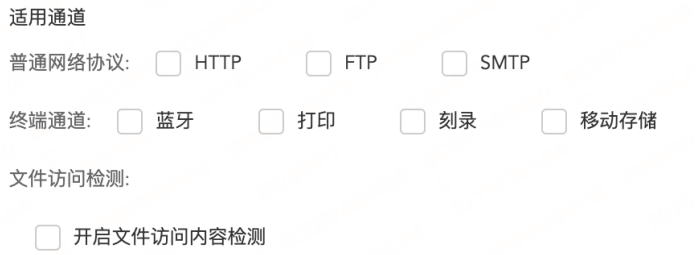
信息；如果不符合例外规则，会进一步检测是否符合匹配规则的内容定义，如果符合，会被认定为含有敏感信息。

检测内容：定义所要检测的敏感内容，支持将多种内容元素按照“与”、“或”、“非”以及逻辑子组合的方式进行混合定义，目前信创终端已支持关键字、正则表达式、数据标识符、文档大小、文件内容指纹和文件类型的检测：



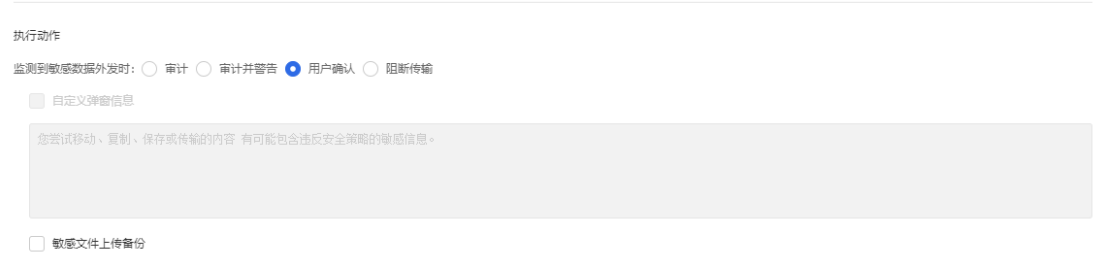
内容级别：定义内容规则的内容级别，系统内置 4 个内容级别，直接自定义添加和重命名。

适用通道：定义内容规则的开启通道范围，被开启的通道在检测到数据外发时，会自动使用策略配置的检测内容进行敏感性检测。



执行动作：定义外发数据在符合敏感内容的定义时的响应动作。

- 审计：对于外发的敏感数据进行事件的详细审计。
- 阻断传输：对于外发的敏感数据进行事件的详细审计基础上，对外发的数据本身进行传输阻止并弹窗告警。
- 审计并警告：对于外发的敏感数据进行事件的详细审计基础上，系统弹窗告警。
- 上传文件：当外发的文件符合策略定义的敏感内容时，将原文件上传到文件服务器进行备份，并在日志中提供下载链接。
- 用户确认：外发的数据被检测到含有敏感信息时，系统弹框提醒用户外发的数据中含有敏感信息，由用户自行选择是否继续外发或主动阻断。无论最终结果是外发放行还是阻断，都会对外发进行事件的详细审计。



12.3.4.2. 功能配置

数据防泄漏策略的复加功能配置项，用来补充完善数据安全策略的细分需求。

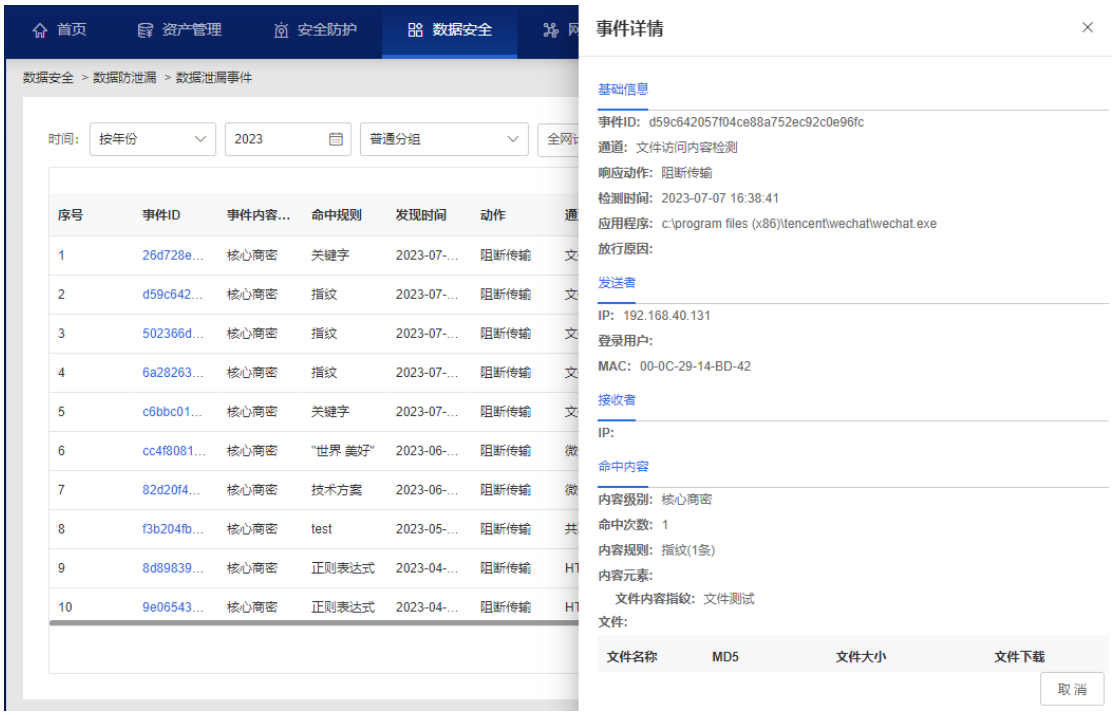
业务联动：可配置对奇安信加密 U 盘的对应分区进行加白，加白后往加密 U 盘对应分区的文件拷贝不再进行内容检测。

加密压缩包处理：阻断或用户确认模式下，当系统检测到外发含有打开密码的 ZIP/7Z/RAR 文件时，自动弹出密码输入框供用户输入，解压后进行压缩包内文件内容的检测。

12.3.5. 数据泄漏事件

当外发数据被检测到含有敏感内容时，系统自动记录审计日志，包括外发数据命中的内容规则、时间、IP、使用人等信息，对一次泄漏事件形成有效佐证。

系统采用列表+弹窗展示方式，每一个事件的常规信息通过列表展示，点击事件 ID 弹层展示该事件的详情。



12.3.6. 泄漏事件信息溯源

数据安全日常运维中，可能会产生大量的泄漏事件。奇安信天擎数据防泄漏支持管理人员在对泄漏事件的梳理时，对泄漏的敏感内容或文件进行反向追溯：

13. 安全水印

随着软硬件技术的不断发展，通过打印、截屏、拍照等方式造成的数据泄漏越来越普遍。安全水印覆盖打印、截屏、屏显多个场景，可以对泄漏信息进行有效溯源。

安全水印的主要目的是泄密溯源取证，它由打印水印、屏幕水印、截屏水印三款不同场景的模块组成，通过直观读取、二维码扫描还原、导入管理平台方式进行结果取证。

13.1. 基本概念

13.1.1. 打印水印

使打印的结果附带水印信息，包括自定义文字、图片背景和变量的用户和终端信息，来对打印者的信息进行溯源。

打印的触发方式可以监控个别或全部进程，在这些进程触发打印时自动附加水印信息。

打印水印支持参数：

类别	正文水印	页眉页脚水印
水印类型	明文水印、图片背景、二维码水印	明文水印、二维码水印
水印内容	自定义文本、用户名、打印时间、IP 地址、MAC、手机尾号、资产责任人	自定义文本、用户名、打印时间、IP 地址、MAC、手机尾号、资产责任人
水印行间距	0-100	
水印列间距	0-100	
透明度	0-255	

角度	0-60	
文字大小	5-72	小、较小、中、较大、大
文字颜色	选择+输入	选择+输入
水印位置		左、中、右

13.1.2. 屏幕水印

屏幕水印采用屏幕浮水印技术，使水印信息呈现在屏幕最外层，通过截图、拍照方式获取的图片结果会附带相应的水印信息。

根据水印的显示区域不同，分为进程区域显示水印和全屏显示水印。

屏幕水印支持参数：

类别	全屏显示水印	进程区域显示水印
水印类型	明文水印、点阵水印	明文水印
水印文字	当前日期、用户名、当前时间、IP 地址、MAC、操作系统账号、计算机名、使用人（姓名）、手机尾号、资产责任人	当前日期、用户名、当前时间、IP 地址、MAC、操作系统账号、计算机名、使用人（姓名）、手机尾号、资产责任人
水印行间距	0-100	0-100
水印列间距	0-100	0-100
透明度	0-255	0-255
文字大小	5-72	5-72
水印角度	0-60	0-60
应用（触发）进程	全部进程、自定义进程（来源于进程知识库）	自定义进程（来源于屏幕水印进程库）

13.1.3. 截屏水印

截屏水印采用暗水印技术，通过截屏获取的图片，会自动附带终端信息、截屏时间和用户信息。使用过程中屏幕无任何水印信息展示，图片泄漏后，将图片导入系统可以溯源用户、时间及终端信息。

截屏水印支持参数：

类别	全屏显示水印
水印信息	用户名、截屏时间、IP 地址、MAC、操作系统账号、计算机名、资产责任人
触发进程	所有进程、自定义进程

13.2. Windows 终端基本功能

13.2.1. 安全水印运维基本思路

奇安信天擎安全水印的设计理念是对截屏、打印、拍照等场景造成的数据泄漏进行信息溯源，对以上方式的泄漏行为形成有效威慑。

13.2.2. 打印水印策略设置

正文水印

正文打印水印按类型可分为明文水印、二维码水印和图片背景水印，其中图片背景水印处于最下层，和明文件水印/二维码水印呈重叠关系。

水印文字：水印文字支持自定义内容和变量内容的混合输入，并可按显示需求自定义换行排版，满足多字段信息展示时的显示布局需要。

图片背景水印：支持不大于 800*600 像素的 PNG 或 JPG 图片作为打印结果的背景内容。

页眉页脚水印

页眉和页脚可以单独设置水印文字或二维码信息，设置方法与正文相同。

触发进程

全部进程：所有进程触发的打印结果均附带水印信息。

自定义进程：列表中的进程打印结果附带水印信息，进程来源于进程知识库。

13.2.3. 屏幕水印策略设置

明文水印

屏幕水印支持自定义内容和变量内容的混合输入，并可按显示需求自定义换行排版，满足多字段信息展示时的显示布局需要。

水印文字：水印文字支持自定义内容和变量内容的混合输入，并可按显示需求自定义换行排版，满足多字段信息展示时的显示布局需要。

显示参数：屏幕最外层展示的水印不会被第三方软件窗口遮挡，屏幕最里层展示的水印会被第三方软件窗口遮挡。

显示区域：屏幕水印显示方式分为全屏显示和进程区域显示。

触发进程：全屏显示水印：可选择屏幕常驻水印，也可选择监控应用进程的启动情况显示屏幕水印，进程来源于进程知识库。

进程区域显示水印：触发水印显示的进程来源于安全水印业务中的屏显水印进程库，该进程库支持页面添加，添加时需计算进程类名和窗口名。

点阵水印

通过屏幕输出点阵水印信息，用户通过截图、拍照等方式获取的图片，导入到系统后可以根据点阵的位置进行信息还原。

水印参数：点阵水印的水印默认为全屏展示水印信息，水印颜色支持自定义调整。每个点阵水印基本单位由九个点位组成，点位中又区分中心点和周围点八个点，在实际的场景当中，中心点的显示效果在颜色、大小上与周围的点形成差异，有利于管理员进行区分，简化还原的难度。

触发进程：可选择屏幕常驻水印，也可选择监控应用进程的启动情况显示屏幕水印，进程来源于进程知识库。

13.2.4. 截屏水印策略设置

截屏水印不在屏幕上展示任何信息，在系统进行截屏操作的时候，将需要添加的水印信息转换为和截图区域相关的图像，并将水印信息叠加到截取区域的图像上。

触发进程

全部进程：只要有截屏行为，就触发截屏水印策略。

自定义进程：列表中的进程在启动时进行截屏操作，会触发截屏水印策略。进程来源于进程知识库。

13.2.5. 屏显水印进程维护

当屏幕水印的显示模式选择进程区域显示水印时，因为需要计算进程的窗口区域值，系统内置了常用办公软件的类名和窗口名。

进程添加：新进程的添加需要计算进程的类名和窗口名。

13.3. 信创终端基本功能

13.3.1. 安全水印基本介绍

信创终端安全水印包括打印水印和屏幕水印两部分，对通过截屏、打印、拍照等场景造成的数据泄漏行为形成有效威慑。

13.3.2. 打印水印策略设置

正文水印

正文打印水印按类型为明文水印，除了支持展示计算机名、IP 等信息之外，还可以支持自定义文字信息和排版顺序。

水印参数：水印显示设置支持字体、字号、颜色、角度、透明度和密度的调整。

13.3.3. 屏幕水印策略设置

明文水印

屏幕水印支持自定义内容和变量内容的混合输入，并可按显示需求自定义换行排版，满足多字段信息展示时的显示布局需要。

水印文字：水印文字支持自定义内容和变量内容的混合输入，并可按显示需求自定义换行排版，满足多字段信息展示时的显示布局需要。

水印参数：水印显示设置支持字体、字号、角度、透明度和密度的调整。

点阵水印

通过屏幕输出点阵水印信息，用户通过截图、拍照等方式获取的图片，导入到系统后可以根据点阵的位置进行信息还原。

水印参数：点阵水印的水印默认为全屏展示水印信息，水印颜色支持自定义调整。每个点阵水印基本单位由九个点位组成，点位中又区分中心点和周围点八个点，在实际的场景当中，中心点的显示效果在颜色、大小上与周围的点形成差异，有利于管理员进行区分，简化还原的难度。

13.3.4. 截屏水印策略设置

截屏水印不在屏幕上展示任何信息，在系统进行截屏操作的时候，将需要添加的水印信息转换为和截图区域相关的图像，并将水印信息叠加到截取区域的图像上。

13.4. macOS 终端基本功能

13.4.1. 安全水印基本介绍

macOS 终端具备屏幕水印能力，对通过截屏、拍照等场景造成的数据泄漏行为形成有效威慑。

13.4.2. 屏幕水印策略设置

明文水印

屏幕水印支持自定义内容和变量内容的混合输入，并可按显示需求自定义换行排版，满足多字段信息展示时的显示布局需要。

水印文字：水印文字支持自定义内容和变量内容的混合输入，并可按显示需求自定义换行排版，满足多字段信息展示时的显示布局需要。

水印参数：水印显示设置支持字号、角度、透明度和密度的调整。

13.5. 水印信息溯源

对于含截屏水印信息的图片，将图片上传到系统后，可提取图像中叠加数据的图像信息，并从信息中还原数据。支持的图片类型：jpg、png。

截屏水印信息：

图片上传后，当前页面反馈还原信息，图片不做后台保存。

点阵水印信息：

经过拍照，打印、截屏等场景获取的点阵结果，人工进行任意 16 宫格点阵的信息输入，可对终端、用户、时间信息进行查询。

14. 终端管控

管控模块主要是对终端进行安全管理以及维护。主要功能有外设管理、网络使用管理、进程运行管理等，防止用户在使用外接设备、软件运行、能耗管理、非法外联等多种场景下出现的安全问题，提前避免安全事件的发生。

14.1. 基本概念

终端管控中外设管控只要对接口、光驱、蓝牙，红外限制其使用。进程管控主要根据进程的名称，软件厂商，签名等多种方式限制。能耗管控结合终端是否长时间未运行对其进行管控，管控方式包括锁屏，关机。网络管控通过根据源目IP 端口限制终端对网络的非法访问。非法外联根据终端能否和互联网进行连通对其进行断网或告警处理。

14.1.1. 外设管理

- 设备类型：对串口、并口、1394、PCMCIA、USB 接口、USB 存储设备，存储卡，冗余硬盘，软驱，打印机，扫描仪，磁带机，键盘，鼠标，红外，蓝牙，摄像头，手机/平板,移动数据网卡，MODEM 设备，ISDN 设备，ADSL 设备进行管控，控制方式为禁用。
- 设备特征：VID/PID、设备实例路径、设备名称，控制方式为允许和禁用两种方式。
- 光驱控制：对所有光驱和 USB 光驱进行管控，控制方式为禁用、允许刻录、只读三种方式。

- USB 移动存储设备附加定义：可在 USB 存储设备识别的基础上进一步定义存储空间，可以实现达到一定存储空间的设备才会被定义为移动存储设备。

14.1.2. 进程管理

- 进程黑名单：终端不能运行黑名单中的进程，可以对终端运行的进程进行主动收集上报至管理中心，管理员可自定义设置进程组，通过知识库直接将需要限制的进程组进行管控。
- 进程白名单：终端只能运行白名单中的进程，不在白名单中的进程均被禁止运行。
- 进程红名单：守护运行的进程，当终端运行红名单进程时，客户端会守护其不被恶意关闭。
- 部署模式：对于违规的进程不拦截，只上报告警日志。
- 防护模式：对于违规的进程拦截，并上报告警。

14.1.3. 外发管控

- 文件外发管控：不阻断外发通道的连接，只阻断外发的文件。
- 网页上传管控：对网页文件上传行为的管控，并支持通过 URL、文件加白 md5 等方式例外上传行为管控。

14.2. 基本功能

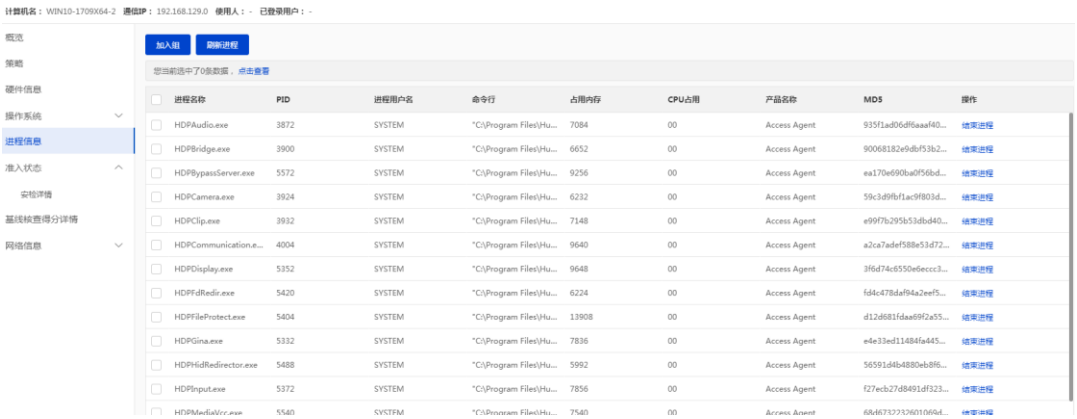
14.2.1. 终端维度的互联网出口状态展示

14.2.2. 单点维护-进程信息

在终端概况的终端列表里，点击计算机名，可以打开该终端的单点维护界面。

点击进程信息菜单，可以查看该终端的进程信息。

支持进程实时结束，支持将进程加入分组生成进程知识库规则。



14.2.3. 单点维护-网络信息-网络配置

在终端概况的终端列表里，点击计算机名，可以打开该终端的单点维护界面。

点击网络信息菜单，可以查看该终端的网络配置信息。

14.2.4. 单点维护-网络信息-网络流量

在终端概况的终端列表里，对在线的终端点击计算机名，可以打开该终端的单点维护界面。

点击网络信息菜单，可以查看该终端的网络流量信息。

定义：本次开机以来的流量使用统计

14.2.5. 单点维护-网络信息-网络连接

在终端概况的终端列表里，对在线的终端点击计算机名，可以打开该终端的单点维护界面。

点击网络信息菜单，可以查看该终端的网络连接信息。

定义：实时查看终端进程的网络连接详情。

14.2.6. 外设库

本内置了外设库信息，如终端上报的设备信息可识别，则后台程序会自动给设备分类，并自动填写设备的厂商和产品名。

如未识别出终端上报的设备，则默认不分组，厂商和产品信息为空，如用户开启未识别设备自动上报功能，我们后台会定期更新外设库，以提高外设库设备的识别率，方便用户管理。

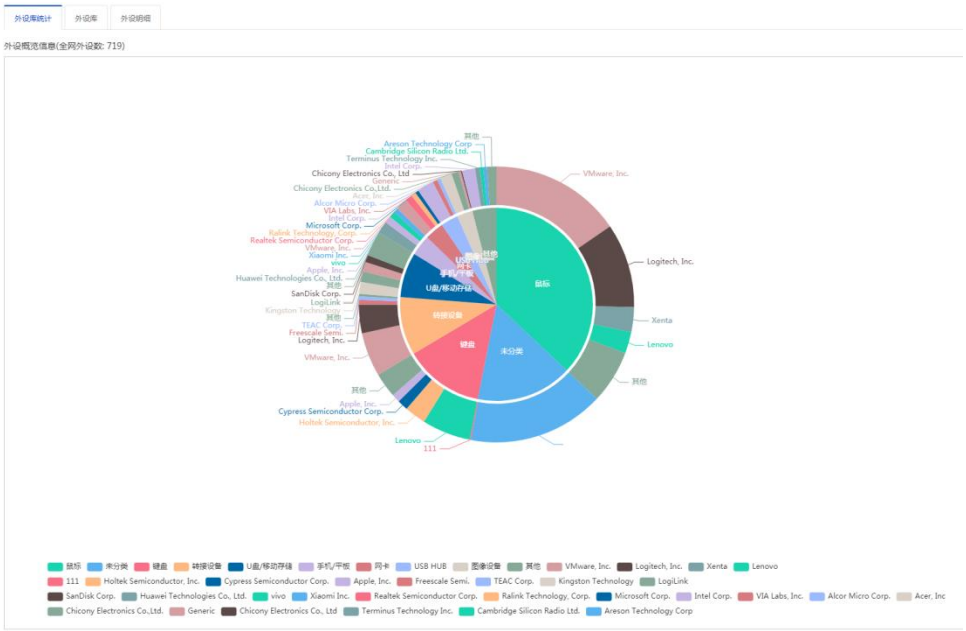
如用户知晓设备信息，也手工编辑设备属性。

14.2.6.1. 外设上报

终端管控>业务设置，TAB 外设库启用终端外设采集，则终端会收集外设信息（存在 VID 和 PID）上报到管理中心。

14.2.6.2. 外设库统计

对管理中心收集到外设进行统计，内圈显示所有收集外设的设备分类占比统计，外圈为每个类型中外设厂商占比统计。



14.2.6.3. 外设库

外设列表记录，按相同 VID 和 PID 进行聚合，列字段“数量”标识，外设属性（设备名称，VID，PID）相同的设备实例路径个数。

14.2.6.3.1. 设备分类

设备类别内置 10 余中类型，客户可手工增加设备类型

1）手工添加设备类型

鼠标移到左侧设备类型树的图标，点击弹出按钮[新建设备类型]，在弹出界面上输入类型名，点击[确定]，即可自定义设备类型

2）删除设备类型（注：仅手工添加的设备类型可被删除）

鼠标移到手工添加类型行的图标，点击弹出按钮[删除设备类型]，在弹出界面上点击[确认]按钮，即可完成删除设备类型

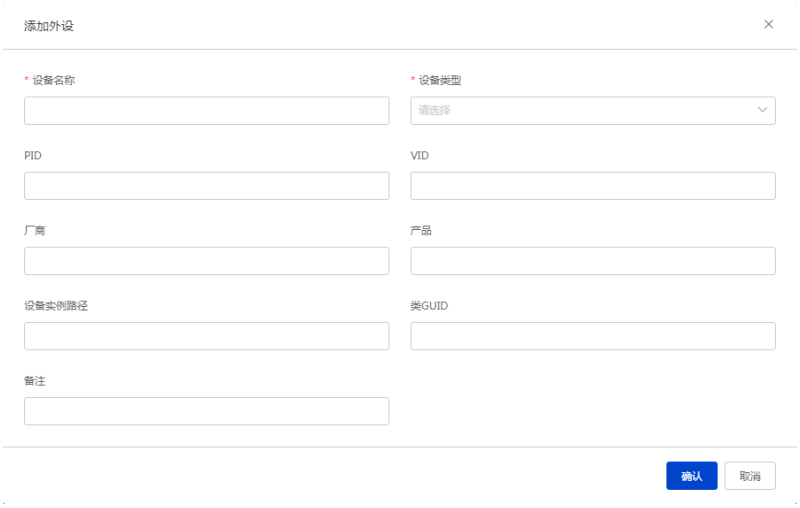
3）设备类型下外设数量统计

左侧设备类型树，每种类型后的括号内数字代表该类型的外设数量

14.2.6.3.2. 手工添加设备

支持管理员手工添加设备类型。

点击页面[添加]按钮，在弹出界面上输入设备对应属性，点击[确认]，即可完成手动添加设备。



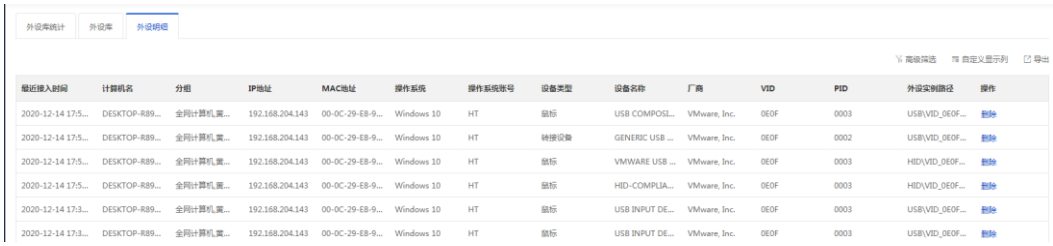
点击记录行的按钮[修改]，可对外设信息进行修改；修改界面，可对空字段内容、“设备类型”和“备注”进行修改，其他不为空的设备属性字段不允许修改

点击记录行的按钮[删除]，可对该条外设记录进行删除（同时删除 TAB-外设明细下对应 VID，PID 的外设记录）。

14.2.6.4. 外设明细

此页面只记录设备最后一次接入时间，接入的计算机名称，IP，mac，设备类型等。

点击列表[删除]按钮，外设明细记录被删除（同时更新 TAB-外设库下对应 VID，PID 的外设记录的“数量”统计）。



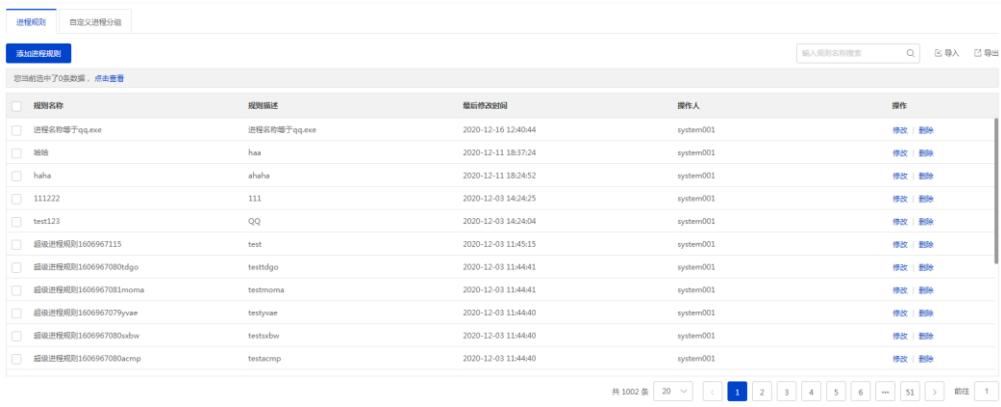
14.2.6.5. 外设库更新

系统管理>更新管理>数据安全中，可设置外设库更新。

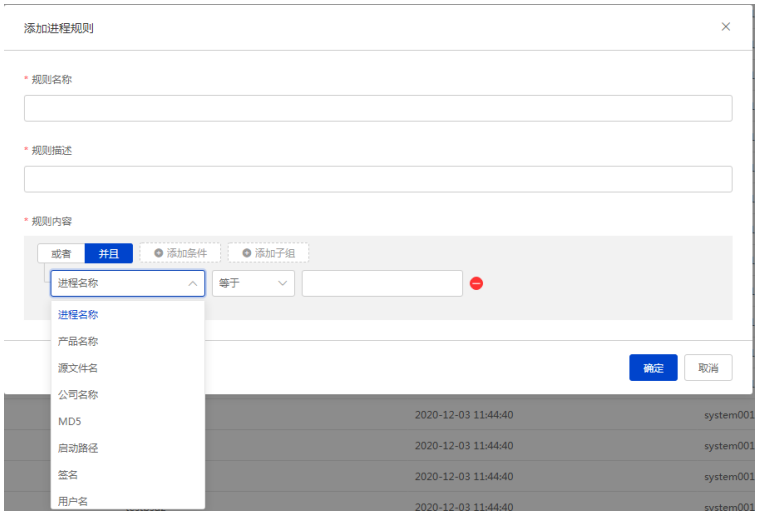
14.2.7. 进程知识库

终端运行的进程自动上报至管理中心，通过单点维护-进程信息将进程加入知识库分组。管理员可设置进程组，也可设置进程规则，以便策略使用。

14.2.7.1. 进程规则



点击按钮[添加进程规则]，在弹出界面上输入规则内容，点击[确定]，即可成功添加进程规则。



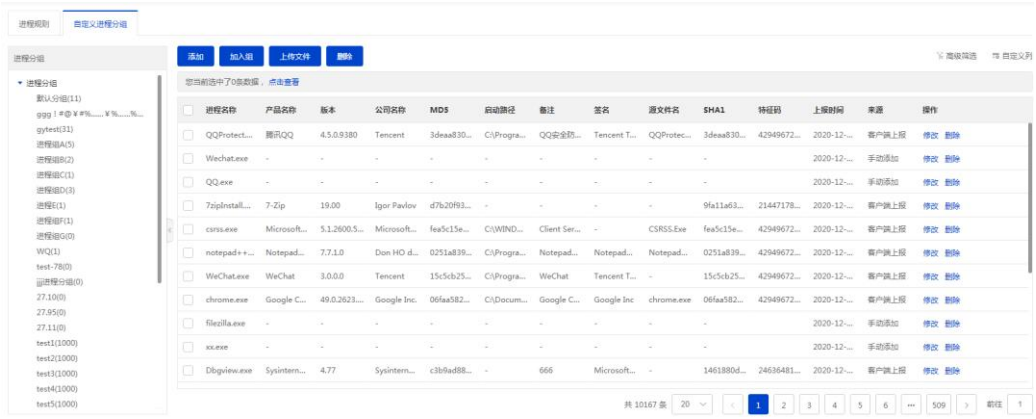
点击记录行的按钮[修改]，可对进程规则进行修改

点击记录行的按钮[删除]，可对进程规则进行删除

点击按钮[导入]，可按模版样式配置进程规则，批量导入进程规则

14.2.7.2. 自定义进程分组

左侧进程分组树，每个分组后的括号内数字代表该分组下的进程数量。



进程分组中内置“默认分组”。

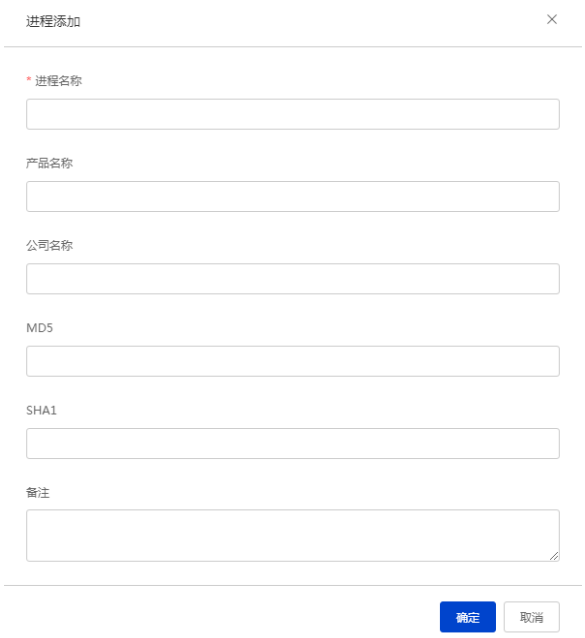
1）进程分组

鼠标移到左侧进程分组树的图标，点击弹出按钮[新建进程分组]，在弹出界面上输入进程组名称，点击[确定]，即可自定义添加进程分组。

鼠标移到进程分组的图标，点击弹出按钮[修改]或[删除]，可对已添加的分组进行分组名称修改或删除分组（默认分组无法被修改或删除）。

2）进程

点击按钮[添加]，在弹出界面上输入进程信息，点击[确定]，即可自定义添加进程。



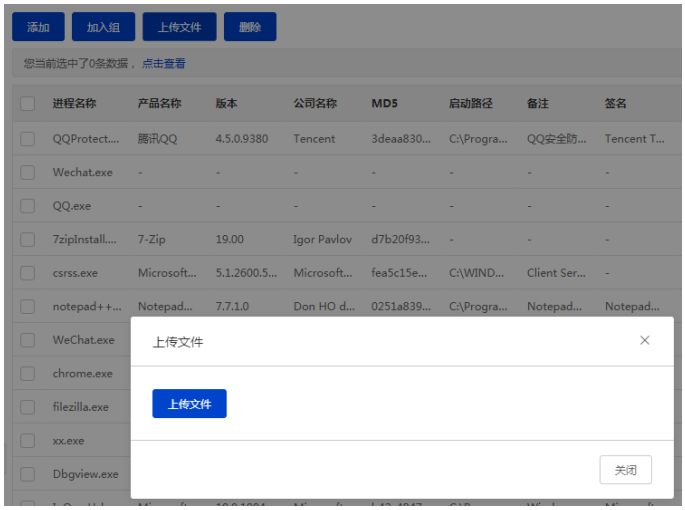
点击记录行的按钮[修改]，可对进程进行修改。

点击记录行的按钮[删除]，可对进程进行删除。

勾选进程记录前的复选框，点击按钮[加入组]，可将选中进程加入到某个分组下。

勾选进程记录前的复选框，点击按钮[删除]，可批量删除选中进程。

点击[上传文件]，在弹出界面上选择进程 EXE 文件，可添加 EXE 的进程信息。



14.2.8. WIFI 库

WIFI 库入口：数据安全>知识库>WIFI 库

1）SSID 上报

启用网络管控策略后（数据安全>终端管控>策略管理>网络管控）终端会收集接入的 WIFI 信息上报到管理中心，管理员可设置 WIFI 分组，以便策略使用

2）WIFI 分组

鼠标移到左侧 WIFI 分组树的图标，点击弹出按钮[新建]，在弹出界面上输入 WIFI 组名称，点击[确认]，即可自定义添加 WIFI 分组

鼠标移到已添加分组的图标，点击弹出按钮[修改]或[删除]，可对已添加的分组进行分组名称修改或删除分组（默认分组无法被修改或删除）

3）SSID 规则

点击[添加]按钮，在弹出界面上输入 SSID 信息，点击[确认]，即可自定义添加 SSID 规则

点击记录行的按钮[修改]，可对 SSID 规则进行修改。

点击记录行的按钮[删除]，可对 SSID 规则进行删除。

勾选 SSID 规则记录前的复选框，点击按钮[加入组]，可将选中 SSID 规则加入指定分组生成 WIFI 分组规则。

点击按钮[导入]，可按模版样式配置 SSID 规则，批量导入 SSID 规则。

14.2.9. 网络出口名单

入口：资产管理>知识库>网络出口名单

1）终端出口上报

如果开启了违规外联策略互联网出口探测，终端会将探测到的出口地址上报到管理中心，管理员可设置白名单分组，也可设置自动分组规则，以便策略使用

注意：终端触发违规外联并且出口 ip 在所配置的网络出口名单中才会显示，否则会显示空白。

2）出口名单分组

系统支持对出口名单分组进行创建和编辑操作， 违规外联策略可使用分组数据进行白名单的配置，来实现对网络出口的违规与否定义。

3）出口名单 IP 规则

点击[导入]按钮，可按模板样式配置网络出口名单 IP 规则，批量导入出口名单 IP

注：网络出口名单不支持手工添加名单 IP。

14.3. Windows 终端管控策略

策略入口：数据安全>终端管控>策略管理

14.3.1. 外设管理

外设管理范围：对外接设备按照设备分类的使用控制

设备类别	设备类型	控制方式
设备分类	1394、串口、并口、PCMCIA、USB 接口、USB 存储设备、存储卡、冗余硬盘、软驱、打印机、扫描仪、磁带机、键盘、鼠标、红外、蓝牙、摄像头、手机/平板、移动数据网卡、MODEM 设备、ISDN 设备、ADSL 设备	禁用
设备特征	VID/PID、设备实例路径、设备名称	禁用、例外
光驱控制	所有光驱设备、USB 光驱设备	禁用、允许刻录、只读

USB 移动存储设备附加定义：可在 USB 存储设备识别的基础上进一步定义存储空间，可以实现达到一定存储空间的设备才会被定义为移动存储设备。

终端弹窗：可定义是否开启终端弹窗，并可进一步定义弹窗内容。

日志上报：外接设备被拦截时，可定义是否上报拦截日志到管理中心，并支持控制终端上报日志的频率。

【注意】 windows 外设控制禁用 USB 接口时会导致 USB 存储设备以及通过 USB 连接的鼠标、键盘等所有 USB 接口类型的设备都将被禁用。

14.3.2. 进程管理

进程防护是通过进程匹配规则对运行在终端上的进程进行保护，阻止第三方进程对受保护进程进行操作的安全机制。

进程管理：

功能	描述
管控模式	支持仅告警不拦截的部署管控模式和拦截且告警的防护管控模式。
允许/禁止第三方进程运行	即黑白名单外进程的处理逻辑。允许第三方进程运行即默认允许黑白名单外第三方进程运行。禁止第三方进程运行即默认禁止黑白名单外第三方进程运行。
黑白名单	支持对第三方应用程序设置白名单管控或黑名单管控模式。
精确识别	通过对文件名、文件路径、MD5、数字签名、产品名称及用户名的精准或模糊匹配以及简单逻辑组合对终端上的进程进行匹配。匹配后的规则会依据相应的防护策略触发防护动作，从而实现进程黑白名单控制。
进程红名单	支持对指定进程的进程保护，防止终端关键进程被误杀。
拦截审计	支持对进程拦截行为进行弹窗告警和日志上报管理中心。
白名单审计	支持对白名单进程运行提供审计日志。

【注意】黑白名单操作属于高风险操作，并且配置后会全局生效，如果添加错误可能导致整个内网内相关进程均被拦截。为了避免出现误禁事件，建议如果有添加黑名单的需求，应先在测试环境中验证无异常后，再投入生产实施。

14.3.3. 能耗管理

对终端计算机长期不关机等现象进行统一管理，降低使用能耗。

能耗管理：

功能	描述
开机告警	支持设置工作时间外开机告警
定时关机	设置终端定时关机，如终端人员正在办公，终端人员可取消关机策略
主机运行监测	支持终端长时间运行监测
自动锁屏/注销	支持终端长时间未操作时进行锁屏或注销等节能措施
节能告警	终端触发节能告警时，支持倒计时告警，在倒计时结束之前可对终端运行文件进行保存整理。
空闲时间节能	终端暂不能立即进入节能措施时，支持临时取消节能措施，指定时间后重新进入节能措施流，终端完成节能措施后，刷新终端状态进入下次节能监测。
终端性能监控	CPU、内存、磁盘使用监控和告警

14.3.4. 网络管控

网络管控提供了终端网络连接相关的参数配置。

网络管控：

功能	描述
网卡防护	提供网卡 IP 地址修改控制、MAC 修改控制、热点创建控制、DNS 地址设置（非地址绑定）、无线网卡禁用控制、USB 网卡使用控制、使用动态 IP 控制，并支持 IPV6 地址禁止。
WIFI 管理	提供 WIFI 连接控制，禁止终端同时连接多个无线信号（多无线网卡环境），禁止被连接的无线网络支持在终端隐藏显示。
WIFI 管控例外	设置可信 WIFI 列表，终端只能连接白名单中的无线 ssid，其他无线信号不可连接

【注意】 通过策略批量修改终端的 DNS 配置，有可能造成终端的网络连接和访问等问题，请做好提前验证和操作系统版本兼容性核对后谨慎操作。

14.3.5. 违规外联

违规外联业务主要解决隔离网环境下，对终端电脑违规连接使用外网的发现和处理。系统通过对外网地址的可连通性探测，来定义用户存在的违规行为。

违规外联：

探测地址类型	地址类型	出口探测	处罚方式
普通地址	URL、IP	不支持	断网、关机、断网+锁屏、锁屏
公共外联响应中心地址	固定地址	支持	断网、关机、断网+锁屏、锁屏
自建外联响应中心地址	自建 URL、IP	支持	断网、关机、断网+锁屏、锁屏

名词解释

出口探测：探测外网地址时获取本地的互联网出口地址。

tracert 探测：tracert 路径探测，作为日志中的辅证。

外联响应中心：系统提供的程序，用来帮助用户搭建自有外网探测中心。

违规外联时处罚动作

断网：终端在断网状态下，只能连接管理中心，断网状态重启后恢复

锁屏：可以使用策略预置密码进行解锁

关机：支持 1 分钟的缓冲，可以对终端操作文件进行保存和整理。

注意：处罚动作会造成终端断网、锁屏、关机等行为，建议根据管控强度制定处罚力度。

14.3.6. 远程协助

管理员主动对在线的 Windows PC 终端发起远程协助。

远程协助入口：数据安全>终端管控>管控概况>远程协助

在远程协助过程中，支持管理员在主控端和被控端直接进行文件传输、快捷键、多屏幕切换。

14.3.7. 服务管控

支持对黑名单服务通过服务名称进行禁止启动的管控。

支持对关键服务通过服务名称设置自启动的管控。

14.3.8. 桌面加固

支持对 internet 属性中的信任站点进行统一配置添加。

支持对 internet 属性中的代理服务进行代理禁用或统一管控代理配置。

【注意】 通过策略批量修改终端的 Internet 代理服务器，有可能造成终端的网络访问受限与阻断等问题，请做好提前验证后谨慎操作。

支持禁止终端从安全模式启动或设置安全模式登录密码。

支持自定义桌面图片背景。

支持自定义桌面屏保，且可定义系统的最长等待时间，如果客户已经配置了小于该配置的屏保等待时间，则直接取客户自己配置的值生效；若客户已经配置了大于该配置的屏保等待时间，则会强制修改客户配置与策略一致。

支持禁止修改计算机名、禁止开启文件共享和禁止使用注册表编辑器。

【注意】 “通过策略批量修改终端的注册表内容，有可能造成终端操作系统和软件的运行问题，请做好提前验证和操作系统版本核对后谨慎操作”

【注意】 禁用本地账号后，终端将不能使用本地帐号登陆系统，请谨慎使用！

14.3.9. 外发管控

外发管控业务管控的对象是外发的数据，而不是外发的通道本身，从而实现在不影响外发通道连接的基础上阻断数据外发。

文件外发管控：可添加蓝牙通道的文件外发管控，实现对通过蓝牙外发的文件进行传输阻断，但不阻断蓝牙连接的效果。最终实现在不影响蓝牙鼠标、耳机、键盘等使用的前提下，对通过蓝牙外发的文件进行管控。

网页上传管控：对通过网页上传进行的文件传输进行管控，不影响正常的网页访问。

14.4. 信创终端管控策略

策略入口：数据安全>终端管控>策略管理

14.4.1. 外设管理

信创终端对外设的管理分为设备的禁用和读写控制。

设备类别	详情
设备禁用	1394、串口、并口、PCMCIA、USB 接口、USB 存储设备、存储卡、软驱、打印机、扫描仪、磁带机、键盘、鼠标、红外、蓝牙、摄像头、手机/平板
权限控制	内置光驱读写、外置光驱读写、U 盘设备读写、闪存设备读写、移动硬盘读写。
高级设置	按设备 PID/VID、设备名称、设备实例路径，在设备禁用基础上的使用禁止或允许。

14.4.2. 违规外联

违规外联业务主要解决隔离网环境下，对终端电脑违规连接使用外网的发现和处理。系统通过对外网地址的可连通性探测，来定义用户存在的违规行为。

违规外联：

探测地址类型	地址类型	出口探测	处罚方式
普通地址	URL、IP	不支持	断网、关机、断网+锁屏、锁屏
公共外联响应中心地址	固定地址	支持	断网、关机、断网+锁屏、锁屏
自建外联响应中心地址	自建 URL、IP	支持	断网、关机、断网+锁屏、锁屏

名词解释

出口探测：探测外网地址时获取本地的互联网出口地址。

违规外联时处罚动作

断网：终端在断网状态下，只能连接管理中心，断网状态重启后恢复

锁屏：可以使用策略预置密码进行解锁

关机：关闭终端电脑。

14.4.3. 远程协助

管理员主动对在线的信创终端发起远程协助。

远程协助入口：数据安全>终端管控>管控概况>远程协助

主控端	被控端	远程连接
Windows 系统	信创系统	支持
信创系统	Windows 系统	支持
信创系统	信创系统	支持

为保障用户知情权，远程过程中被控端有桌面悬浮窗口回显远程状态，并可主动结束远程连接。

14.4.4. 进程管理

进程黑名单：对符合黑名单规则的进程进行阻断启动或关闭进程。

进程白名单：对不符合白名单规则的进程进行阻断启动或关闭进程。

进程红名单：对符合红名单规则的进程进行运行守护（保护不被非正常关闭）或主动拉起进程。

进程流量监控：可对特定进程设置流量上限，超过流量上限使用时支持阻断网络访问。

进程性能监控：可对特定进程设置单位时间长度内，内存或 CPU 占用率持续超过一定百分比的监控。

【注意】黑白名单操作属于高风险操作，并且配置后会全局生效，如果添加错误可能导致整个内网内相关进程均被拦截。为了避免出现误禁事件，建议如果有添加黑名单的需求，应先在测试环境中验证无异常后，再投入生产实施。

14.4.5. 能耗管理

能耗管理主要包括节能管理以及非工作区间对终端电脑的使用监控和终端系统性能的监控。

节能管理：设置终端定时关机，如终端人员正在办公，终端人员可取消关机策略。

非工作区间监控：可配置工作时间段，以对非工作时间开机进行事件告警。

系统性能监控：主要对终端的 CPU、内存和磁盘空间使用超过阈值时，产生事件告警。

14.4.6. 网络管控

网络流量管控主要实现了对终端电脑网络流量的使用监控，对于异常的网络使用情况可进行断网处置。

功能	描述
外联设备控制	提供网卡 IP 地址修改控制，MAC 修改控制，热点创建控制，无线网卡禁用控制，有线、无线共用控制，应用代理、浏览器代理使用控制，并支持 IPV6 地址禁止。
WIFI 控制	支持 WIFI 连接控制。可自定义可信 WIFI 列表，终端只能连接白名单中的无线 ssid，其他无线信号不可连接。

14.4.7. 桌面加固

支持自定义桌面图片背景。

支持自定义桌面屏保，且可设置是否允许终端配置比策略设置值低的屏保时间。

支持账户权限管控。

14.4.8. 服务管理

通过服务名的配置对服务进行禁止启动、开机自启动、启动、停止、开机不启动的管控。

14.5. macOS 终端管控策略

14.5.1. 外设管理

通过对蓝牙及大容量 USB 存储设备的使用管控，管控通过这些通道造成的数据泄漏。

支持参数：

外设类型	管控能力
蓝牙设备使用管理	禁止通过蓝牙连接其它设备 禁止通过蓝牙连接其它手机、电脑设备
USB 设备使用管理	禁止连接大容量 USB 存储设备（容量支持自定义）

14.5.2. 网络管控

通过对无线网络的管理，防止用户私搭、私连无线网络产生安全隐患。

支持参数：

管控项	管控能力
无线热点	禁止创建无线热点
无线连接	禁止连接无线网络
多 SSID 同时连接	禁止多 SSID（同时连接两个以上）同时连接

14.6. 管控日志

终端管控覆盖外设、进程、网络等多个子业务能力，不同的子业务产生的相关日志差异较大，所以在管控的日志根据子业务类型进行分类展示。

通过管理中心：数据安全理-终端管控-管控日志，查看终端管控相关管理日志。

- 外设管理日志：根据策略配置记录外接设备的违规使用记录。
- 进程管理日志：根据策略配置记录黑、白、红进程的相关使用记录。

- 违规外联日志：根据策略配置记录外联日志，并区分违规外联和合法外联。
- 能耗管理日志：根据策略配置记录能耗管理的相关日志。
- 远程协助日志：记录包括时间、时长等远程记录。
- 远程文件传输日志：记录在远程协助期间发生的文件传输记录。
- 网络管控日志：记录网卡防护和网络使用相关的日志。
- 外发管控日志：分为文件外发日志和网页文件上传日志，主要记录在不允许外发或上传文件的前提下的外发或上传尝试行为。
- 服务管理日志：根据策略记录相关服务的使用记录。
- 桌面加固日志：根据策略配置记录共享目录的相关日志。

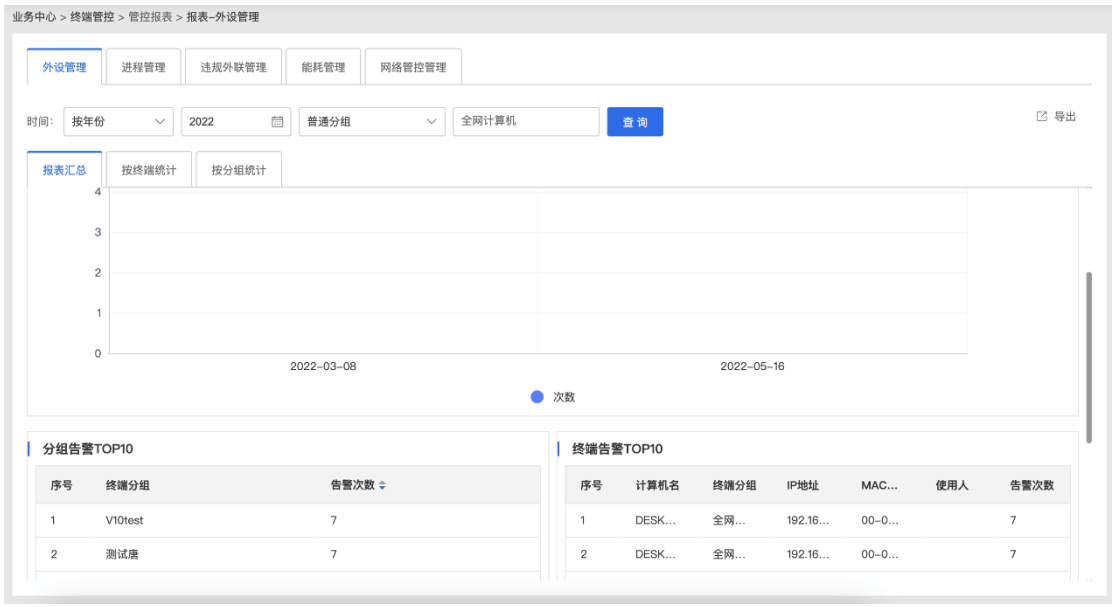
14.7. 管控报表

通过数据抽象，将终端管控一些关键的日志统计并进行展示。由于管控业务自身的分散性，管控相关的报表分为外设、进程、违规外联、能耗、网络五种类型进行展示。

通过管理中心：业务管理>终端管控>管控报表，查看终端管控相关信息统计。

14.7.1. 外设管理报表

外设管理报表统计单位时间段内终端外设使用告警，包括告警总体趋势和分组、终端维度的告警 TOP10 信息。另外还可以从终端、分组维度进行告警次数的统计。



14.7.2. 进程管理报表

进程管理报表统计单位时间段内进程运行的整体情况，包括进程运行告警的趋势和各种告警类型的占比分析和分类 TOP 信息。另外还可以从终端、分组、进程维度进行专项分析统计。

14.7.3. 违规外联管理报表

违规外联报表统计单位时间段内内部终端外联的整体情况，包括外联时网络出口访问的趋势和违规统计。另外还可以从终端、分组、合规出口和违规出口维度进行专项分析统计。

14.7.4. 能耗管理报表

能耗管理报表统计单位时间段内内部终端违反能耗策略的整体情况，包括各种能耗违例的类型占比和 TOP 统计。另外还可以从终端、分组维度进行专项分析统计。

14.7.5. 网络管控管理报表

网络管控管理报表统计单位时间段内内部终端网卡防护告警和无线网络使用告警情况，包括分组、终端和无线网络维度的 TOP 统计。另外还可以从终端、分组和无线网络维度进行专项分析统计。

15. 终端审计

终端审计业务支持 Windows PC 终端、信创终端和信创服务器操作系统。对终端文件操作、打印等行为进行安全审计，协助运维人员发现安全问题。

15.1. Windows 终端审计

文件审计：终端用户在对文件进行操作、流转、网络使用、即时通讯等场景操作时，对终端用户的行为进行审计，事件发生时，用以还原文件的流转轨迹及终端的使用情况。

行为审计：终端用户在使用 IM、打印等场景时的行为记录。

文件水印：写入文档的信息，用户不可见。包括文件唯一 ID（对用户不可见，编辑、修改、另存、复制时不改变）、当前用户标识、当前终端 MAC 地址、当前终端机器名，其中用户信息与终端信息写入文件的上限数量为 3，超出后自动覆盖历史数据，只保留最后 3 份信息。

15.1.1. 文件审计

15.1.1.1. 文件审计运维基本思路

终端用户对文件进行本地操作及对外流转时，在对操作行为形成审计日志的同时，进一步对文件写入文件水印信息。文件流转到企业外部时，可在获得文件的同时对文件水印的信息进行直接溯源，也可进一步根据唯一 ID 信息对文件的内部流转轨迹进行还原，展现文件的生命周期。

15.1.1.2. 文件审计策略设置

文件审计策略设置，位于管理中心>数据安全>终端审计>策略管理。

15.1.1.2.1. 文件流转审计

文件流转审计分为出向和入向流转两部分，对于出向流转的文件，支持对 DOCX、XLSX、PPTX、PDF 格式的文件写入文件水印。

- 出向和入向流转都进行审计的通道：共享目录、移动存储、微信、企业微信、光盘

- 只审计出向的通道：HTTP、HTTPS、SMTP、SMTPS、FTP、FTPS、QQ、钉钉、OUTLOOk

针对协议数据的获取，支持特定软件的配置。

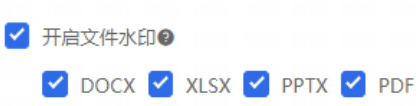
备注：协议和对应软件均配置完成，才可获取到协议内容。

文件后缀：管理员可选择对所有文件类型或指定文件类型进行审计策略的配置，为控制日志总量，建议使用指定文件后缀模式，将需要审计的文件类型依次添加。

文件名内容过滤：系统支持对包含特定文件名的文件进行审计。

文件归档：系统支持在对文件的流转进行审计的同时，将原文件同步归档到文件服务：

文件水印：系统支持在对文件的流转进行审计的同时，开启文件水印能力。



15.1.1.2.2. 文件操作审计

记录终端用户对文件的操作行为，支持对文件的新建、复制、移动、删除和重命名行为的审计。

文件路径：管理员可选择对全部文件路径或指定文件路径进行审计策略的配置，为控制日志总量，建议使用指定文件路径的审计，将需要审计的文件路径依次添加。

文件后缀：管理员可选择对所有文件类型或指定文件类型进行审计策略的配置，为控制日志总量，建议使用指定文件后缀模式，将需要审计的文件类型依次添加。

【注意】文件操作审计开启“全部”审计，可能会产生大量的审计日志，增加服务器的性能压力，建议参考服务器配置参数谨慎开启。

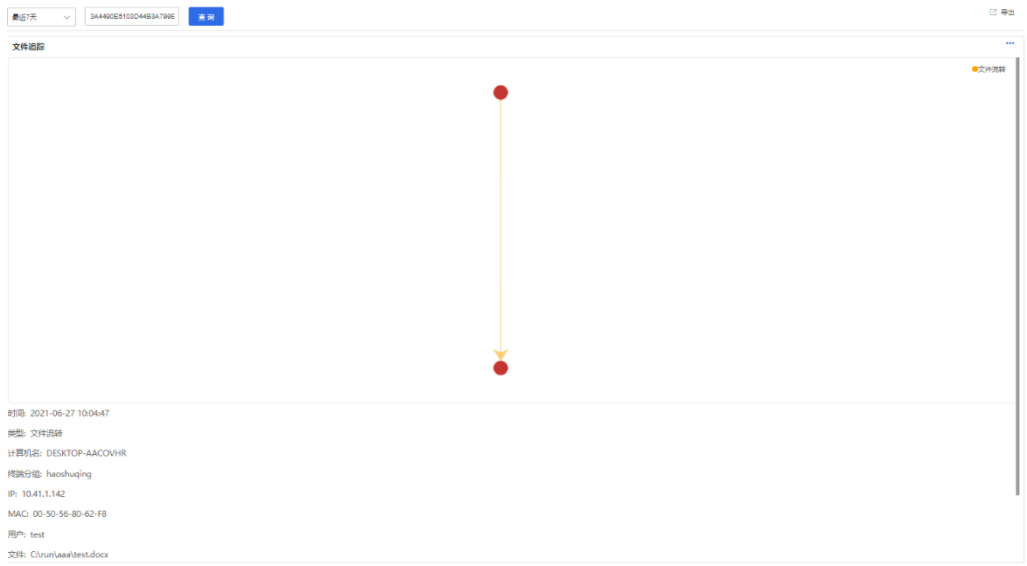
15.1.1.3. 文件信息溯源

主要应用场景：文件泄漏后，在已经获取到泄漏文件的前提下，可以对文档的最后 3 次操作流转信息（时间信息、终端信息、用户信息）进行还原。

15.1.1.4. 文件追踪

主要应用场景：依赖文件流转审计日志，通过文件水印定位和还原文件在内部的流转轨迹。

在文件追踪的图示中，每一个连接点代表一台终端，每一条线代表一次文件流转，点击相应的箭头线，可直接展示该次审计日志的详情：



15.1.1.5. 文件审计运维基本思路

终端用户对文件进行本地操作及对外流转时，在对操作行为形成审计日志的同时，进一步对文件写入文件水印信息。文件流转到企业外部时，可在获得文件的同时对文件水印的信息进行直接溯源，也可进一步根据唯一 ID 信息对文件的内部流转轨迹进行还原，展现文件的生命周期。

15.1.2. 行为审计

行为审计策略设置，位于管理中心>数据安全>终端审计>策略管理。

15.1.2.1. 行为审计运维基本思路

行为审计可对终端用户日常的打印、IM 通讯等操作行为客观记录，当安全事件发生时，运维人员根据已产生的行为审计日志对事件进行溯源。

15.1.2.2. 行为审计策略设置

15.1.2.2.1. IM 审计

入口：数据安全>终端审计>策略管理

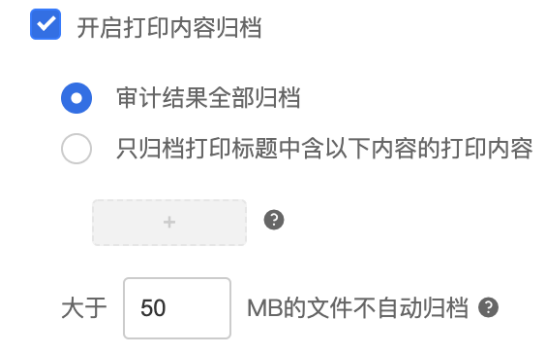
支持对 QQ、微信、企业微信和钉钉的即时通讯消息进行审计，并在审计的基础上对通过 IM 的文件流转进行归档。

15.1.2.2.2. 打印审计

入口：数据安全>终端审计>策略管理

对终端打印行为的日志记录，支持对所有打印行为或指定打印标题的打印行为进行审计。

归档：可针对所有打印内容或指定打印标题包含内容备份到服务器上。

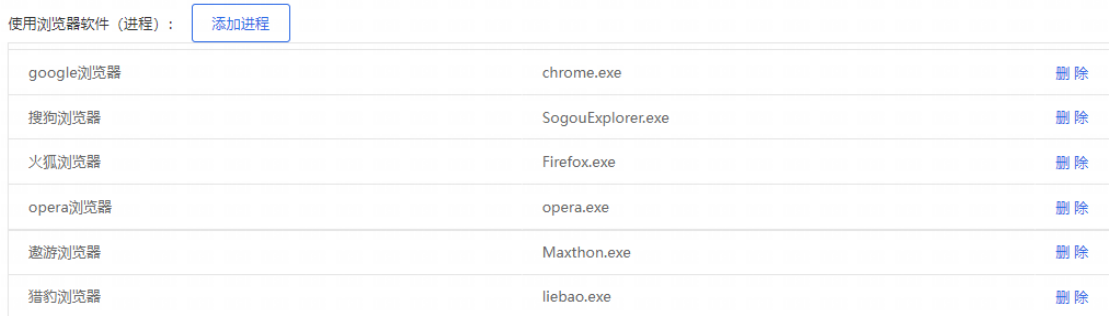


15.1.2.2.3. 网站访问审计

入口：数据安全>终端审计>策略管理

对终端通过浏览器访问网络行为的日志记录，支持对所有网站或指定网站访问行为进行审计。

支持配置指定浏览器



15.1.2.2.4. 邮件外发审计

入口：数据安全>终端审计>策略管理

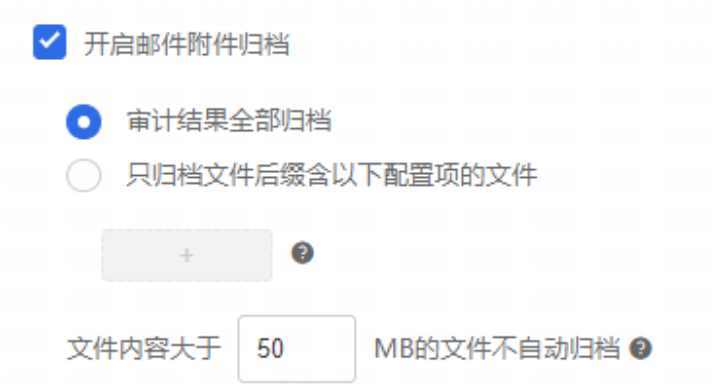
对终端通过邮件客户端/网页邮箱进行邮件外发行为的日志记录，支持对全部发件/收件地址或指定发件/收件地址的邮件发送行为的审计/不审计。

支持审计内容的配置：

针对协议数据的获取，支持特定软件的配置。

备注：协议和对应软件均配置完成，才可获取到协议内容。

归档：可针对所有邮件外发文件或包含指定后缀名的邮件外发文件备份到服务器上。

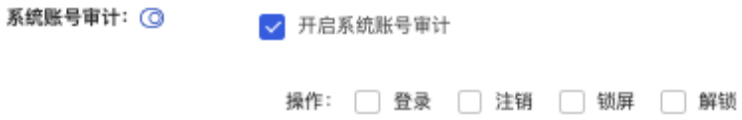


备注：目前 webmail 审计支持 163 和 qq 邮箱。

15.1.2.2.5. 系统账号审计

入口：数据安全>终端审计>策略管理

对终端系统账号的登录、注销、锁屏和解锁操作行为进行审计。



15.1.3. IM 软件库更新设置

IM 软件库更新设置，位于管理中心>系统管理>更新管理>数据安全，用于及时适配新版本的 IM 软件，增强行为审计中“IM 审计”的能力。目前管理中心提供了通用的默认设置，企业管理员可根据企业自身的特点来调整设置。

15.1.3.1. 系统更新设置

该模块设置 IM 软件库的更新时间，支持按月、周、天、小时周期性自动更新。

15.1.3.2. 终端更新设置

该模块设置全网终端更新 IM 软件库的时间，即 IM 软件库更新的灰度批次。

15.2. 信创终端审计

15.2.1. 基本思路

通过对终端计算机进行全面监控，包括文件的操作行为、外接设备挂载及卸载行为、打印行为、刻录行为以及网络访问等行为进行实时监控，提供详尽的行为审计日志，管理员可对上报的审计日志进行统一分析，及时发现单位内部终端计算机存在的安全隐患，保证内网主机的安全。

15.2.2. 策略设置

策略设置入口：管理中心>数据安全>终端审计>策略管理。客户端类型选择信创终端，信创终端支持终端策略，暂不支持用户策略。

审计策略包括系统监控、行为审计、文件监控、异常行为监控等。

系统监控：支持对系统登录、系统账户、系统服务、系统时间变更等信息进行监控和设置。

系统账户监控开启后，会对终端主机的账户进行监控，当有增加、修改、删除等账户操作，将产生审计日志。

系统服务可设置对用户添加的服务进行监控，匹配规则后终端生成审计日志并上报。

系统时间监控开启后，会对终端主机的系统时间进行监控，时间发生变更产生审计日志。

行为监控：针对打印行为、刻录行为、移动设备行为、上网行为、网路配置等的审计监控策略进行设置。

打印监控开启后将收集终端主机打印信息，包括文件名称、文件类型等；刻录信息开启后会收集终端主机刻录事件信息。

移动设备监控可设置监控类型，包括U盘和移动硬盘，可设置监控行为，包括设备插入拔出、数据流入流出、存储文件的操作行为（拷贝、打开、删除、修改）。

文件监控：设置文件监控策略，可设置具体的文件、文件夹，可指定文件格式，对指定的文件进行监控，并且产生审计日志。支持对文件的新建、删除、重命名、写入等行为监控，支持对文件篡改的监控，文件内容发生变化时上报告警日志。

异常行为监控：可以设置端口的监测周期、访问次数，在设定时间内，访问端口次数过多将告警，产生审计日志。ARP攻击可以设置局域网网关IP、局域网网关MAC，根据设定进行监控。

15.2.3. 审计日志

可按时间及分组对审计日志进行查询，可将审计日志导出报表，支持xls、pdf、图片等格式报表。

16. 移动存储

移动存储是奇安信天擎核心模块之一，是单独的授权模块。主要功能是针对移动存储介质的注册、授权的安全管理，实现按不同使用要求授予不同的权限，同时对移动介质进行状态管理，方便管理员进行集中管控。主要分为设备注册、设备分类授权、设备 ID 授权、挂失管理、外出管理、终端申请、跨服务器兼容管理（U 盘漫游），移动存储例外，安全 U 盘（自带文件审计）几大控制模块。

16.1. 基本概念

16.1.1. 设备注册

- 责任人

  管理注册 U 盘或者终端申请注册 U 盘时，需要设置的 U 盘责任人，方便管理员可以根据 U 盘信息定位到 U 盘使用人。

- 有效期

  有效期分为内网有效期和外网有效期，有效期到期后默认把 U 盘的授权权限取消，管理员可继续设置有效期。

- 状态

  显示当前 U 盘使用情况：是否停用等。

- 停用：

  将 U 盘内网授权全部取消

- 服务器 ID

加密U盘或者安全U盘注册时，会将管理中心的serverID写入U盘中，方便U盘判断内外网环境。

- 设备类型

  仅注册，加密U盘，安全U盘三种类型。

- 设备来源

  标识U盘注册来源信息，管理员管理中心注册或者终端申请

- 硬件信息

  显示U盘的PID/VID 厂商等硬件信息

- 设备分类

  加密U盘注册时，设置的分类信息，方便后期做分类授权。

- 漫游U盘

  显示U盘是否漫游U盘，可在U盘注册时设置。

- 申请终端

  U盘申请注册的计算机名称

16.1.2. 仅注册

- 仅注册

  仅注册只是将U盘ID记录在管理中心，不会将U盘格式化，即普通U盘注册。

- 普通U盘授权

  授权时会将U盘ID以及对应的权限下发至客户端。

- 普通U盘

  不支持漫游，外出管理等设置

16.1.3. 加密U盘

- 加密U盘注册

  将普通的第三方U盘进行格式化，会将U盘分成三个分区（启动区、加密区和内网交换区（可选）），默认插入电脑后，只可以看到5M空间

的启动区，在启动区内执行安全U盘程序并输入密码后，才可打开隐藏的加密分区

备注：若开启加密U盘支持信创终端功能，格式化后，U盘将新增一个启动区，用于存放信创终端的启动程序。

- 启动区

  加密U盘启动区里存放了加密U盘的启动程序，在内网环境下此分区是只读权限，在外网环境下无法限制启动区内的文件修改，当U盘启动区被修改后，再拿回内网使用时，会被客户端重新初始化将多余的文件清除（U盘登录页有提示）

- 加密区

  加密区在认证通过才显示该分区

- 内网交换区

  加密区在安装本网客户端时可不需要认证即可进行数据操作

- 加密U盘授权

  加密U盘可以采用类似普通U盘的ID方式授权，也可以采用设备分类授权

16.1.4. 设备分类

- 设备分类说明

  可以将一批U盘同时注册为一种分类，管理员只需将分类权限下发即可，无需再下发每个U盘的ID，提高终端响应速度，减少策略文件下发。

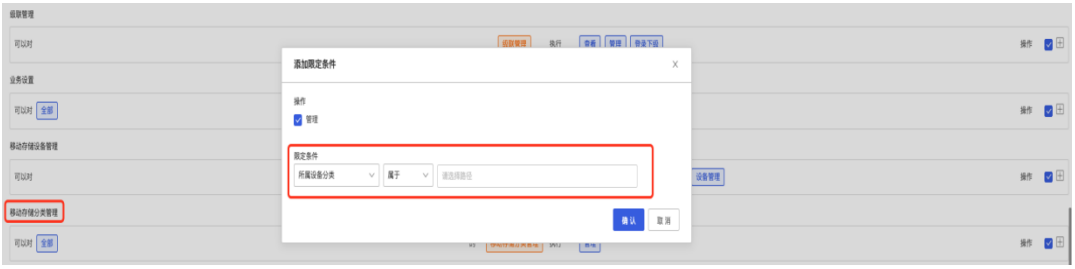
  设备授权逻辑：将U盘的ID以及对应的权限下发至客户端，这样U盘量巨大时，会需要所有U盘的ID和权限下发至每个终端，响应速度较慢。

  如分类授权和设备授权同时存在时，设备授权优先。简化U盘管理，建议使用此方案

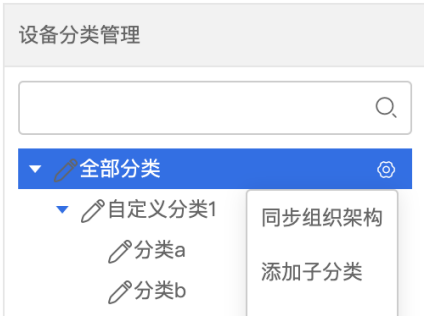
- 分类适用场景

综上所示分类授权机制适用于U盘量较大，且权限设置较为统一的用户

- 设备分类支持多级，分为自定义分类和自动同步分类两种类型，并可定义管理员对移动存储设备分类的查看和管理范围。



- 自动同步设备分类：系统支持设置将设备分类树与用户组织架构自动同步，同步后的U盘设备自动按照其设备责任人属性划归到相应的设备分类中。



16.1.5. 安全U盘

安全U盘是奇安信集团与第三方合作定制的一款硬件产品，具有病毒隔离，安全加密，离线审计等功能

- 安全U盘单位名称

  购买安全U盘后，安全U盘中的单位名称是获取的管理系统授权文件里的客户名称，如需正常管理安全U盘，需要将安全U盘在管理中心上重新注册即可。

- 安全U盘使用

  安全U盘授权支持设备ID授权，U盘插入电脑后只有光驱盘符，双击盘符后，才可打开启动区，执行安全U盘程序后，需要输入密码才可进入管理页面。

U 盘内部不能直接运行文件，只可做文件的导入导出工作。安全 U 盘除了只读，读写，禁用权限外，还支持只写权限。

- 安全 U 盘离线审计

  客户购买移动存储模块后，会默认开启审计模块中的安全 U 盘审计策略功能。设置此策略后即可实现安全 U 盘离线审计

  安全 U 盘的文件操作审计由 U 盘内置芯片完成，当离线情况下审计日志会缓存在 U 盘内部，接入内网后再上报日志

  普通 U 盘和加密 U 盘的审计需要审计模块中的文件操作策略实现，且只支持内网终端上生效。（审计模块是单独的授权，需要单独购买）

16.1.6. 外出管理

- 外出管理

  此功能适用于加密 U 盘和安全 U 盘。需将 U 盘插入管理员电脑，设置外出权限。

  外网环境：U 盘在未安装奇安信天擎的客户端以及安装了其他管理中心的客户端均认为是外网环境，默认执行外出权限：只读，读写，禁用。

- 外网判断逻辑

  加密 U 盘或者安全 U 盘内部在注册时会保存一份管理中心的 serverID，同时客户端本机也会保存一份 serverID。U 盘插入终端后会先比较双方 serverID 是否相同，如相同则走内网权限；如 serverID 不相同，则执行外网权限或者漫游权限。

16.1.7. 跨服务器兼容（U 盘漫游）

此场景适用于跨服务器 U 盘使用管理，采用 serverID 校验的方式，来实现不同服务器 U 盘设备的统一使用管理。管理员需要将需兼容服务器的 serverID 添加到管理中心，同时设置使用权限，最终实现跨服务器的设备兼容。

16.2. 基本功能

16.2.1. Windows 终端

16.2.1.1. U 盘注册

16.2.1.1.1. WEB 页面注册

注册入口：数据安全>移动存储>移动存储列表>U 盘注册。

WEB 注册 U 盘时，首次使用需要安装注册控件（页面自动提示）。控件安装后，系统自动检测当前插入电脑的 U 盘设备，并显示注册入口（若系统对插入的设备没有自动识别，请点击“刷新设备”进行页面刷新后操作）。

16.2.1.1.2. 客户端注册

注册入口：客户端右键>移动存储

将 U 盘插入装有客户端的电脑，且当前用户有直接注册 U 盘的权限时，终端 U 盘注册页面会自动识别当前 U 盘的注册状态，并提供相应的注册入口。

16.2.1.2. U盘注册类型

U盘注册前需注意服务器标识ID设置：

此ID默认与U盘做绑定，当外来U盘接入电脑时，或者本地加密U盘外出时，加密U盘内置的serverID会与终端的serverID做比对，如不一致则按照外网U盘来处理。

ServerID设置如下图所示：（数据安全>业务设置>移动存储）

注：修改服务器标识ID后，已注册的U盘会变更为外网U盘，请勿随意修改服务器标识ID!

该区域主要管理入网的移动存储介质注册，管理员根据介质的使用对象进行设定编号、名称及责任人，注册的移动介质可以按不同使用要求进行注册，分为需要或不需要密码验证、需要或不需要外出使用。

U盘插入电脑后，系统自动识别注册状态，U盘注册页面：

16.2.1.2.1. U 盘仅注册

普通 U 盘不可设置外出使用权限，注册完成后，列表显示注册记录，同时注册设备处于启用状态。

16.2.1.2.2. 加密 U 盘注册

加密 U 盘可设置外出权限和外出有效期；注册完成后，列表显示注册记录，同时注册设备处于启用状态。

- 加密 U 盘注册时，会进行数据格式化，提示弹窗如下：

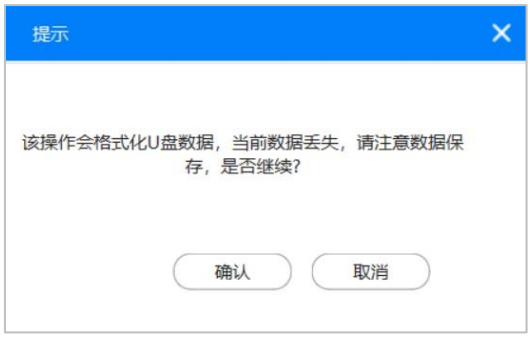
➢ 加密 U 盘注册成功后，会提示默认密码，如下图所示：

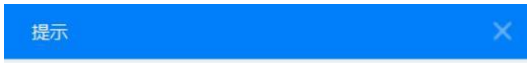
加密 U 盘双击启动区 QCMSafeUd.exe，在登录界面输入密码登录后，托盘任务栏中，可见 U 盘图标，右键该图标，可以修改该加密 U 盘密码，如下图所示：

16.2.1.2.3. 安全 U 盘注册

安全 U 盘不进行设备 UID 重新计算，设备硬件编号和设备 UID 相同。注册完成后，列表显示注册记录，同时注册设备处于启用状态。

➢ 安全 U 盘注册时，会进行数据格式化，提示弹窗如下：





备注：点击确认后，启动数据更新，在此过程中请勿插拔设备。

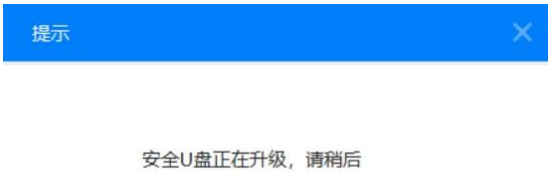
- 安全 U 盘注册成功后，会提示默认密码，如下图所示：

16.2.1.2.4. 兼容 V6 安全 U 盘

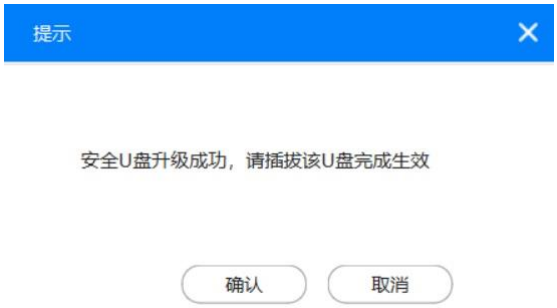
目前终端支持 V6 安全 U 盘设备的在线升级，升级后可在 V10 中注册使用。

- V6 安全 U 盘接入终端后，会提供“升级”入口。

➢ 点击升级后，系统会提示保持设备处于连接状态，如下图所示：



升级完成后，系统会提示插拔后完成生效，如下图所示：



备注：设备再次接入后，展示注册入口。

16.2.1.2.5. 已注册 U 盘管理

已完成注册的 U 盘，管理员可对 U 盘做进一步包括密码重置、换绑用户、取消注册等后续管理。系统提供 WEB 页面和客户端两种场景的已注册 U 盘管理：

16.2.1.2.5.1. Windows 客户端管理模式

注册入口：客户端右键>移动存储

插入终端电脑后，若当前客户端登录的用户有管理权限，则自动根据 U 盘的注册状态对已注册 U 盘显示其它操作入口：

16.2.1.2.5.1.1. 信息展示

终端接入 U 盘的条件下，点击【信息展示】，可查看终端已接入 U 盘的信息。

16.2.1.2.5.1.2. 取消注册

终端接入 U 盘的条件下，点击【取消注册】，可以取消已注册的移动存储介质的登记信息。

注册 U 盘取消注册后，移动存储列表不可见该 U 盘记录。

注：U 盘取消注册时，加密 U 盘和安全 U 盘会进行数据格式化，请谨慎操作。

16.2.1.2.5.1.3. 密码重置

终端接入 U 盘的条件下，点击【密码重置】，为忘记 U 盘登录密码提供密码重置功能。

密码重置成功后，会提示默认密码，如下图所示：

注：为防泄密，安全 U 盘重置密码会格式化 U 盘数据，请谨慎操作。

16.2.1.2.5.1.4. U 盘外出

终端接入 U 盘的条件下，点击【U 盘外出】，在弹出界面上进行外出权限设置和外出有效期设置。

注：

1) 安全 U 盘：外出权限支持禁止、读写、只读和只写，不能设置外出有效期和外出使用次数；
2) 加密 U 盘：外出权限支持禁止、读写和只读，支持设置外出有效期和外出使用次数；
3) 普通 U 盘无外出权限。

16.2.1.2.5.1.5. 换绑用户

终端接入 U 盘的条件下，点击【换绑用户】，为需要更新设备责任人的加密 U 盘提供责任人和设备分类重置功能。

16.2.1.2.5.2. WEB 页面管理模式

管理入口：数据安全>移动存储>移动存储列表>U 盘注册

插入终端电脑后，系统自动识别硬件设备和注册状态，对于已注册的 U 盘设备，提供与客户端管理模式相同的管理功能。

注：操作页面与客户端管理模式一致。

16.2.1.3. 信创终端

16.2.1.3.1. U盘注册

16.2.1.3.1.1. WEB页面注册

注册入口：数据安全>移动存储>移动存储列表>U盘注册。

WEB注册U盘时，首次使用需要安装注册控件（页面自动提示）。控件安装后，系统自动检测当前插入电脑的U盘设备，并显示注册入口（若系统对插入的设备没有自动识别，请点击“刷新设备”进行页面刷新后操作）。

16.2.1.3.1.2. 客户端注册

注册入口：客户端右键>移动存储管理

将U盘插入装有客户端的电脑，默认进入设备信息查看界面，点击“U盘注册”，进入到U盘注册界面。

16.2.1.3.2. U 盘注册类型

U 盘注册前需注意服务器标识 ID 设置：

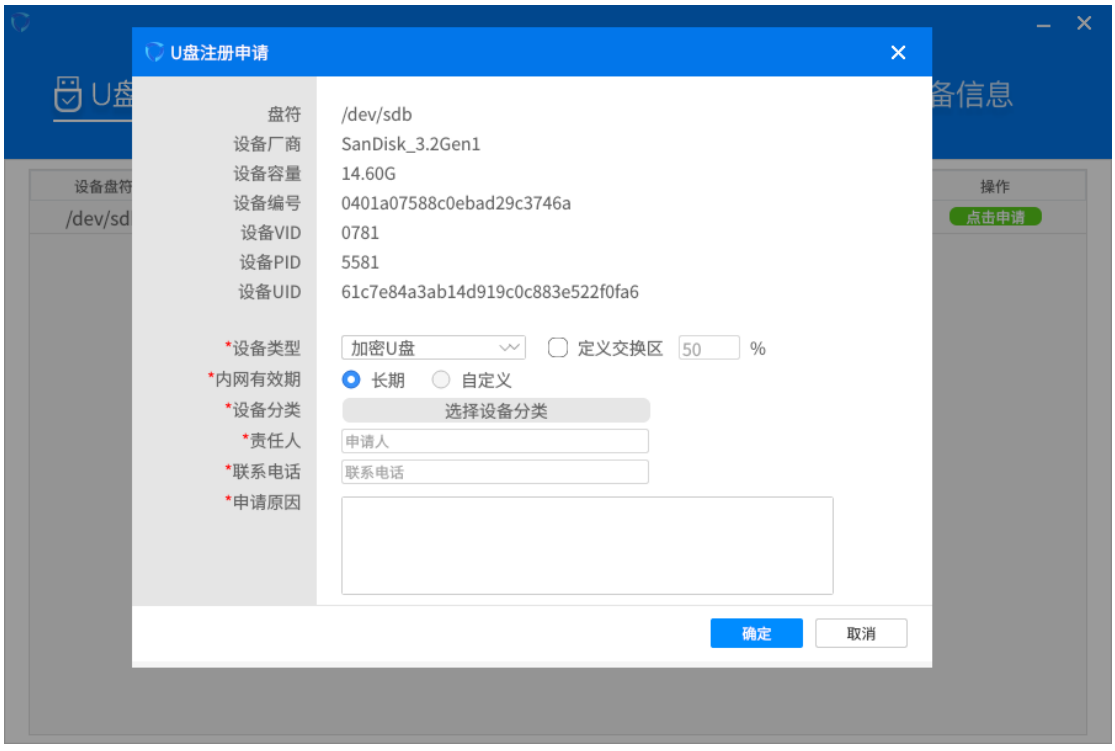
此 ID 默认与 U 盘做绑定，当外来 U 盘接入电脑时，或者本地加密 U 盘外出时，加密 U 盘内置的 serverID 会与终端的 serverID 做比对，如不一致则按照外网 U 盘来处理。

ServerID 设置如下图所示：（数据安全>业务设置>移动存储）

注：修改服务器标识 ID 后，已注册的 U 盘会变更为外网 U 盘，请勿随意修改服务器标识 ID！

该区域主要管理入网的移动存储介质注册，管理员根据介质的使用对象进行设定编号、名称及责任人，注册的移动介质可以按不同使用要求进行注册，分为需要或不需要密码验证、需要或不需要外出使用。

U 盘插入电脑后，默认进入设备查看界面，需要点击 U 盘注册，进入 U 盘注册页面：



16.2.1.3.2.1. U盘仅注册

普通U盘不可设置外出使用权限，注册完成后，列表显示注册记录，同时注册设备处于启用状态。

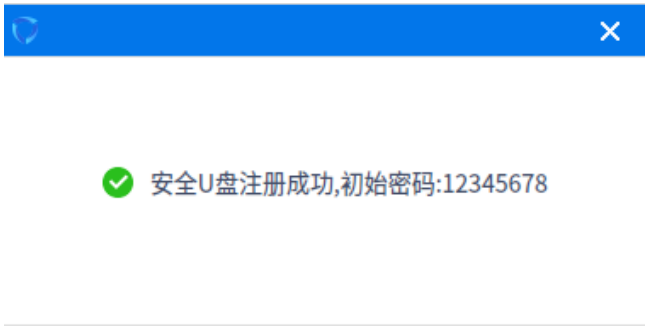
16.2.1.3.2.2. 加密U盘注册

加密U盘可设置外出权限和外出有效期；注册完成后，列表显示注册记录，同时注册设备处于启用状态。

16.2.1.3.2.3. 安全U盘注册

安全U盘不进行设备UID重新计算，设备硬件编号和设备UID相同。注册完成后，列表显示注册记录，同时注册设备处于启用状态。

- 安全U盘注册时，会进行数据格式化；
- 安全U盘注册成功后，会提示默认密码，如下图所示：



16.2.1.3.3. 已注册U盘管理

已完成注册的U盘，管理员可对U盘做进一步包括密码重置、换绑用户、取消注册等后续管理。系统提供WEB页面和客户端两种场景的已注册U盘管理：

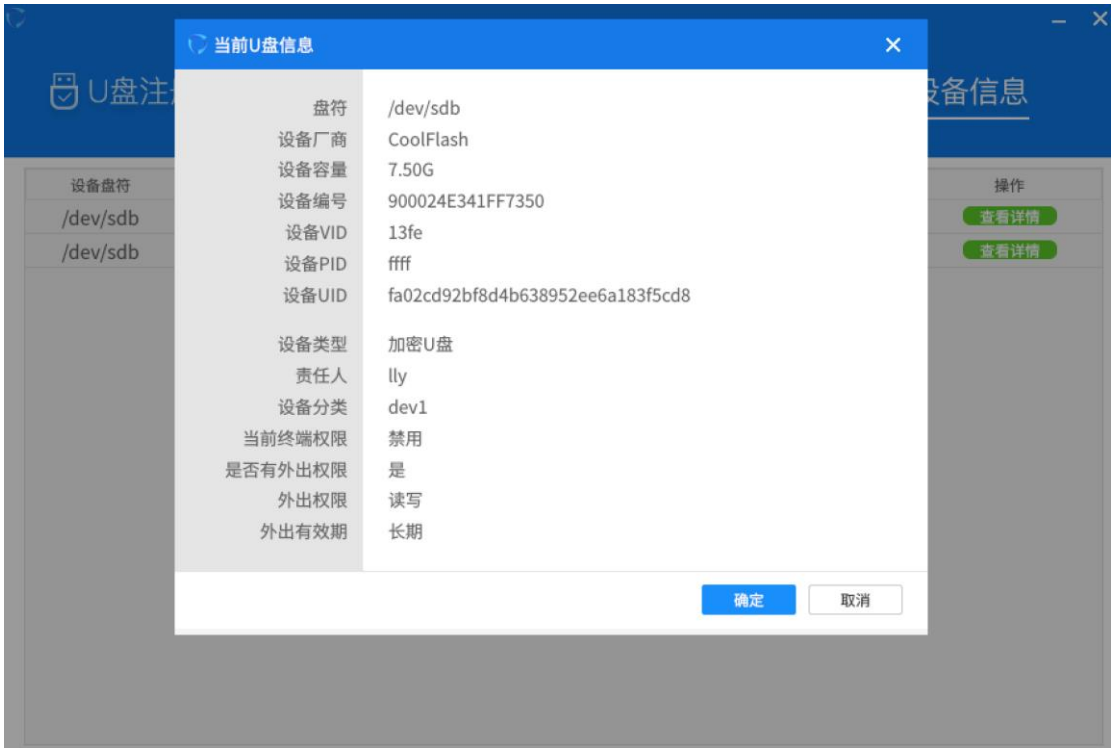
16.2.1.3.3.1. 信创终端管理模式

注册入口：客户端右键>移动存储管理

插入终端电脑后，默认页面为设备信息页面：

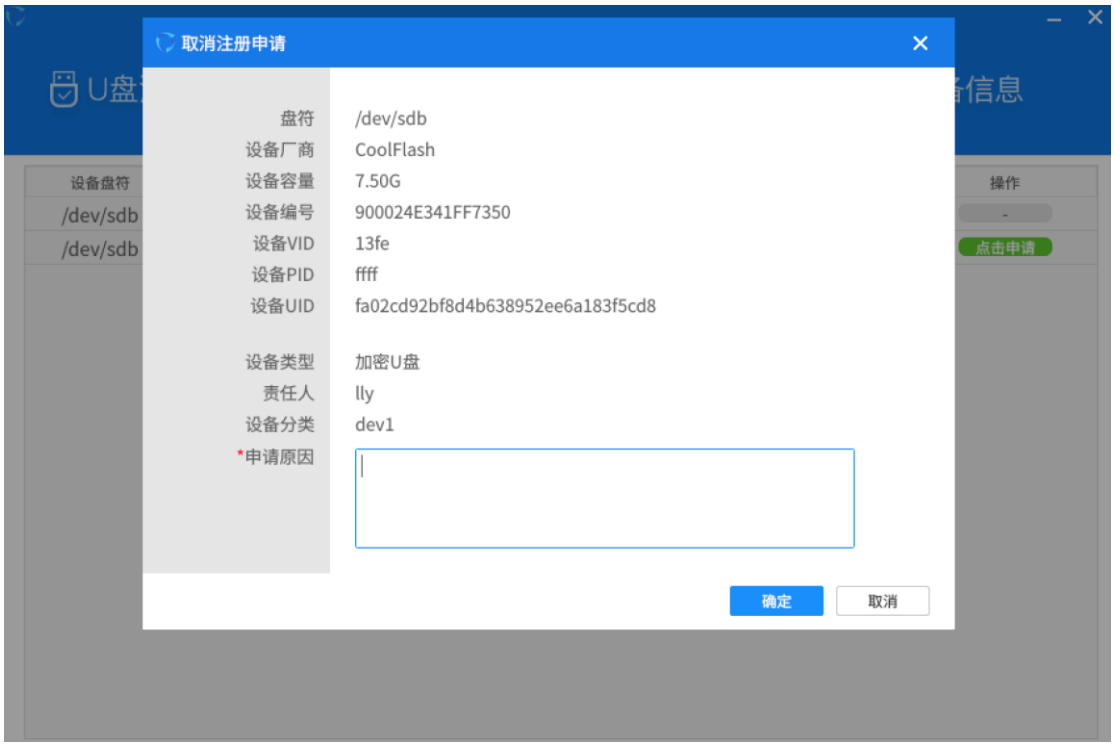
16.2.1.3.3.1.1. 信息展示

终端接入U盘的条件下，默认进入设备信息界面，点击【查看详情】，可查看终端已接入U盘的信息。



16.2.1.3.3.1.2. 取消注册

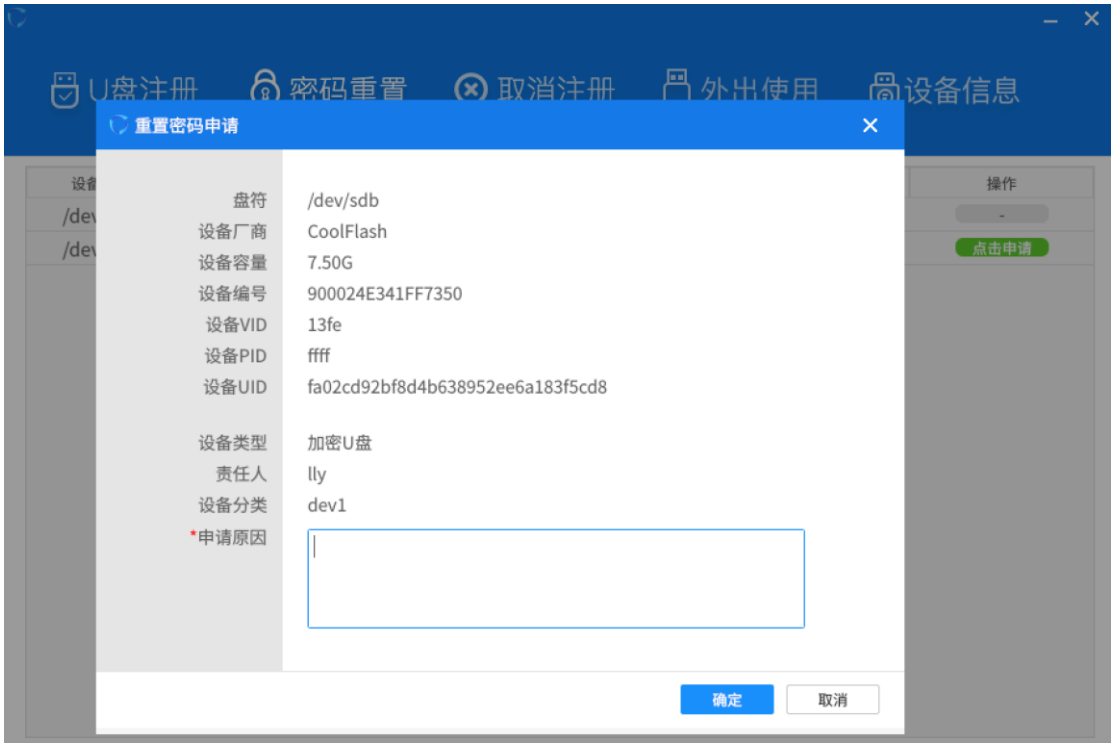
终端接入U盘的条件下，进入取消注册界面，点击【点击申请】，可以取消已注册的移动存储介质的登记信息。



注：U盘取消注册时，加密U盘会进行数据格式化，请谨慎操作。

16.2.1.3.3.1.3. 密码重置

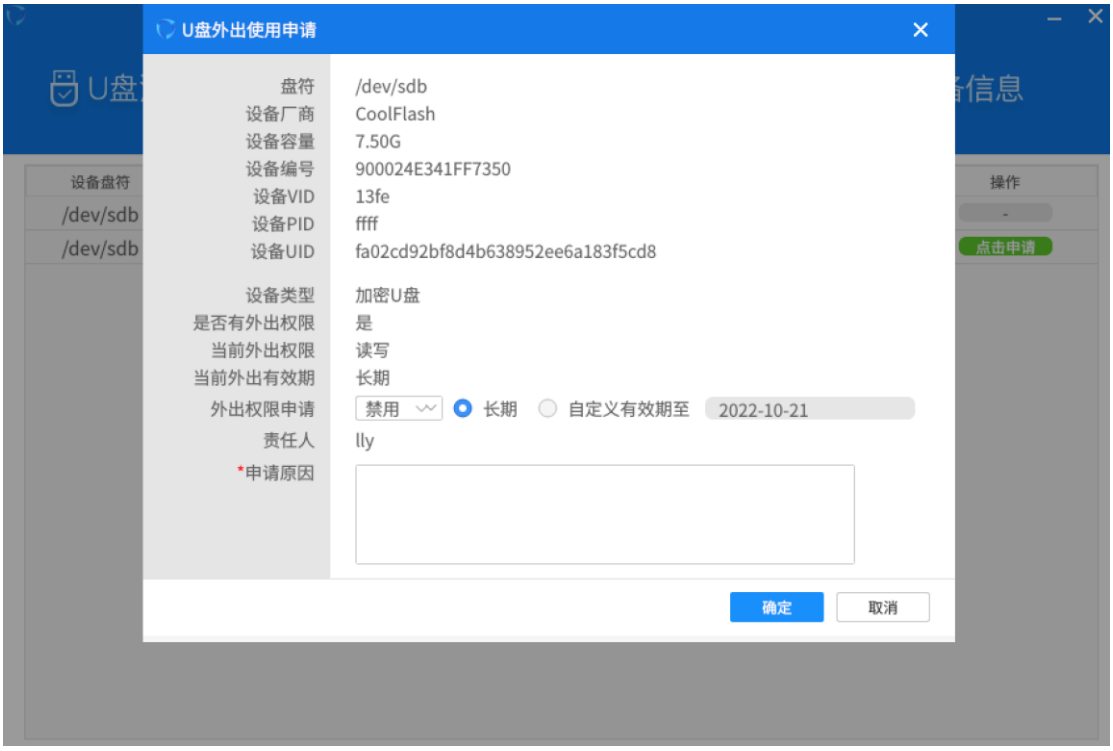
终端接入U盘的条件下，进入密码重置界面，点击【点击申请】，为忘记U盘登录密码提供密码重置功能。



密码重置成功后，会提示默认密码，如下图所示：

16.2.1.3.3.1.4. U 盘外出

终端接入 U 盘的条件下，进入外出使用界面，点击【点击申请】，在弹出界面上进行外出权限设置和外出有效期设置。



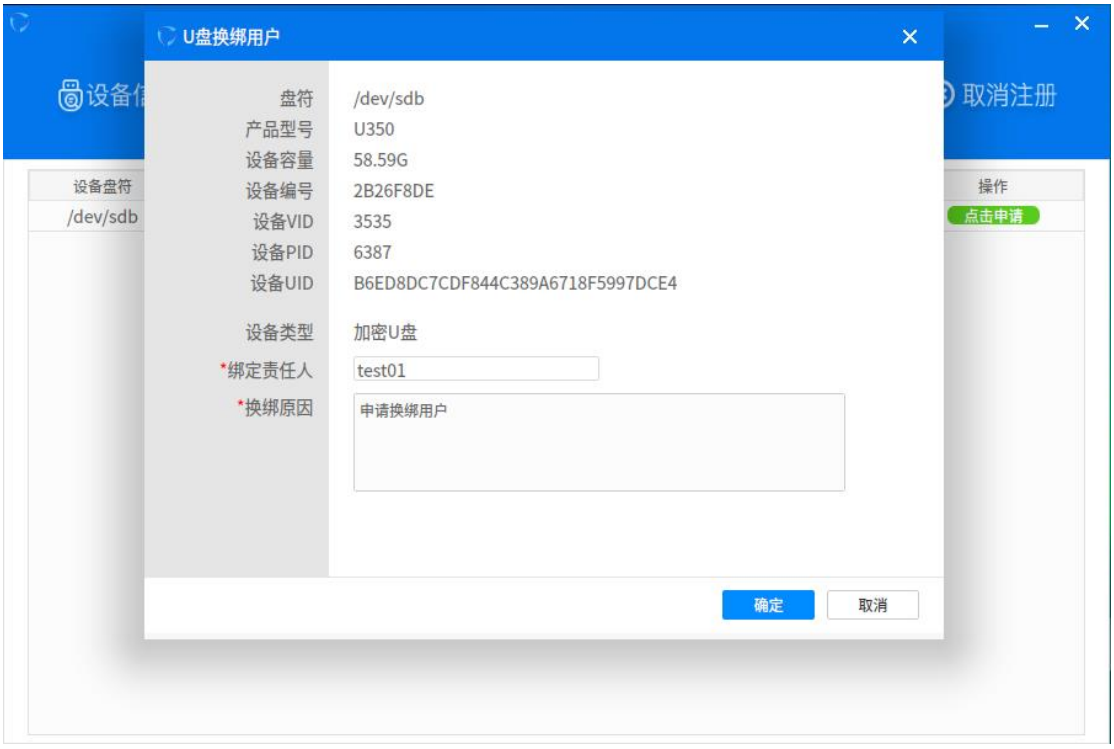
注：

1）加密 U 盘：外出权限支持禁止、读写和只读，支持设置外出有效期；

2）普通 U 盘无外出权限。

16.2.1.3.3.1.5. 换绑用户

终端接入 U 盘的条件下，点击【换绑用户】，为需要更新设备责任人的加密 U 盘提供责任人和设备分类重置功能。



16.2.1.3.3.2. WEB 页面管理模式

管理入口：数据安全>移动存储>移动存储列表>U 盘注册

插入终端电脑后，系统自动识别硬件设备和注册状态，对于已注册的 U 盘设备，提供与客户端管理模式相同的管理功能。

注：操作页面与客户端管理模式一致。

16.2.1.4. U 盘使用管理

管理员根据移动介质管理的需要，可以对已注册的移动介质进行授权管理。

16.2.1.4.1. 单设备使用权限分配

U 盘注册后，系统支持单独将使用权限分配给以下使用对象：

使用对象	可分配权限
终端	只读、读写、禁用
终端分组	只读、读写、禁用
用户	只读、读写、禁用
用户分组	只读、读写、禁用

备注：目前信创终端暂不支持用户维度的授权分配。

16.2.1.4.2. 设备分类使用权限分配

系统支持按照设备分类批量将 U 盘使用权限分配给以下使用对象：

使用对象	可分配权限
终端	只读、读写、禁用
终端分组	只读、读写、禁用
用户	只读、读写、禁用
用户分组	只读、读写、禁用

备注：目前信创终端暂不支持用户维度的授权分配。

16.2.1.4.3. 使用权限优先级

设备给用户>设备给用户组>设备分类给用户>设备分类给用户组>设备给终端>设备给终端组>设备分类给终端>设备分类给终端组。

16.2.1.4.4. U 盘停用、启用、内网有效期、删除、调整设备分类

管理员根据 U 盘管理的需要，可以对已注册 U 盘进行启用、停用、删除、设置内网有效期和调整设备分类。

启用、停用、删除：可以对已注册的介质注册信息进行状态启用、停用或者删除操作。

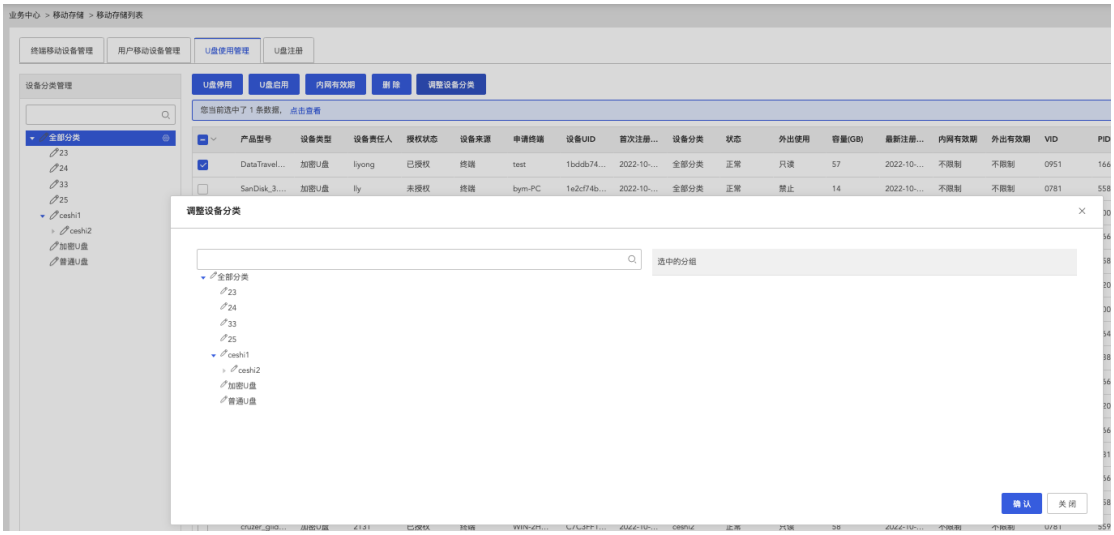
选择列表记录“U 盘停用”或“U 盘启用”，可以控制列表 U 盘的状态是“停用”或“正常”；

点击“删除”，可从列表删除 U 盘记录，对应 U 盘接入该管理中心下终端，判断该 U 盘非内网 U 盘。

选择设备，点击“内网有效期”，可以控制移动存储介质在内网使用的有效期。

注：U 盘为停用状态或 U 盘内网有效期到期后，U 盘为禁用权限。

选择设备，点击“调整设备分类”，可调整已注册移动存储介质的所属设备分类。



16.2.1.4.5. 终端移动设备管理

以终端视角查看已分配的 U 盘使用权限，并可一键修改已授权给当前终端的使用权限。

16.2.1.4.6. 用户移动设备管理

16.2.1.4.6.1. 用户列表

以用户视角查看已分配的U盘使用权限，并可一键修改已授权给当前用户的使用权限。

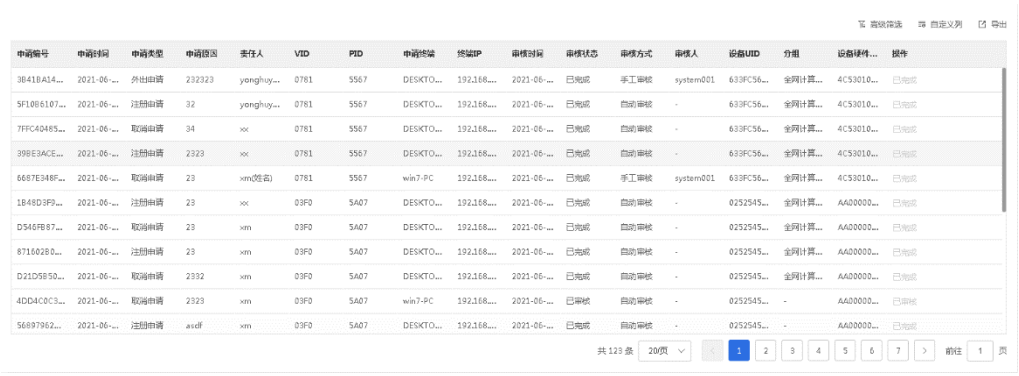
16.2.1.4.6.2. 设备列表

以设备资产视角查看当前用户分组下已注册的U盘设备。

16.3. 移动存储申请审核

当客户端没有登录用户信息，或者登录的用户没有注册U盘的权限时，可以由客户端发起U盘注册申请，管理员在管理中心审核的方式完成U盘的申请审核。

管理员登录管理中心，进入数据安全>移动存储>移动存储审核界面，管理员在该界面可完成对客户端申请的审核处理。



可通过小铃铛消息通知，直接跳转到对应的审核界面。

审核完成后，终端将收到审核结果通知。

16.4. 移动存储全局设置

设置入口：数据安全>业务设置>移动存储

16.4.1. 移动存储服务器标识 ID

移动存储服务器标识 ID（又叫 server ID），在 U 盘注册时，会写入 U 盘头文件，通过 server ID 对 U 盘使用的终端环境进行内外网判断。

每一个管理中心在导入授权时会默认生成一个唯一的标识 ID，未经过管理中心注册的 U 盘中不存才 serverID，判定 U 盘为未授权。

允许运维人员对管理中心的 serverID 进行修改，修改后，会导致已注册 U 盘的使用权限发生变更，因此，会提示运维人员“请注意，修改服务器标识后，已注册的加密 U 盘会变更为外网 U 盘，请注意备份！”。

【注意】服务器标识 ID 修改操作属于高风险操作，并且配置后会全局生效，修改后可能导致整个内网已注册的设备无法识别，进而影响已注册设备的相关使用。为了避免出现误操作事件，建议如下：

如果有明确诉求需要修改服务器标识 ID，可在测试环境中修改并验证效果后，再在正式环境中进行操作。

16.4.2. 跨服务器兼容设置

针对跨服务器 U 盘使用的管理。启用功能后，可以设置允许使用的服务器标识 ID，并控制外来 U 盘的使用权限。

16.4.3. U 盘统一配置管理

为简化 U 盘注册流程，更方便管理员进行 U 盘注册运维，业务设置-移动存储页对 U 盘的部分属性进行统一管理，主要影响 U 盘注册时的初始化设置和初始化权限。

- 注册 U 盘时责任人绑定用户：开启后，终端申请注册 U 盘时需校验用户名密码的正确性；

  备注：目前信创终端暂不支持责任人绑定用户功能。

- 移动存储设备定义：通过移动存储容量的定义，明确设备管控范围；
- 首次登录强制修改密码：开启后，加密 U 盘和安全 U 盘首次登录，以及重置密码后的首次登录，均会强制修改密码。
- 加密 U 盘支持信创终端：开启后，注册后的加密 U 盘支持在信创终端的使用。
- 注册 U 盘时强制输入申请理由：开启后，设备注册、取消注册、换绑、重置密码以及申请外出权限时，均需要输入申请理由；
- 加密 U 盘权限变更生效方式：支持设置加密 U 盘权限变更时的生效方式，默认配置“下次使用生效”；
- 注册 U 盘登录界面显示：设置登录界面显示信息；
- 加密 U 盘注册设置：支持设置加密 U 盘密码尝试次数以及默认外出权限；

➢ 安全U盘注册设置：支持设置安全U盘密码尝试次数以及默认外出权限。

16.4.4. 加密U盘个性化设置

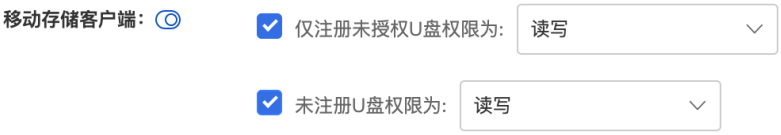
管理员在注册加密U盘时，可对U盘的显示名称进行个性化设置。

16.5. 移动存储策略

策略入口：数据安全>移动存储>策略管理。

16.5.1. 未注册U盘和未授权U盘的初始使用设置

对于没有在管理中心注册的U盘，和在管理中心已经注册但未做授权的U盘，默认使用权限分别定义。



16.5.2. 终端提示策略设置

支持设置终端对于接入U盘的权限提示，终端用户可在U盘接入时了解使用权限。

16.5.3. 移动存储客户端策略设置

- 支持未通过域认证的终端禁止发起 U 盘申请

  备注：信创终端不支持域认证
- 支持终端离线状态下移动存储权限控制
- 支持直接禁止使用移动存储设备

16.5.4. 安全 U 盘审计策略设置

支持对注册安全 U 盘的使用行为进行日志审计，并支持文件操作的后缀名过滤

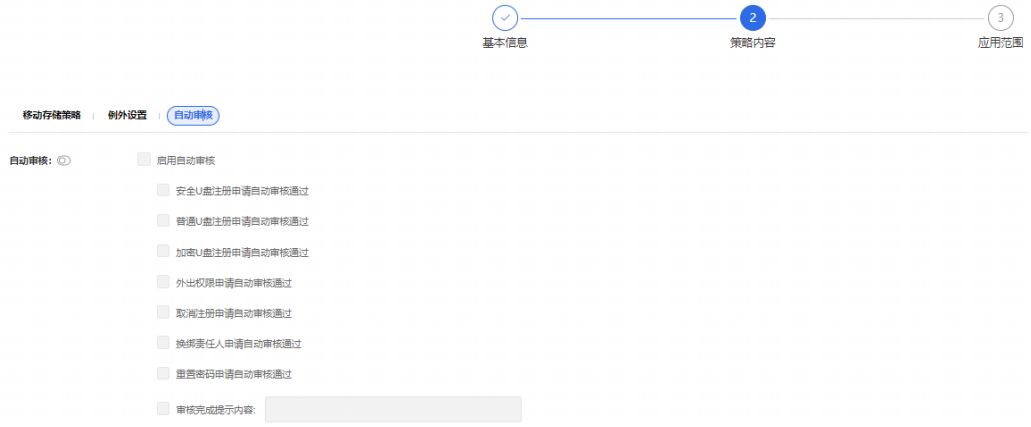
16.5.5. 移动存储例外

当移动存储模块误禁某些设备后，可以使用此功能做放行处理。通过管理中心>数据安全>移动存储>策略管理，TAB-例外设置对移动存储介质例外进行配置。

点击【添加】，在添加界面选择例外“内容”，输入对应的内容项，点击【确定】，即可完成例外规则添加。移动存储例外支持设备产品型号例外，VID/PID 例外和设备硬件编号/设备 UID 例外三种例外方式。移动存储例外权限支持读写和只读两种例外类型。

16.5.6. 自动审核

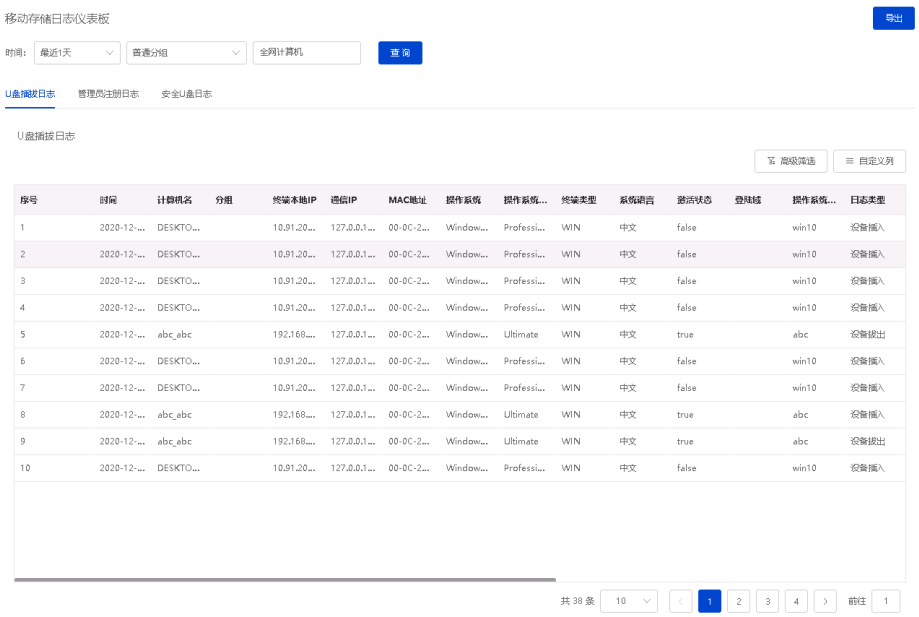
当客户端发起U盘审计时，管理员可以配置自动审核规则对客户端申请完成自动审核。



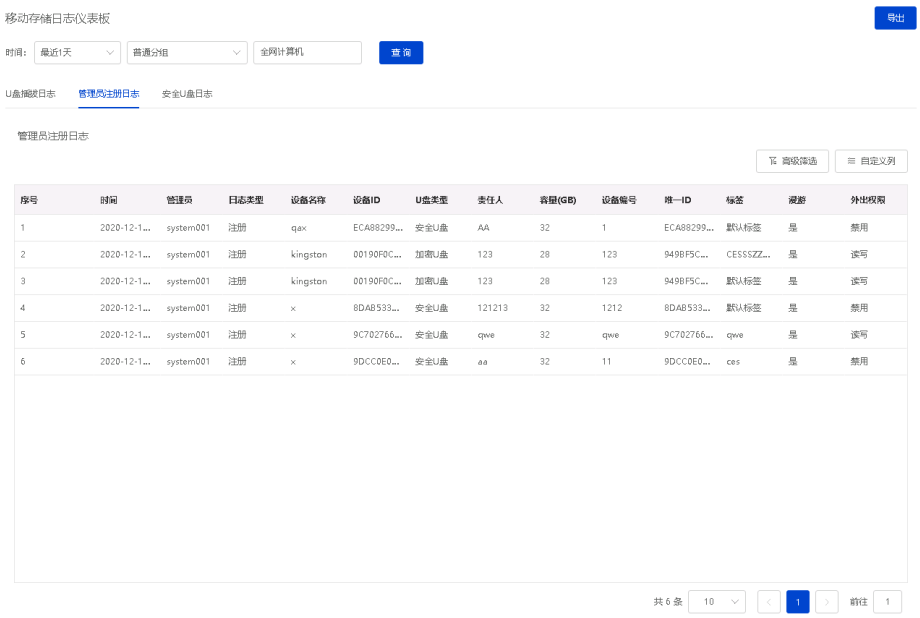
16.6. 移动存储日志

通过管理中心：业务管理>移动存储>移动存储日志，查看移动存储介质相关管理日志。

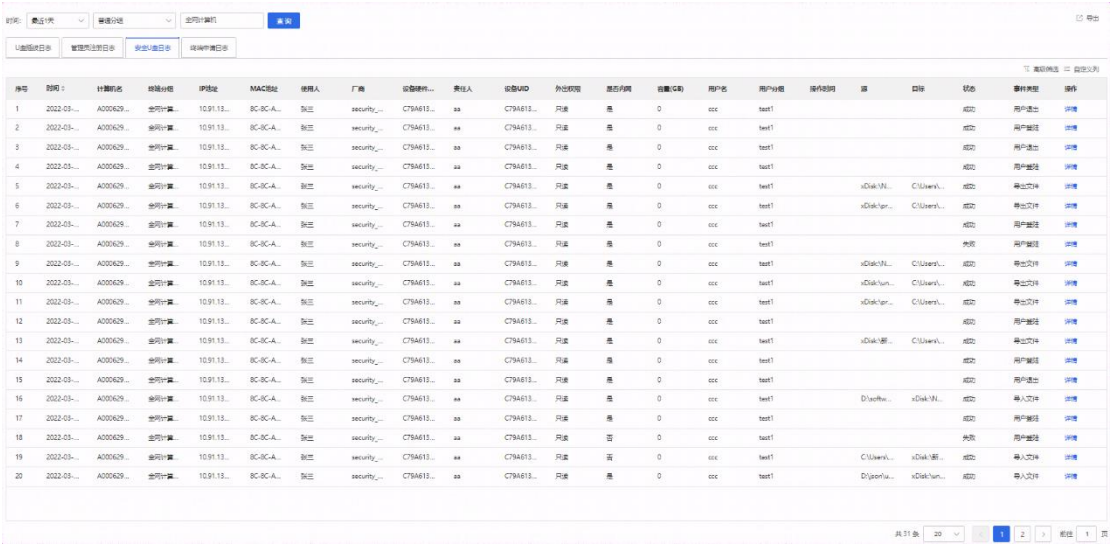
16.6.1. U盘插拔日志



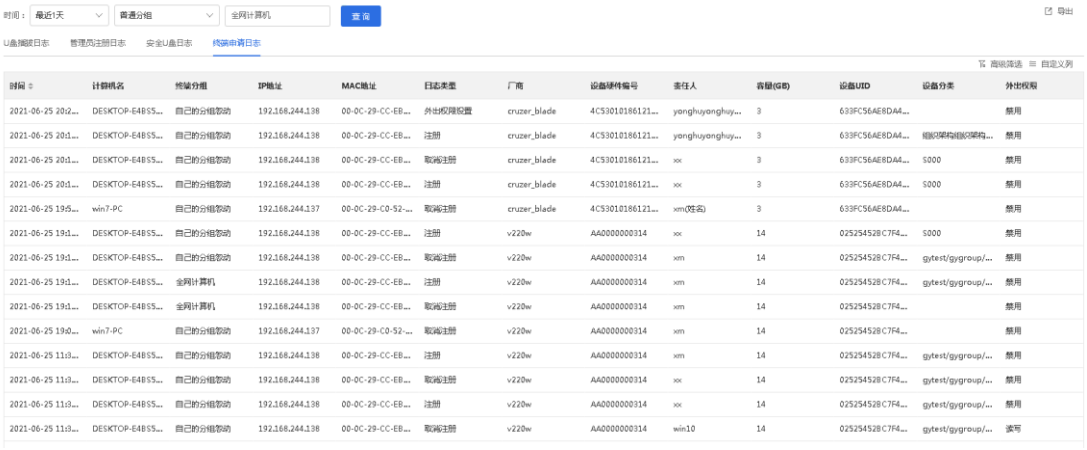
16.6.2. 管理员注册日志



16.6.3. 安全U盘日志



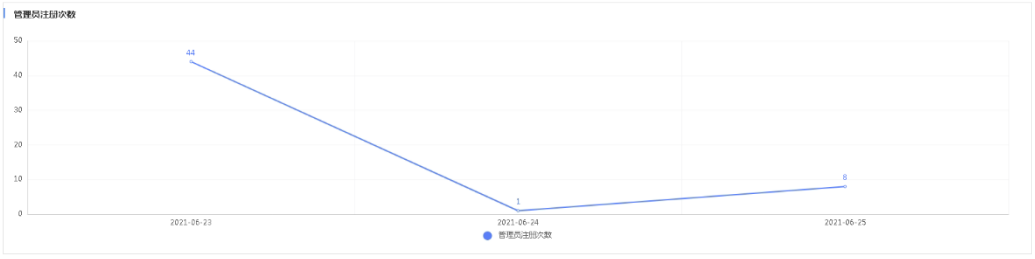
16.6.4. 终端申请日志



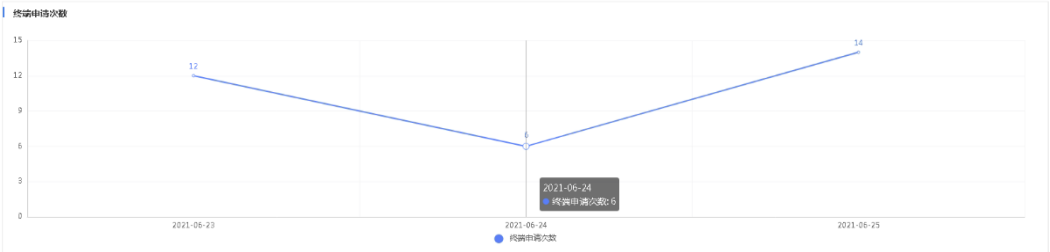
16.7. 移动存储报表

通过数据安全>移动存储>移动存储报表，查看移动存储介质相关信息统计。

管理员注册次数趋势图

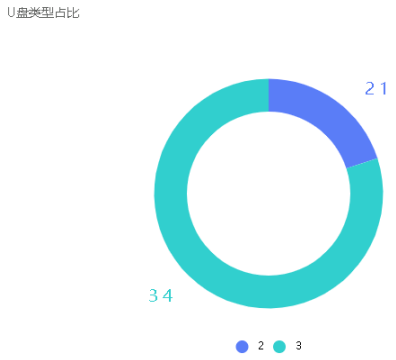


16.7.1. 终端申请次数趋势图



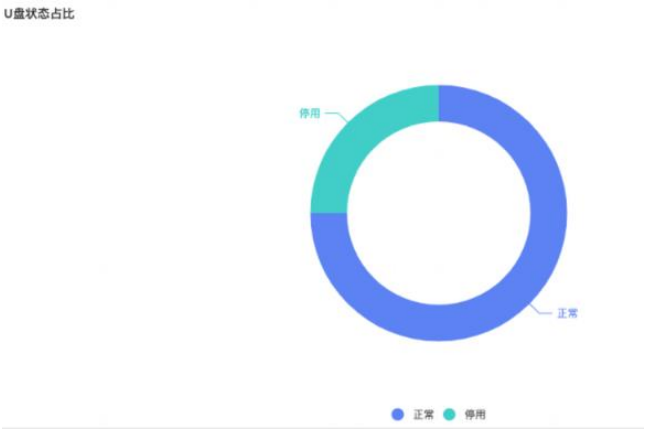
16.7.2. U盘类型占比统计

U盘类型：仅注册，加密U盘，安全U盘。

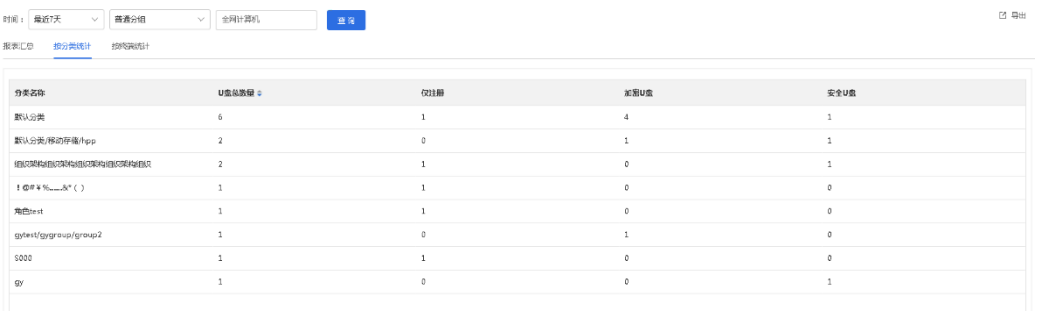


16.7.3. U盘状态占比统计

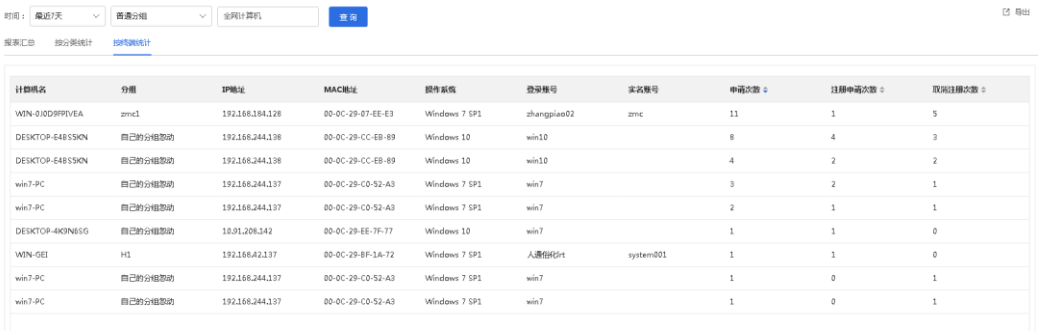
U盘状态：正常，停用，删除，取消注册。



16.7.4. 按分类统计各类型的注册U盘数量



16.7.5. 按终端统计各类型的注册U盘数量



16.8. 典型场景

16.8.1. 如何设置终端默认所有未授权U盘权限为禁用

16.8.1.1. 实现目的

设置终端默认情况下所有未授权U盘权限为禁用。

16.8.1.2. 操作步骤

数据安全>移动存储>策略管理，给全网计算机制作并下发未授权设备使用权限为禁用的策略，终端在接收到策略后，默认所有插入未授权U盘均为禁用权限。

16.8.1.3. 提示消息设置

开用提示消息后，U盘插入终端后，终端会自动判断U盘权限，并弹框提示。

16.8.2. 注册U盘为加密分类盘及使用说明

16.8.2.1. 实现目的

注册U盘为加密U盘，且明确设备分类。

16.8.2.2. 注册步骤

16.8.2.2.1. 注册信息填写

- 选择设备类型为加密注册设备
- 输入责任人信息
- 分类说明：多个设备可注册为同一种分类，管理员可针对分类类别下发使用权限。

16.8.2.2.2. 业务设置

可设置 U 盘密码复杂度、密码是否强制修改、密码尝试次数

点击注册

注册为加密 U 盘需要将 U 盘格式化。注意 U 盘文件保存。

16.8.2.2.3. 注册成功

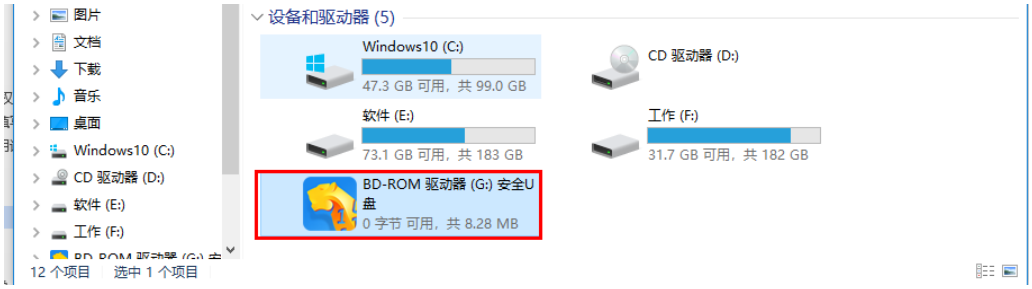
注册成功后，会提示加密 U 盘初始密码

注册成功后，U 盘效果

加密 U 盘登录页面

16.8.3. 安全 U 盘使用

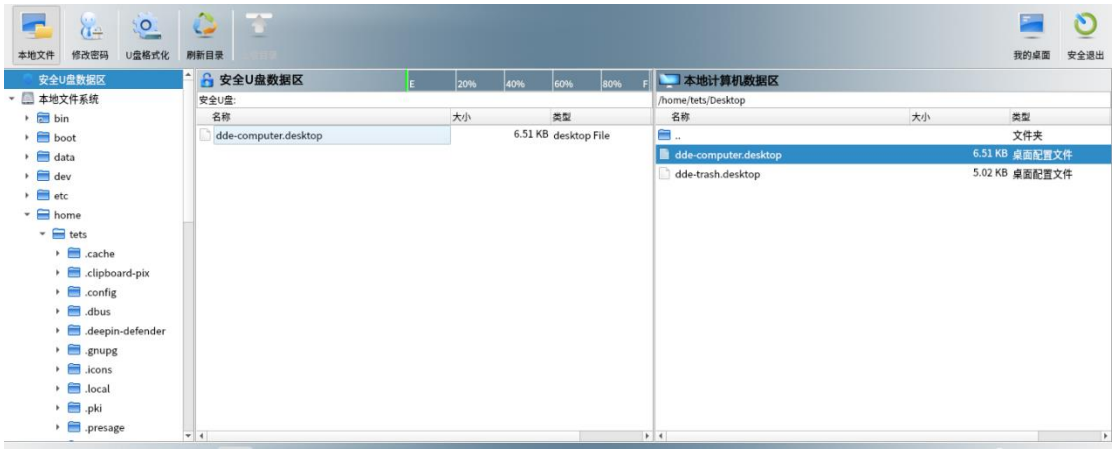
16.8.3.1. 安全 U 盘登录



默认密码 12345678

16.8.3.2. 文件导入以及导出

仅需要在本地计算机数据区以及安全 U 盘数据区进行文件拖拽即可。



17. 安全空间

17.1. 基本概念

17.1.1. 安全空间

指在电脑中构建出安全的工作环境，通过管理员赋予权限可有安全空间的使用权，安全空间内的一切操作将会被严格保护。

17.1.2. 个人空间

电脑上非安全空间的区域，统称为个人空间。即员工自己的个人环境，该系统不会对该环境进行任何操作，员工在个人环境中的任何行为，将不会记录。

17.1.3. 安全空间授权

安全空间内数据默认保存在空间内，不允许外出。管理员可以通过策略中对空间内部分通道进行授权，允许数据外出。目前已支持的授权有剪切板导出导入、文件导出、文件导入、防截屏、屏幕水印、打印控制、打印水印、samba 共享、无痕模式、链接自适应、空间应用等。

剪切板导出：空间内数据可禁止/解密外发（记录外发内容）/允许通过剪切板外发至其他空间或个人空间。

剪切板导入：个人空间内数据可禁止/允许通过剪切板外发至安全空间中。

文件导出：空间内文件通过粘贴复制/拖拽/另存等方式导出至个人空间。

文件导入：个人空间内文件通过粘贴复制/复制/另存等方式导入到安全空间。

防截屏：防止个人空间进程通过截屏获取安全空间内界面数据。

屏幕/打印水印：空间内运行进程/打印展示水印内容。

打印控制：可允许/禁止/允许部分打印机通过打印将空间内数据外泄出去。

Samba 共享：空间内数据可通过 samba 方式共享至其他员工。

无痕模式：默认情况下，空间内的数据会留存在空间内。安全空间提供无痕模式，即空间关闭后清除一切用户数据。

链接自适应：安全空间/个人空间有对应的网络访问控制列表。提供用户在个人空间内访问安全空间网络资源时，可直接跳转至安全空间内浏览器并成功访问；安全空间内反之亦然。提供用户网络资源访问的便捷性。

空间应用：为方便用户在空间内使用软件，管理员可配置相关进程，则安全空间在初始化时将快捷方式自动复制至空间内，用户直接双击即可使用该软件。

17.2. 安全空间管理

17.2.1. 业务说明

安全空间管理可以根据客户物业资源的等级划分不同的空间并对空间进行预先定义，进一步提供给安全空间业务进行策略配置。

17.2.2. 空间定义基本元素

空间名称：定义该空间的名称。

空间标签：即空间名称的缩称，用于管理端/客户端各个展示的界面。

空间加密算法即密钥长度：每个空间都采用磁盘加密的方式对落地数据保护。其中加密的算法和密钥长度在空间首次定义时可以配置，空间一经激活不可更改。目前支持的有 SM4、AES256。

空间等级：安全空间的等级是由系统管理员设置的不同安全级别，个人空间的等级为最低等级，安全空间的等级比个人空间要高。

允许安装应用列表：即允许在空间内安装的应用信息列表。在该列表内配置的应用，可直接在空间内点击安装操作，实际安装至个人空间。

窗口设置：可以设置不同的主题颜色，应用至个人空间，方便用户区分不同空间。

打印水印：配置打印水印相关参数，包括不限于水印内容、透明度、字体大小、水印角度、文字颜色、页眉页脚信息、应用进程等。

屏幕水印：配置屏幕水印相关参数，包括不限于水印内容、文字大小、水印角、应用进程等。

安全应用空间：该类进程和空间绑定，仅允许在空间内运行。在该列表内的进程即使在个人空间启动，运行中数据也将被落地至安全空间内。

17.2.3. 空间添加/维护

系统中允许添加安全空间数量至多 100 个，根据业务类型定义空间，完成后需激活该空间方可在策略中引用。

空间不允许删除，可以通过废弃方式不允许新策略中引用该空间。

激活方式有两种：

17.3. 基本功能

17.3.1. 安全空间运维基本思路

奇安信天擎安全空间的设计理念是将计算机分为两个区域：工作区域和个人区域。在工作区域仅能访问业务资源，且对工作区域内相关操作进行管控，实现办公数据落地安全；个人区域内的任何行为将不受任何影响。

策略下发时根据人员组织、身份不同可以配置空间使用权限。

安全空间内多网切换模块（单独 License 控制）支持在终端上达到通过切换方式切换不同的网络，详见【多网切换】章节。

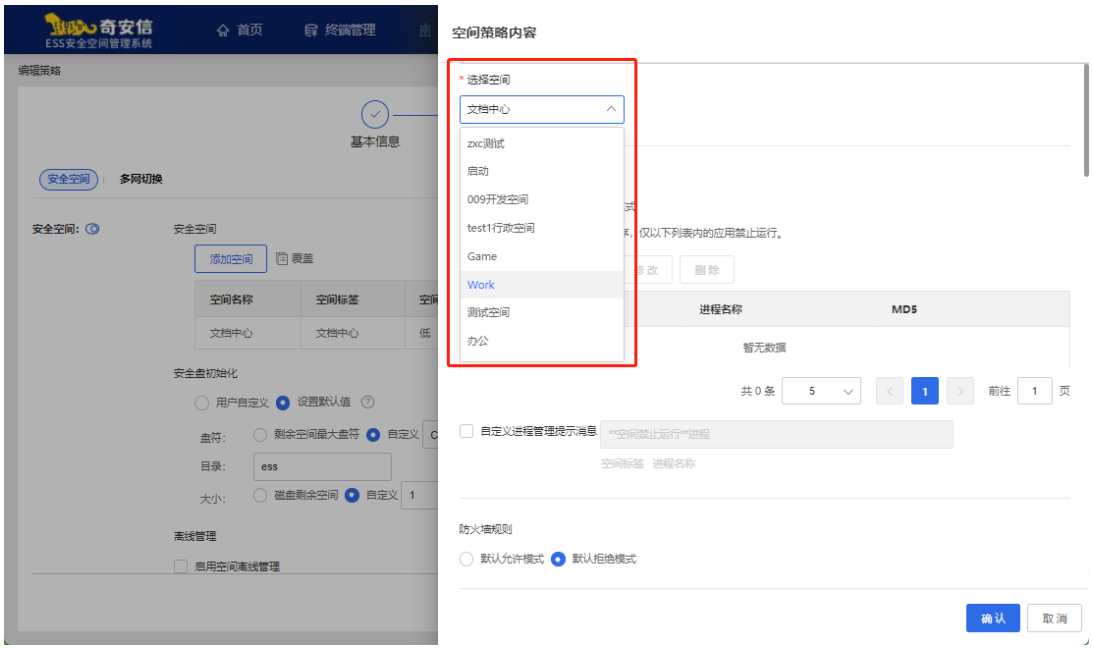
关联文档：《奇安信终端安全工作空间系统 V10.0R7(10.7.0.1000)-用户操作手册》

17.3.2. Windows 终端安全空间策略设置

17.3.2.1. 添加空间

同一条策略中，可以添加多个空间，空间内授权了根据实际需要进行配置。

1) 数据安全>安全空间>策略管理>编辑，在弹出的编辑策略配置页面，点击[添加空间]按钮，页面抽屉栏拉出【空间策略内容】添加/编辑页面，如下图所示：



2) 在【选择空间】的下拉列表中，找到需要添加的空间名称，再完成空间的其他项配置后，点击[确认]按钮，完成空间的添加任务。

3) 安全空间完成后，可根据应用对象不同，配置不同的策略项，管理员可配置的策略项包括：进程管理、防火墙规则、剪切板防护、截屏防护、文件导出、文件导入、打印控制、安全水印、无痕模式、SMB 文件共享服务、链接自适应、空间应用、生效场景等规则，详细配置在下面的章节有具体介绍。

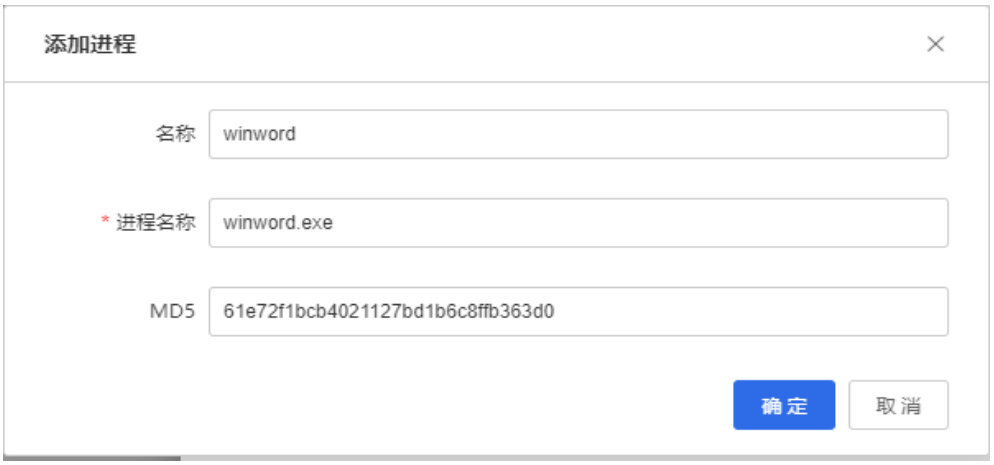
17.3.2.1.1. 进程管理

管理员进入添加/编辑安全空间配置页面，配置修改【进程管理】策略项，如下图所示：

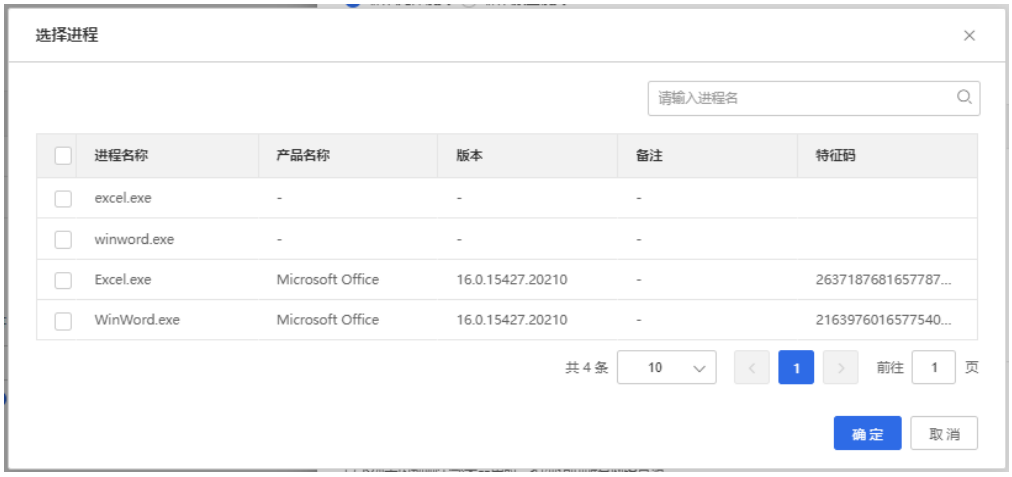
【默认允许模式】：该空间内默认允许运行所有应用程序，仅以下列表内的应用禁止运行；例如添加应用 notepad.exe 进程，下发到终端后，安全空间内禁止用 notepad.exe 进程打开文件。

【默认禁止模式】：该空间内默认禁止运行所有应用程序，仅以下列表内的应用允许运行；例如添加应用 winword.exe 进程，下发到终端后，安全空间内仅能用 winword.exe 进程打开 docx，doc 文件

1) 【添加进程】：在空间策略内容页面，【进程管理】栏中，点击[添加进程]按钮，弹窗添加进程窗口，在窗口内，输入进程名等信息，完成进程的添加。



2) 【选择进程】：在空间策略内容页面，【进程管理】栏中，点击[选择进程]按钮，弹窗选择进程窗口，在窗口内，选择对应的进程名，点击[确定]完成进程的添加。



3）选择进程列表中的进程来源于资产管理>知识库>进程知识库栏，进程知识库添加详见天擎操作手册，详见文档中心：01 产品市场资料中心-标准产品专区/0102 终端安全 BG-天擎事业部/新天擎 V10/15 操作维护/《奇安信天擎终端安全管理系统 V10.0R2-管理员手册 V1.0(220321).docx》。

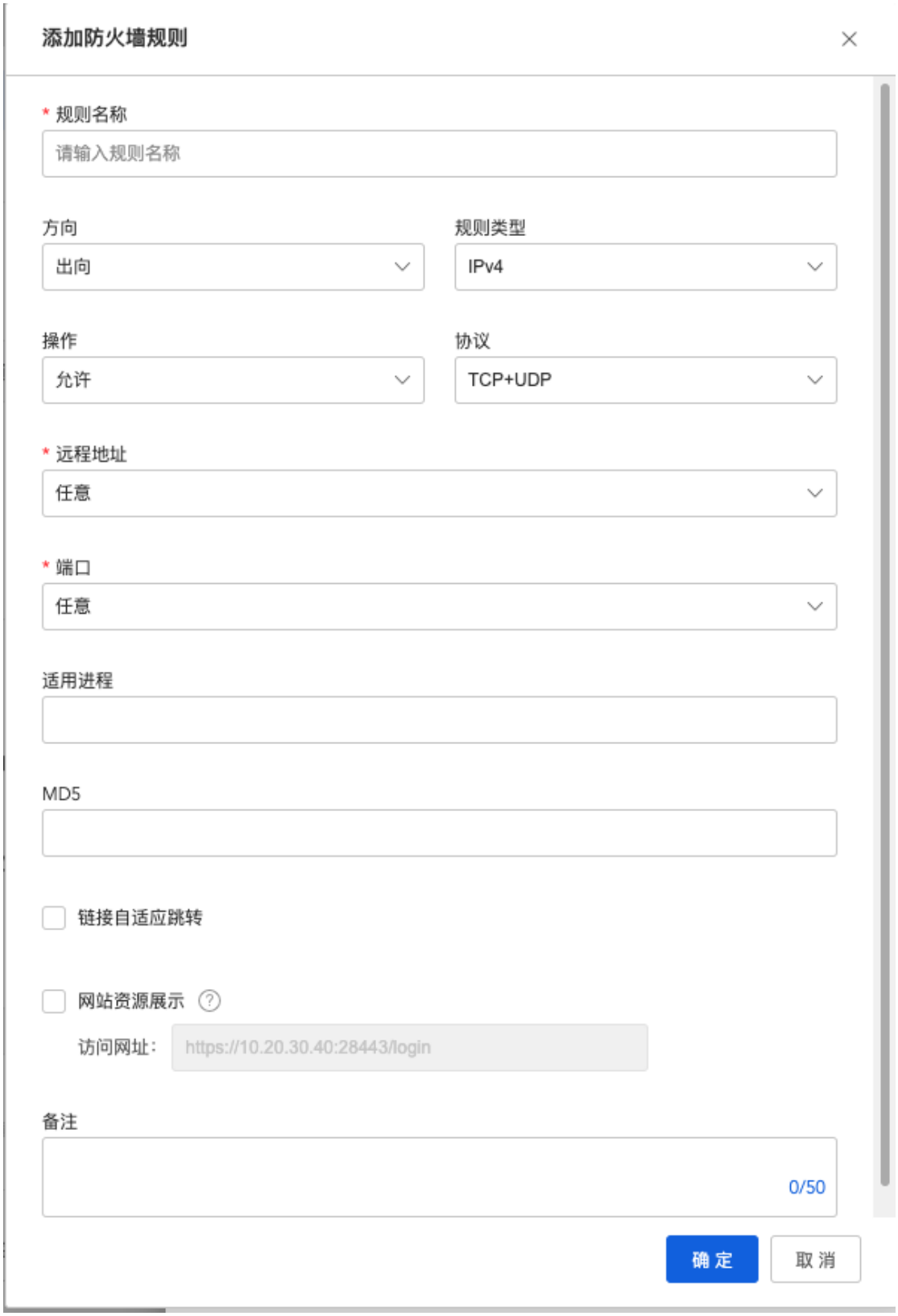
17.3.2.1.2. 防火墙规则

管理员进入添加/编辑安全空间配置页面，配置修改【防火墙规则】策略项。

【默认允许模式】：列表内规则全部未命中时，允许访问所有网络资源。

【默认拒绝模式】：列表内规则全部未命中时，拒绝访问所有网络资源。

支持与零信任联动，点击[选择]按钮，可以选择零信任控制台上配置的应用，来之零信任控制台的规则仅支持应用，不支持在安全空间中修改。


添加防火墙规则
* 规则名称
请输入规则名称
方向
出向
规则类型
IPv4
操作
允许
协议
TCP+UDP
* 远程地址
任意
* 端口
任意
适用进程
MD5
链接自适应跳转
网站资源展示
访问网址：
https://10.20.30.40:28443/login
备注
0/50
确定
取消

17.3.2.1.3. 剪切板防护规则说明

剪切板防护只针对文本内容，不针对文件或应用

1) 空间应用内容禁止通过剪切板拷贝到非空间应用：安全空间内文本内容禁止拷贝至个人空间中。

2) 高级别空间应用内容禁止通过剪切板拷贝到低级别空间应用：高级别空间文本内容禁止拷贝至低级别空间中，同级别、低级别至高级别拷贝不限制。

3) 空间应用内容禁止通过剪切板拷贝到其他空间应用：安全空间之间的文本内容不可相互拷贝。

4) 个人空间应用内容禁止通过剪切板拷贝到空间应用：个人空间内文本内容禁止拷贝至安全空间。

5) 自定义剪贴板防护提示信息：用户可以根据需要自定义：添加空间标签、进程名称、文件名作为提示信息，如下图所示：

17.3.2.1.4. 截屏防护

1) 勾选禁止截屏，在安全空间内启动防护进程，禁止用户在个人空间或其他空间执行截屏操作，在当前操作的空间内截屏不受限制。

2) 多个空间之间切换，或者打开了受保护进程，禁止执行截屏操作。

17.3.2.1.5. 文件导出

文件导出功能需要管理员在空间策略策略中根据部门实际情况做相关策略配置，选项如下图所示：

允许申请导出、允许申请导出且自动上传备份文件需依赖审批工作流（详见审批工作流），业务类型：空间文件导出。

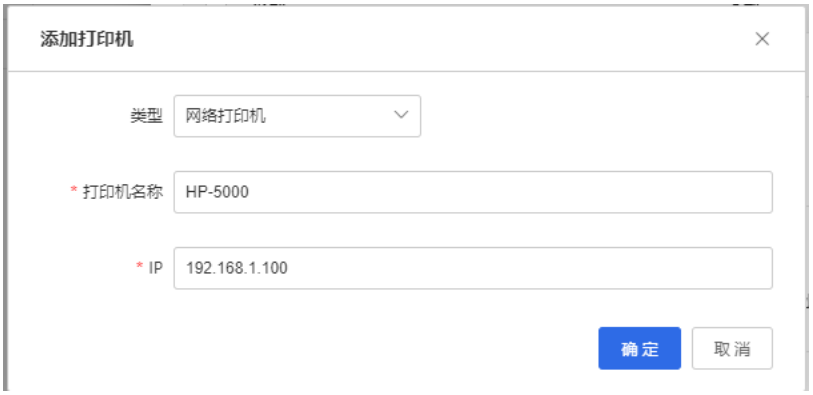
17.3.2.1.6. 文件导入

文件导入功能需要管理员在空间策略中根据部门实际情况做相关策略配置，选项如下图所示：

17.3.2.1.7. 文件打印

1) 安全空间内打印权限控制，可配置项：禁止、允许全部打印、允许指定打印；

2) 指定打印机支持添加本地打印机和网络打印机；



17.3.2.1.8. 安全水印

用于控制屏幕水印、打印水印的开关。

1) 【开启屏幕水印】：安全空间中启动指定进程，屏幕自动加载屏幕水印内容。屏幕水印内容需在安全空间管理“屏幕水印”页面中编辑。

2) 【开启打印水印】：安全空间中启动指定进程执行打印操作时，打印输出物显示打印水印。打印水印内容需在安全空间管理“打印水印”页面中编辑。

3) 数据安全>安全空间管理>新建>【编辑】空间，编辑屏幕水印、打印水印配置，

保存后转到【策略管理】页面中，开启安全水印，启动屏幕水印、打印水印项。

17.3.2.1.9. 无痕模式

“无痕模式”开启后，安全空间关闭（主动、被动）安全空间内的文件将自动删除所有系统及用户数据。该空间再次启动时，默认按首次初始化时配置重新加载空间。

【注意】启动该模式空间关闭后，数据将被删除且无法恢复，请用户在启动该场景时谨慎评估使用场景。

17.3.2.1.10. SMB 文件共享服务

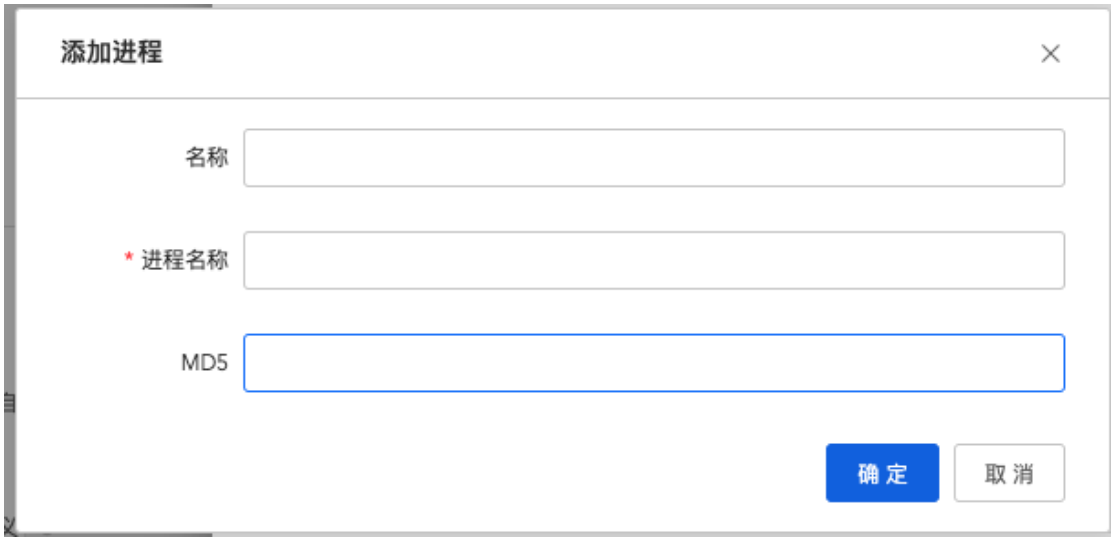
用于安全空间内通过 SMB 协议方式访问文件共享服务器，当设置成功后，安全空间可以访问文件共享服务器，个人空间无法访问文件共享服务器，支持 IP 和域名。

17.3.2.1.11. 链接自适应

- 安全空间内拒绝访问的 URL 自动跳转至对应空间的浏览器并访问。当选中该条目时，安全空间 A 访问已拒绝访问的 URL，会自动跳转到已加载且该安全空间允许访问的浏览器并打开该 URL
- 个人空间内拒绝访问的 URL 自动跳转至对应空间的浏览器并访问。当选中该条目时，个人空间访问已拒绝访问的 URL，会自动跳转到已加载且该安全空间允许访问的浏览器并打开该 URL

17.3.2.1.12. 空间应用

列表内为内置部分常用办公软件，该内置应用用户可做编辑、删除处理，如果常用列表中没有用户使用的软件，用户可以在终端自行安装或者添加。



17.3.2.1.13. 生效场景

为了方便客户端在不同的环境使用不同的策略，用户可以在安全空间中配置使用场景，终端登录后，从策略中获取场景信息，自动加载需要的安全空间。生效场景仅应用于有安全空间 License 时，“个人空间”和“安全空间”模块。

- 同一个空间可以配置不同的使用场景，终端根据使用场景自动适配安全空间策略。如果所有的场景都无法匹配则空间不加载。
- 当策略中未配置选择使用场景时，默认为全部场景，即不受场景限制。
- 空间列表中，同一个空间配置不同的场景，场景自上而下适配，适配到对应的不再往下遍历。
- 相同的场景顶端的优先适配，上面的优先级高于下面的优先级。管理员可以通过【上移】、【下移】调整场景优先级顺序。
- 控制台删除对应的场景，终端无法识别到使用场景，则空间自动回收并关闭安全空间。

- 场景添加：移动安全>安全空间>业务设置，在【生效场景】栏，点击[添加]按钮，弹出添加场景窗口，如下图所示：

- 接口定义：根据不同的选择调用不同的动态库，传入不同的参数，根据返回值来判断。详细细节可以咨询产品线或者研发人员。

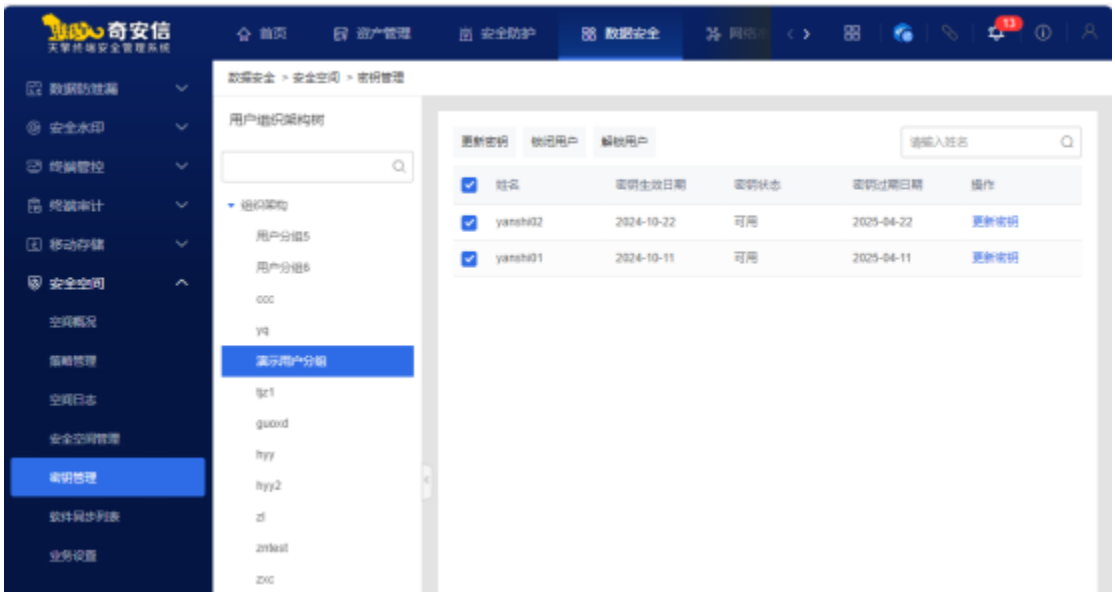
```
son，设备类型调用动态库 module.huawei，接口 GetMachType，参数传入空，如果是则返回 1，表
公设备“，不是则返回 0，表示"个人设备“

 调用动态库 module.huawei，参数传入空，如果是则返回 1，表示"内网"，不是则返回 0，表示"外


ev": {
  "type": "a",
  "dll": "module.huawei",
  "interface": "GetMachType"
  "param1": "",
  "param2": "",
   "true":"办公设备",
   "false":"个人设备“

et": {
  "type": "a",
```

- 配置使用示例如下所示：

17.3.2.1.14. 密钥管理

安全空间的数据保存在虚拟加密磁盘里。每个终端用户拥有不同的虚拟加密磁盘的密钥,并且密钥可定期更换、手动更新和锁闭。每个空间拥有独立的虚拟加密磁盘，每个磁盘使用不同的数据密钥加密，支持不同的加密算法(AES256,SM4)，确保数据存储的安全。

1. 终端从控制台获取密钥后，使用过程中如果发现密钥即将过期则进行联网更新。该更新支持安全盘加载开始时进行更新。否则就只能在关闭的时候更新。
2. 如果主密钥过期，且用户在使用过程中则用户可继续使用直到关闭该安全盘。密钥过期后，密钥变为过期状态，同时本地会将密钥从本地清空，所有的密钥都将不能使用。
3. 用户下一次启动机器后如果没有在线则不能获取密钥，也就不会加载安全空间。
4. 终端用户一旦登录后加载空时发现密钥信息已经过期，终端会请求控制台生成新的密钥信息。获取到新的密钥信息，会更新过期密钥，并将新密钥信息保存在本地。
5. 控制上管理员可以针对组织架构中所有用户批量更新密钥，也可以针对单个用户更新密钥。
6. 管理员可以设置密钥的有效期和密钥到期提示信息。



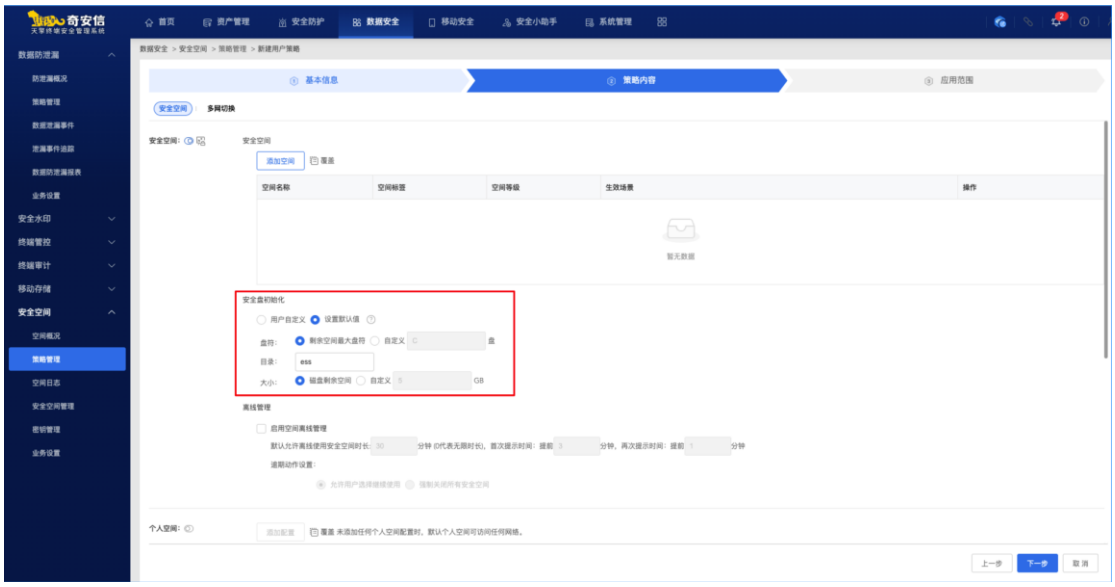
17.3.2.2. 离线管理

用户离线后，针对安全空间的使用，管理员可以根据不同的用户设置不同的管理方式，默认采用两种处理方式供用户选择：允许用户选择继续使用、强制关闭所有安全空间；

【允许用户选择继续使用】：用户离线后，提示用户关闭空间并根据用户选择做出处理；

【强制关闭所有安全空间】：用户离线后，客户端弹出提示，强制 30S 后关闭所有安全空间，该操作可能会丢失用户未保存的数据。

17.3.2.3. 安全盘初始



【用户自定义】：安全空间用户自定义初始化，用户可以根据提示设置空间存放的盘符、目录、大小。

【设置默认值】：安全空间系统后台静默初始化。

17.3.2.4. 个人空间配置

可根据业务需要，配置个人空间内允许访问的网络资源。默认情况下个人空间允许访问所有的网络资源。

17.3.3. 信创终端安全空间策略设置

17.3.3.1. 添加空间

同一条策略中，可以添加多个空间，空间内授权了根据实际需要进行配置。

1)数据安全>安全空间>策略管理>用户策略>编辑，在弹出的编辑策略配置页面，点击[添加空间]按钮，页面抽屉栏拉出【空间策略内容】添加/编辑页面，如下图所示：

2)在【选择空间】的下拉列表中，找到需要添加的空间名称，再完成空间的其他项配置后，点击[确认]按钮，完成空间的添加任务。

3)安全空间完成后，可根据应用对象不同，配置不同的策略项，管理员可配置的策略项包括：防火墙规则、文件导出、文件导入、打印控制、截屏防护、安全水印、无痕模式、空间应用等：

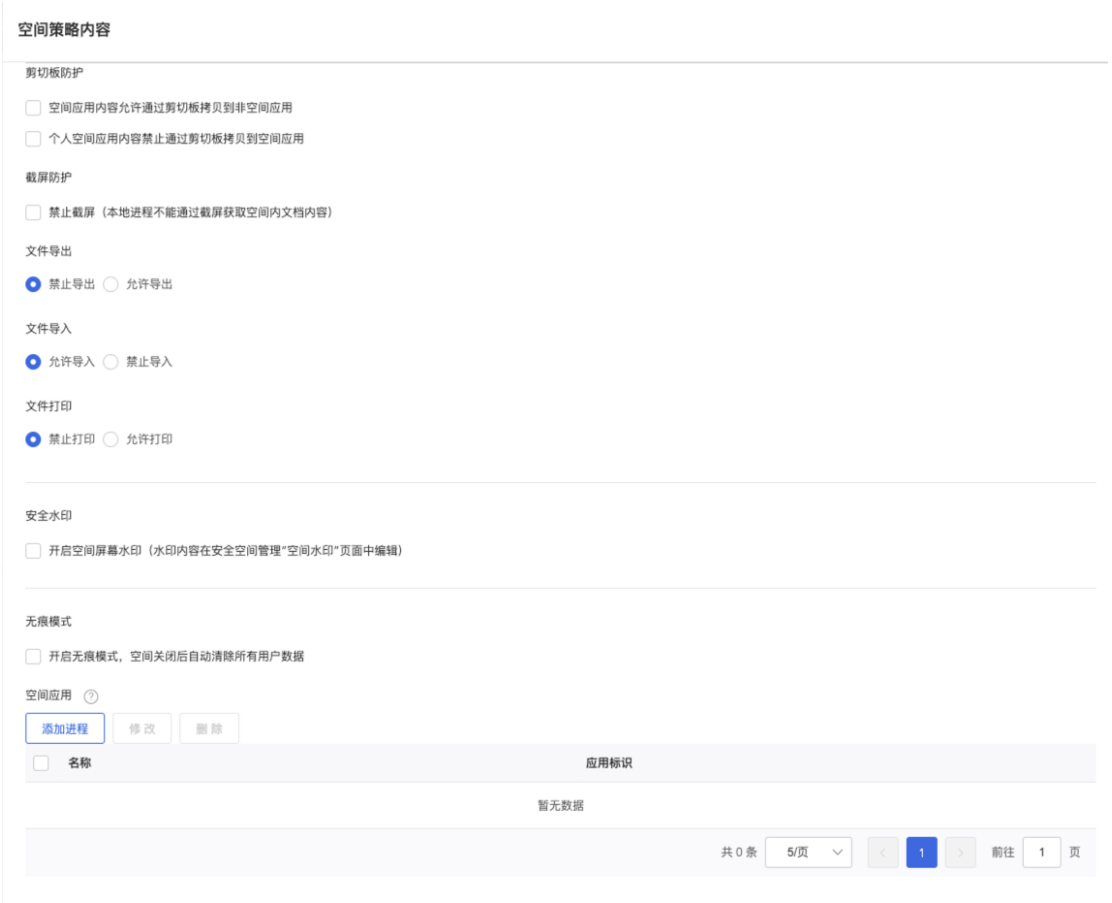
4)防火墙规则：管理员进入添加/编辑安全空间配置页面，配置修改【防火墙规则】策略项。

【默认允许模式】：列表内规则全部未命中时，允许访问所有网络资源。

【默认拒绝模式】：列表内规则全部未命中时，拒绝访问所有网络资源。

支持与零信任联动，点击[选择]按钮，可以选择零信任控制台上配置的应用，来之零信任控制台的规则仅支持应用，不支持在安全空间中修改。

- 文件导出：默认情况下空间内文件不允许通过复制粘贴/拖拽/另存为等方式导出至个人空间，可通过管理员设置允许后，通过共享目录方式外发至个人空间。
- 文件导入：默认情况下个人空间文件可自由进入至安全空间内，可通过管理员设置禁止后，文件无法复制/粘贴/另存等至安全空间内。
- 安全水印：用于空间水印的开关。勾选，且安全空间管理中配置空间水印策略方可显示水印。
- 截屏防护：勾选禁止截屏，禁止用户执行截屏操作。
- 打印控制：安全空间内打印权限控制，可配置项：禁止、允许。
- 无痕模式：当启用该功能，空间关闭后（主动、被动）自动删除所有系统及用户数据。该空间再次启动时，默认按首次初始化时配置加载。
- 空间应用：列表内为内置部分常用办公软件，该内置应用用户可做编辑、删除处理，如果常用列表中没有用户使用的软件，用户可以在终端自行安装或者添加。



17.3.3.2. 个人空间配置

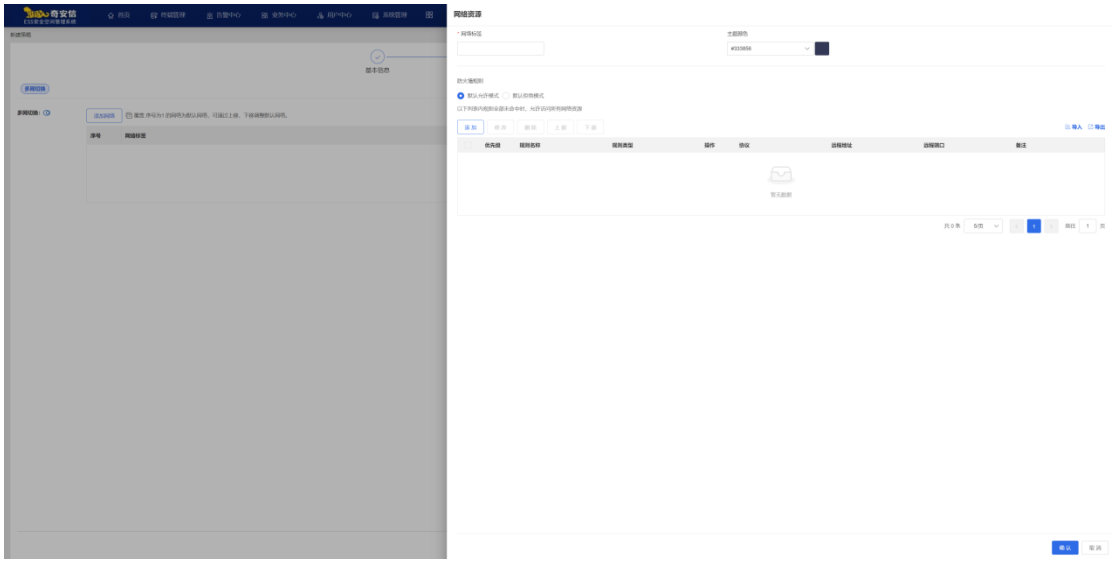
可根据业务需要，配置个人空间内允许访问的网络资源。默认情况下个人空间允许访问所有的网络资源。

17.3.4. Windows 终端多网切换策略设置

即终端上多网切换功能，入口：数据安全>安全空间>安全空间/多网切换

多网切换支持终端策略和用户策略。用户策略优先级高于终端策略。

网络配置时支持 IPV4、IPV6、域名、IP 段，同时支持 TCP、UDP、ICMP 等协议。



18. 移动安全

18.1. 移动安全空间

安全空间是查看和设置终端管控策略的管理模块，在该功能下可以通过配置管控策略对终端进行空间与合规管理。

18.1.1. 终端概况

18.1.1.1. 分组查询

管理员可以通过检索框精确查询分组信息，展示分组下的终端设备。

18.1.1.2. 筛选

管理员可以通过高级筛选功能查看符合条件的终端设备。高级筛选通过添加条件、添加子组的形式灵活组合进行查询。

操作步骤：

查询：移动安全>终端概况,页面列表右上角点击【筛选】按钮，输入筛选条件点击【应用】按钮进行查询。

清除：点击【清除】按钮清除全部筛选条件。

保存：点击【保存】按钮保存已添加的筛选条件，在筛选框右上角展示已保存的筛选条件。

收起：点击【收起】按钮隐藏高级筛选

组合形式：或者、并且：

或者：条件满足一个即可。例如只要满足 A 条件与 B 条件中任何一个。

并且：条件必须全部满足。例如：必须同时满足 A 条件与 B 条件。

添加条件：选择列表中的条件输入对应的值进行查询。

例如：条件：操作系统 不包含 Android10。

添加子组：添加组合查询内容。

判断符定义：

判断符合	描述
等于	输入值与查询结果一致。例如：精确查询
不等于	输入值与查询结果不一致。例如：排除查询
包含	查询结果中包含输入值。例如：模糊查询
不包含	查询结果不包含输入值。例如：排除查询
大于	查询结果大于输入值并且不含输入值。例如：范围查询
大于等于	查询结果大于输入值并且含输入值
小于	查询结果小于输入值并且不含输入值
小于等于	查询结果小于输入值并且含输入值

18.1.1.3. 自定义列

管理员可以对终端查询结果列表字段进行自定义选择，通过设置调整展示列表字段信息。

操作步骤：移动安全>终端概况,页面右上角选择【自定义列】选项勾选或取消展示的字段列点击确认。

18.1.1.4. 导出

管理员对已查询到的结果信息以表格的形式导出数据。

操作步骤移动安全>终端概况,页面右上角点击【导出】按钮。

导出的数据统一在消息中心进行下载。

18.1.1.5. 查看终端详情

管理员可以通过点击单个终端名称查看终端详情信息,也可以通过批量选择查看终端详情信息，终端信息包括终端基本信息、终端策略信息、终端应用安装详情，在查看详情中可以对终端设备的资产信息进行编辑。

操作步骤：

查看单条：移动安全>终端概况,页面列表点击计算机名称列查询到的设备名称进行查看。

查看多条：移动安全>终端概况页面列表勾选需要查看的设备，点击【查看】。

18.1.1.6. 终端操作

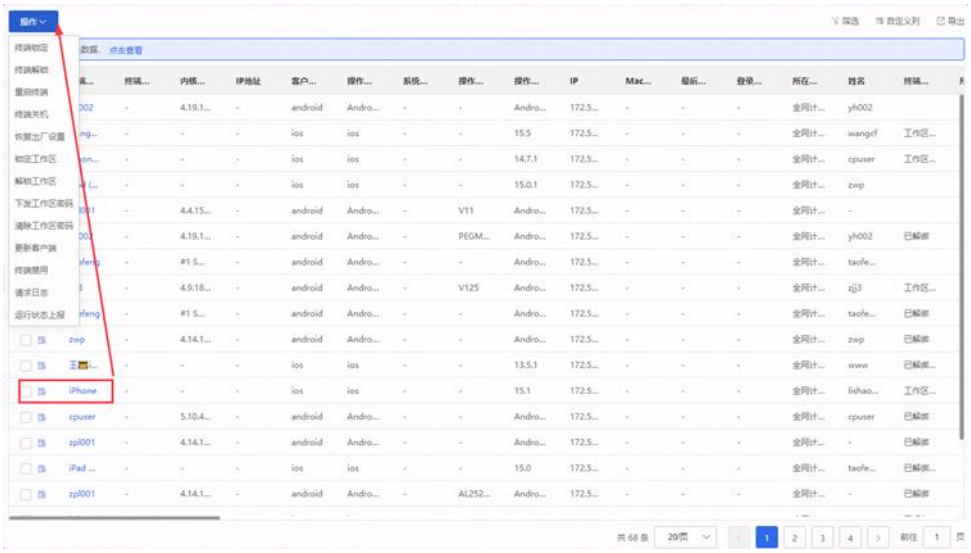
终端操作功能是管理员对终端设备下达远程操作指令。

操作步骤：【移动安全】-【终端概况】-选择指定设备点击【操作】按钮或者点击列表中设备名的操作图标【 】进行操作。

操作项描述：

锁定终端	远程锁定终端设备后将无法登录
解锁终端	解除终端远程锁定
重启终端	远程重启终端设备
终端关机	远程关闭终端设备
恢复出厂设置	远程使终端设备恢复出厂设置，清除数据
锁定工作区	远程锁定终端设备的安全工作区
解锁工作区	远程解锁已锁定的安全工作区
下发工作区密码	远程设置工作区访问密码

清除工作区密码	远程消除工作区访问密码
更新客户端	远程更新客户端版本
禁用终端	远程禁用终端设备，禁用的终端设备将无法操作
请求日志	远程发送请求操作日志指令
运行状态上报	设置终端设备运行报告上报服务端



18.1.2. 安全空间策略

安全空间策略是对终端设备进行策略配置的功能模块，管理员可以在该页面根据业务需要设置相关的管控策略。

18.1.2.1. 新建终端策略

新建策略包含 3 部分策略基本信息、策略内容、策略应用范围。

策略信息字段描述：

普通策略	标准执行策略不会强制执行
强制策略	强制执行策略配置强制策略后下级策略无法覆盖强制策略

策略内容包括：通用策略、空间策略、设备合规三部分。

通用策略包括终端锁定设置、隐私策略设置、WiFi 设置。

1. 通用设置功能描述：

自动锁屏	超过设置时间未操作时自动锁屏设备
锁屏密码更新	超过设置时间天数后需要更换密码
最大解锁错误次数	解锁密码错误机制超过设定次数后锁定终端
禁止与历史密码重复	禁止设置与历史重复密码
图形	开启图形解锁验证
最少连接点数	图形解锁连接点个数
数字密码	开启后密码为纯数字
混合密码	开启后密码为数字、字母、特殊符合、大小写混合
锁屏密码长度	设置密码长度限制
至少包含大写字母个数	混合密码中大写字母个数限制
至少包含小写字母个数	混合密码中小写字母个数限制
至少包含数字个数	混合密码中包含数字个数限制
至少包含特殊符合个数	混合密码中特殊符号个数限制
上传地理位置信息	上传当前终端设备地理位置信息至服务端
WIFI 策略	添加 WIFI 黑白名单

2. 空间配置功能描述

工作区锁屏设置参考通用设置锁屏设置	
隐藏相机及图库	隐藏工作区相机及图库功能
隐藏联系、拨号、短信	隐藏工作区内联系、拨号、短信功能
隐藏文件管理器	隐藏工作区内文件管理器功能
隐藏退出登录按钮	隐藏工作区退出登录功能
隐藏设备解除绑定按钮	隐藏工作区解绑设备功能
隐藏浏览器	隐藏工作区浏览器功能
启用剪贴板隔离	开启禁止复制剪贴
启用认证小助手	开启认证助手功能
禁止客户端文件管理器访问个人区	开启工作区与个人区文件隔离 工作区文件管理无法访问个人区
禁止工作区截屏/录屏	开启后工作区内无法截屏与录屏功能

禁止分享	开启后工作区内禁止分享功能
第三方应用通知栏消息内容隐藏	开启后第三方应用通知栏内容不展示
Banner 配置	Banner 轮播配置
水印配置	设置水印方式、水印内容、水印内容参数
非推送应用配置	配置只对单应用模式生效
VPN 配置	VPN 服务器设置、参数配置
WiFi 配置	配置 WiFi 网络设置

设备合规配置功能描述

设备合规策略触发后会对违规策略进行不同的执行项

上报违规记录	终端违规记录上传至服务端
禁止进入工作区	禁止用户登录工作区
清除单位数据	清除设备中的数据
注销终端	注销终端接入信息，注销后的设备无法进入工作区

应用范围配置

设置策略下发范围，管理员可以根据业务情况选择下发类型

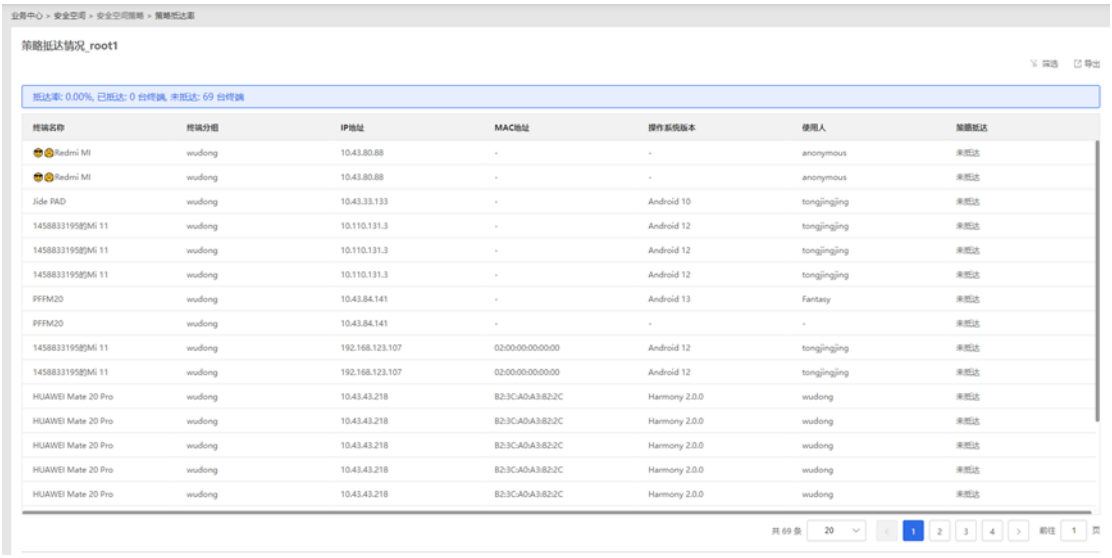
操作步骤：【移动安全】-【安全空间策略】点击【新建】按钮。

18.1.2.2. 查看策略详情

管理员可以在策略列表中点击策略名称查看策略配置详情。

18.1.2.3. 策略执行情况查看

管理用可点击抵达情况查看终端执行策略情况



18.1.2.4. 策略维护

管理员可以在操作栏中对已创建的策略进行维护操作。

1.编辑

修改已生效的策略配置项。

2.复制

复制选中的策略配置参数。

3. 停止

停止策略执行。

4.删除

删除已配置的策略。

18.2. 移动终端管控

定制终端管理时对指定设备或厂商定制设备进行管控。

18.2.1. 定制终端策略

普通策略	标准执行策略不会强制执行
强制策略	强制执行策略配置强制策略后下级策略无法覆盖强制策略

18.2.1.1. 新建终端策略

安装定制终端目前支持小米、OPPO、华为、DeciceOwner 强管控、系统签名管控五种设备类型。

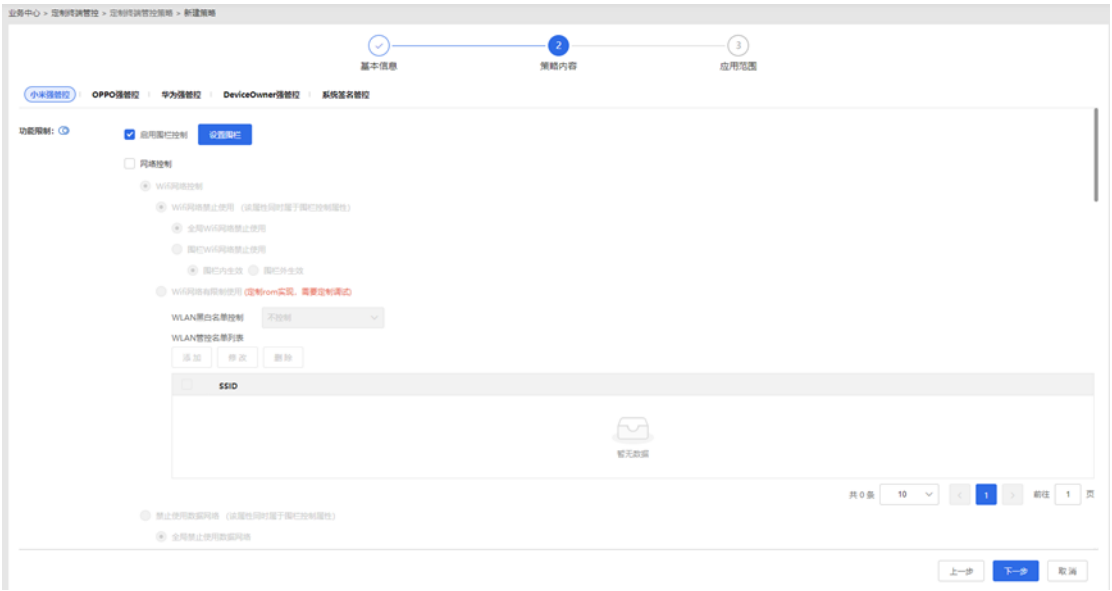
管控能力包括功能限制、数据防泄露、应用管控、APN 配置。

操作步骤：

点击【定制终端管控策略】-【新建】-输入策略名称，选择【策略类型】-选择-【通用策略】-选择【客户端】点击下一步。

选择终端类型，根据需要选择管控策略配置完成后点击下一步。

点击【应用终端分组】选择需要执行策略的分组，点击【应用】配置完成。

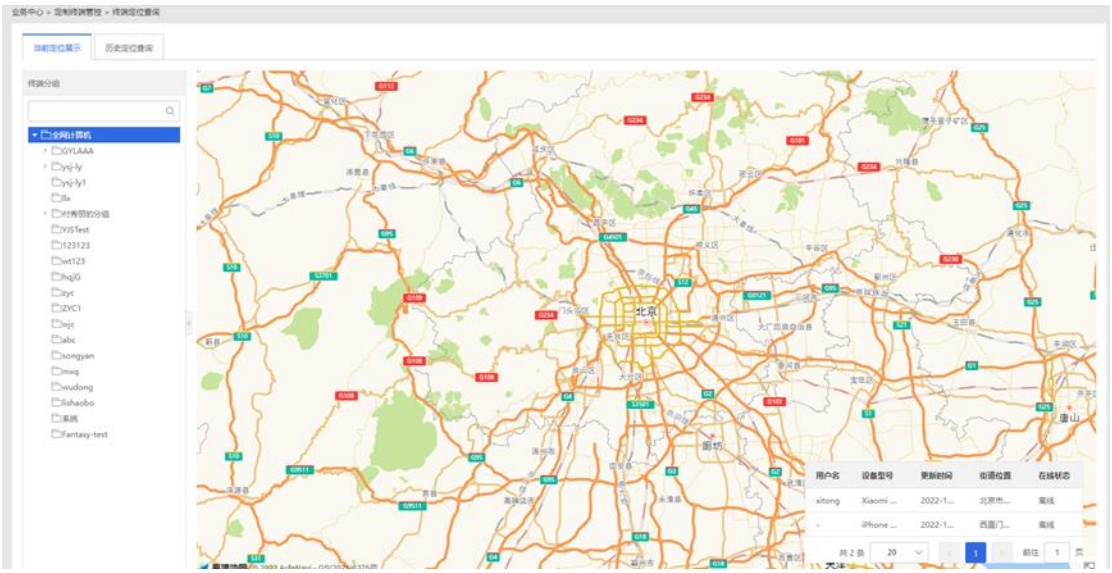


18.2.1.2. 查看终端策略

管理员可通过策略列表查看已配置的策略信息，通过抵达情况可查看策略执行情况。

18.2.1.3. 终端定位查询

管理员可通过该模块查看终端设备定位信息、下班在线状态等信息，终端设备支持分组查询，终端定位查询支持当前定位展示、历史定位查询两种类型。



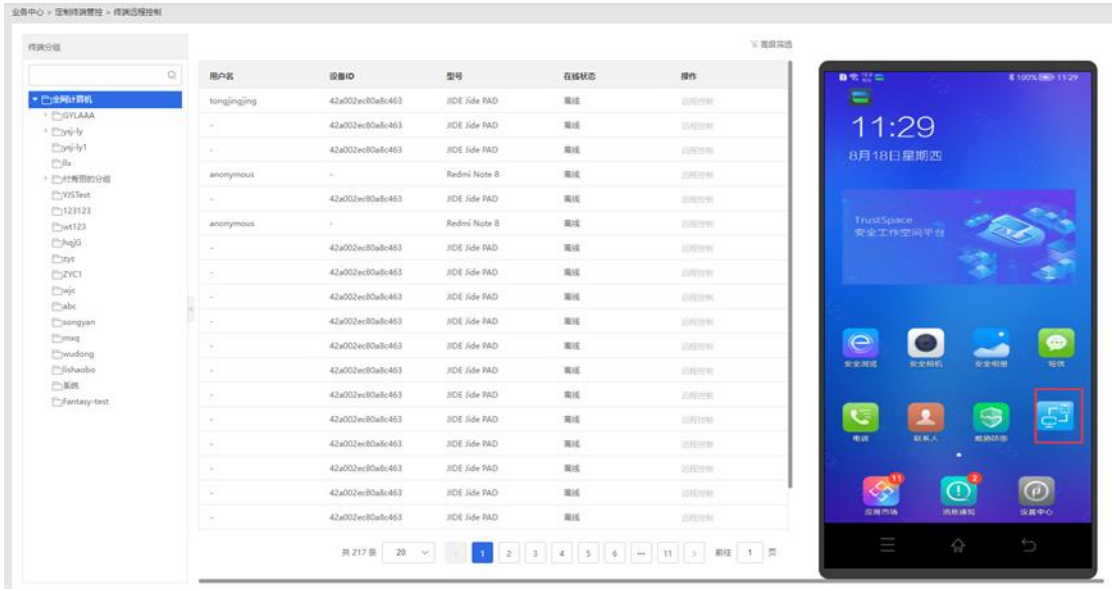
历史定位查询

通过列表形式展示终端设备历史定位信息，数据包括上报时间、定位时间、坐标、街道名称。

18.2.1.4. 终端远程控制

管理员可通过终端远程控制对指定终端设备发起远程指令，同时以远程桌面形式对重点进行远程调试。

注：远程控制功能需要厂商设备证书支持。



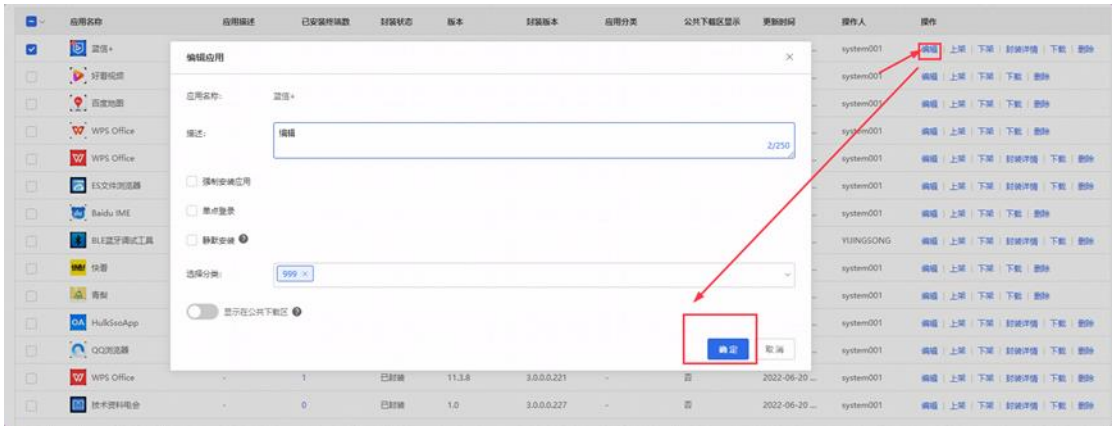
18.3. 移动应用商店

应用商店是对应用商城中的应用进行管理和维护的功能模块，同时管理员可以查看已配置的应用使用情况，该模块由 Android 应用管理、IOS 应用管理、H5 应用管理、应用统计四部分组成

18.3.1.1. 编辑应用

对已添加的应用修改设置信息。

操作步骤：【移动安全】-【应用商店】-【Android 应用管理】选择编辑的应用在操作列点击【编辑】按钮进行修改信息，修改完成后点击【确认】按钮完成应用编辑。



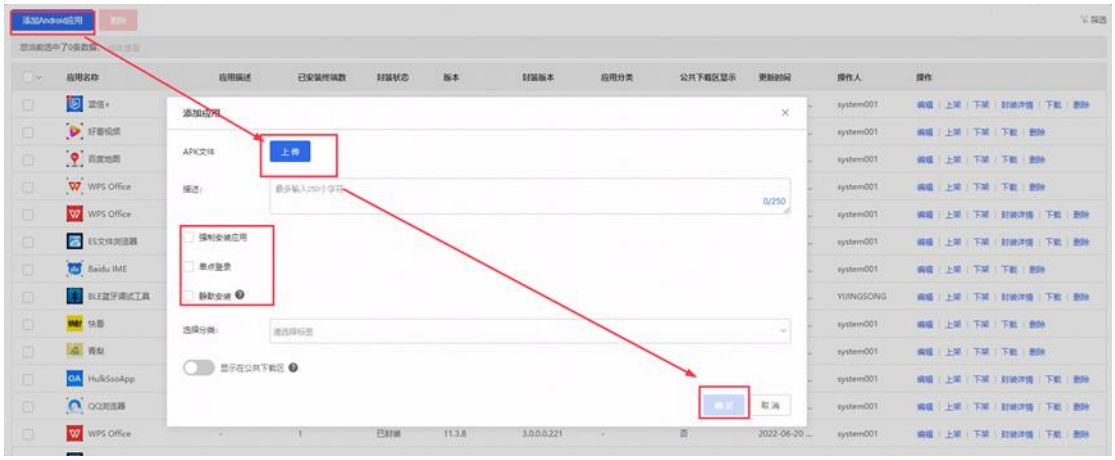
18.3.2. Android 应用管理

管理员可以在该页面添加 Android 应用，对已上线的应用进行维护。

18.3.2.1. 添加应用

添加应用到服务端，管理员可以根据业务需要添加应用

操作步骤：【移动安全】-【应用商店】-【Android 应用管理】点击【添加 Android 应用】按钮上传 APK 文件，设置配置项点击【确定】完成应用添加。



18.3.2.2. 删除应用

删除已添加的应用

操作步骤：

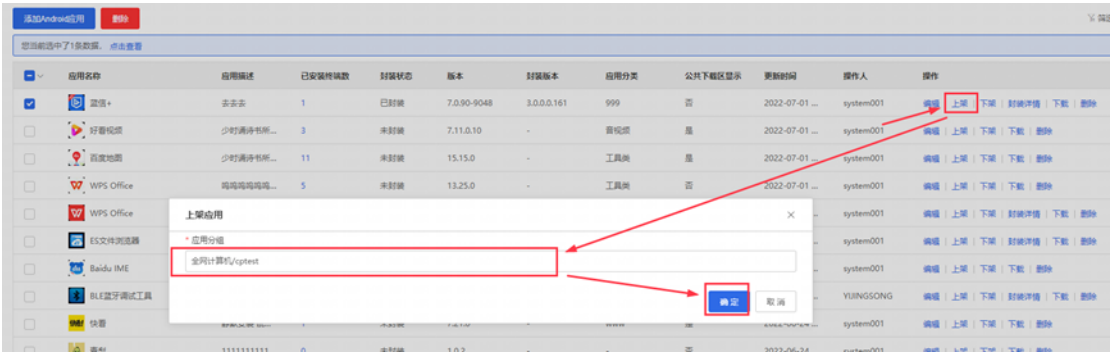
1.【移动安全】-【应用商店】-【Android 应用管理】选择要删除的应用点击【删除】按钮点击提示框中的【确定】完成删除。

2. 【移动安全】-【应用商店】-【Android 应用管理】选择要删除的应用在操作列点击【删除】按钮点击提示框中的【确定】完成删除。

18.3.2.3. 应用上架

对已添加至服务端的应用上架到应用商店中，上架到应用商店的应用终端可以进行下载安装。

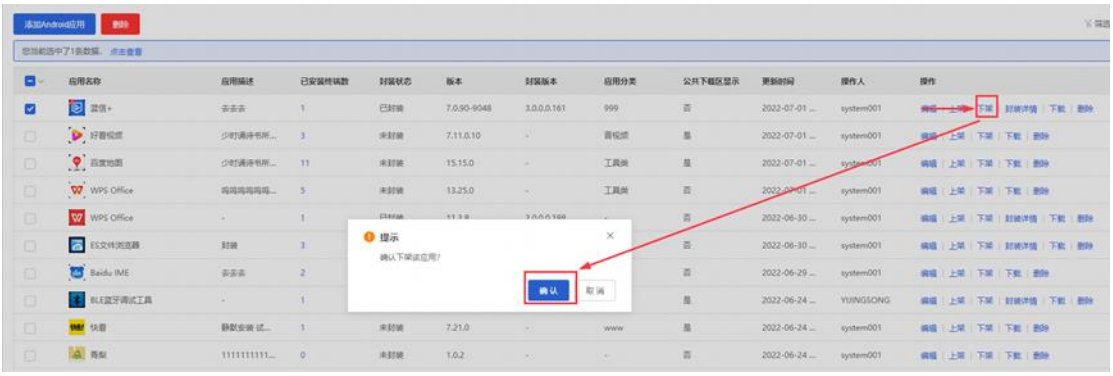
操作步骤：【移动安全】-【应用商店】-【Android 应用管理】选择要上架的应用在操作列点击【上架】按钮，选择需要上架的分组点击【确定】完成上架。



18.3.2.4. 应用下架

对已上架的应用进行下架操作，下架后的应用将不在应用商店提供下载。如图 24

操作步骤：【移动安全】-【应用商店】-【Android 应用管理】选择要上架的应用在操作列点击【下架】按钮在提示框点击【确定】完成下架。



18.3.2.5. 封装详情

查看已封装的应用封装信息与应用配置策略

操作步骤：【移动安全】-【应用商店】-【Android 应用管理】选择已封装的应用在操作列点击【封装详情】按钮查看。

18.3.2.6. 下载

对已上传至服务端的应用下载至本地计算机中，下载操作只允许在 PC 机操作。

18.3.3. IOS 应用管理

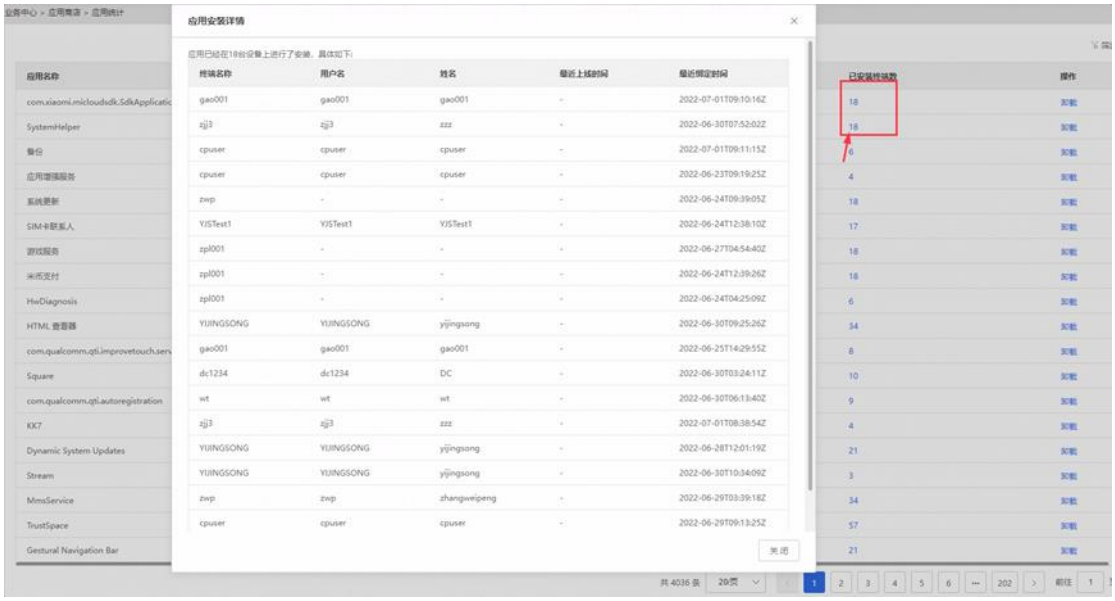
应用添加方式参考 18.3.1 章节。

18.3.4. H5 应用管理

H5 应用添加时需要上传 H5 连接与应用图标，其他设置参考应用添加方式参考 18.3.1 章节。

18.3.5. 应用统计

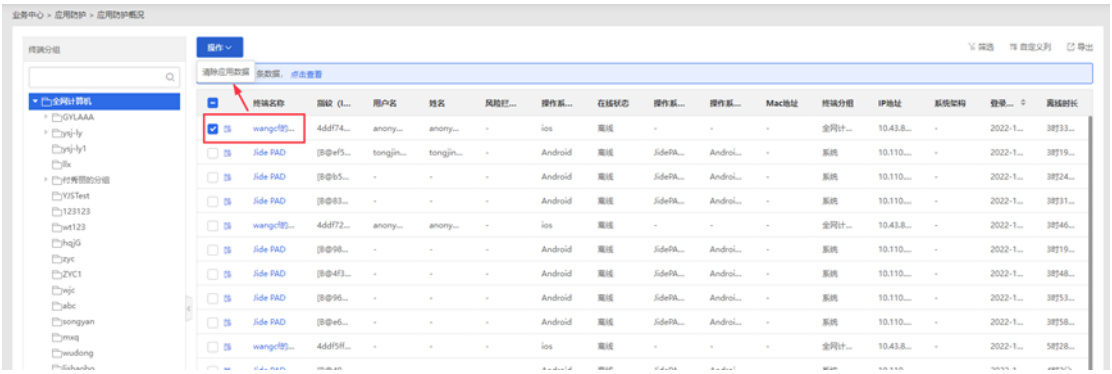
应用统计是查看终端设备对已上架的应用安装详情，管理员可以在该页面查看应用在终端安装的次数，已经安装应用的终端详情列表，同时管理员可以在该页面对已安装应用的终端远程进行卸载操作。



18.4. 移动应用防护

18.4.1. 应用防护概况

管理员可以在页面查看终端安装应用情况，对指定终端可操作清除应用数据操作。



18.4.2. 应用防护策略

应用策略管理模块，管理员可以在该页面下创建应用防护策略，对已创建的策略进行查看与维护。

18.4.2.1 新建策略

点击【应用策略防护】-【新建】按钮依次填写策略信息、策略内容、应用范围点击【确认】完成策略创建。

功能限制-全局封装应用限制

全局封装应用限制是对全部应用设置策略。

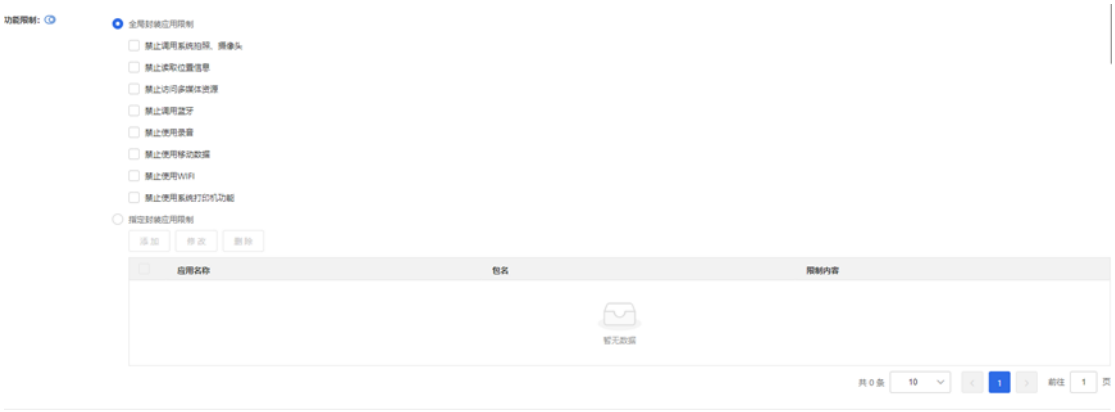
策略字段解释：

功能名称	描述
禁止调用系统拍照、摄像头	应用无法使用摄像头、拍照、录像功能。
禁止读取位置信息	应用无法获取终端设备当前位置信息。

禁止访问多媒体资源	应用无法读取多媒体资源，包括：照片、视频等文件。
禁止调用【蓝牙】	应用无法获取终端设备【蓝牙】开启权限。
禁止使用录音	应用无法获取终端设备录音功能。
禁止使用移动数据	应用在移动数据网络下无法使用。
禁止使用 WIFI	应用在 WIFI 网络下无法使用。
禁止使用系统打印功能	应用无法获取终端设备系统打印功能。

功能限制-指定封装应用限制

指定封装应用限制是对选定的应用设置防护策略，未指定的应用不受策略控制。策略字段解释见：1）全局封装应用限制是对全部应用设置策略。



数据防泄漏

已封装应用行为控制是对封装后的应用部分操作行为进行控制 如图 34

策略字段解释：

功能	描述	操作
应用使用剪切板	控制应用使用剪切板功能	允许、禁止
截屏/录屏/投屏	控制应用使用中是否允许截屏、录屏、投屏功能。	允许、禁止
通知栏 消息内容	控制应用是否在通知栏内显示消息	隐藏、显示

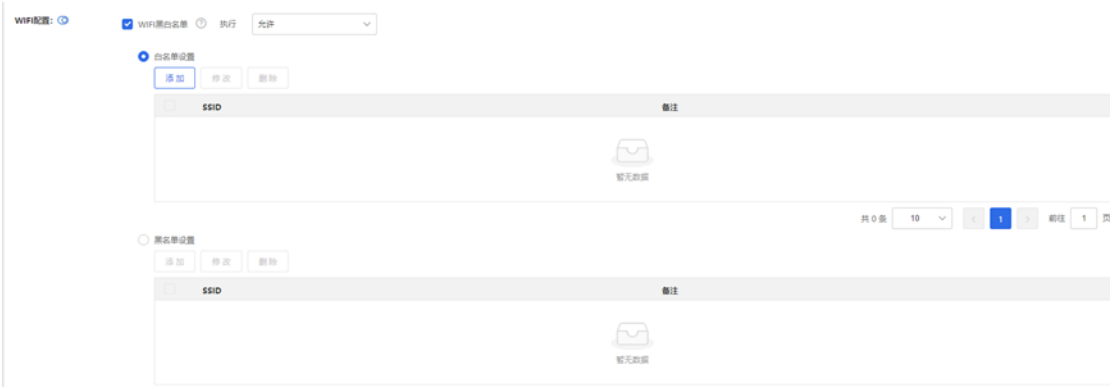
分享控制

1.已封装的应用调用未封装的应用时的控制策略。管理员可以设置允许/禁止来控制调用行为，设置开启允许后需要添加应用白名单。

2.已封装应用调用已封装应用时的控制策略，管理员设设置开启允许后需要添加应用白名单。

WIFI 配置

设置 WIFI 黑白名单，管理开启 WIFI 配置后可以选择禁止或允许开启黑白名单设置。



封装应用水印配置

应用增加水印功能，管理员开启后可以对水印设置方式、样式、内容进行设定。

VPN 配置

VPN 配置功能，管理员开启后可以设置 VPN 配置信息

应用加固

应用加固是对应用设置安全防护，管理员开启后根据需要对应用配置防护类型。

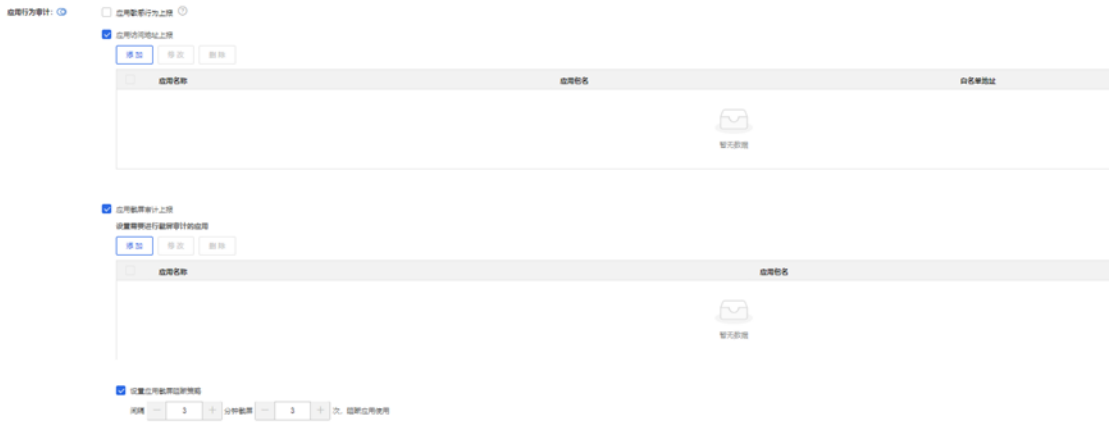
运行环境

运行环境是对应用运行环境的是否安全的防护检测功能。管理员开启后可以设置运行环境检测机制。

应用行为审计

实时监控应用使用行为，对触发敏感或违规的行为进行数据上报，上报的数据管路有可以通过应用防护审计报表中查看。

功能	描述
应用敏感行为上报	应用使用时触发敏感行为操作会进行数据上报，敏感行为包括:剪切板、分享、通知栏等。
应用访问地址上报	配置应用禁止访问 IP 地址。
应用截屏审计上报	应用发生截屏行为时进行数据上报。



18.4.2.2 维护策略

管理员可以在该页面下对已创建的策略进行维护，维护包括：查看策略抵达情况、编辑策略、复制策略、开启策略、删除策略。

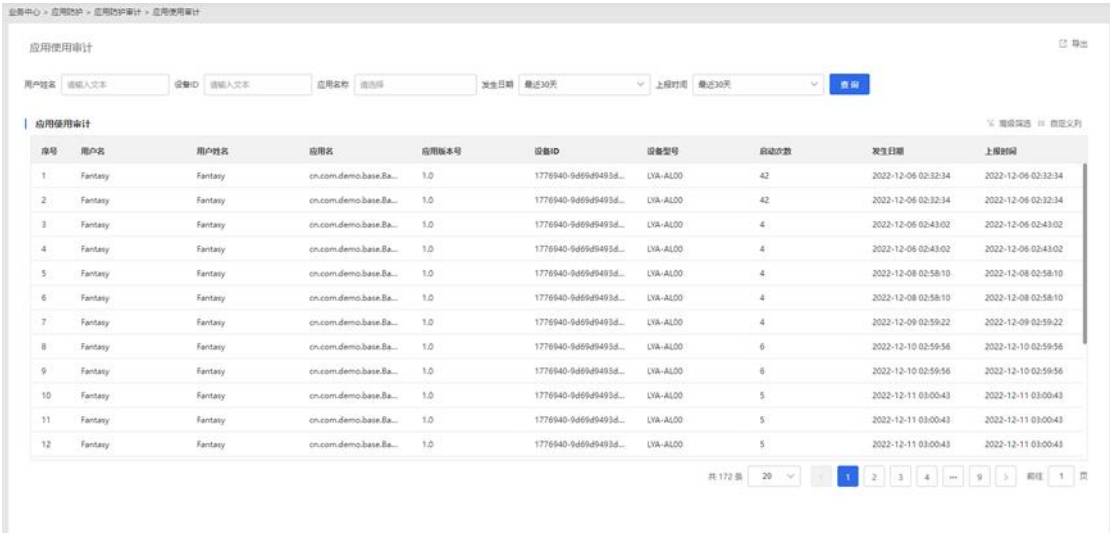
18.4.3. 应用防护审计

应用防护审计是对应用的使用情况进行记录，同时应用执行策略情况进行记录，数据通过列表形式进行展示，审计维度包括：应用敏感行为审计、应用访问地址审计、应用截屏审计、应用使用审计、应用加固审计、运行环境审计。

管理员可以在该模块下查看对应的审计数据，支持数据导出。

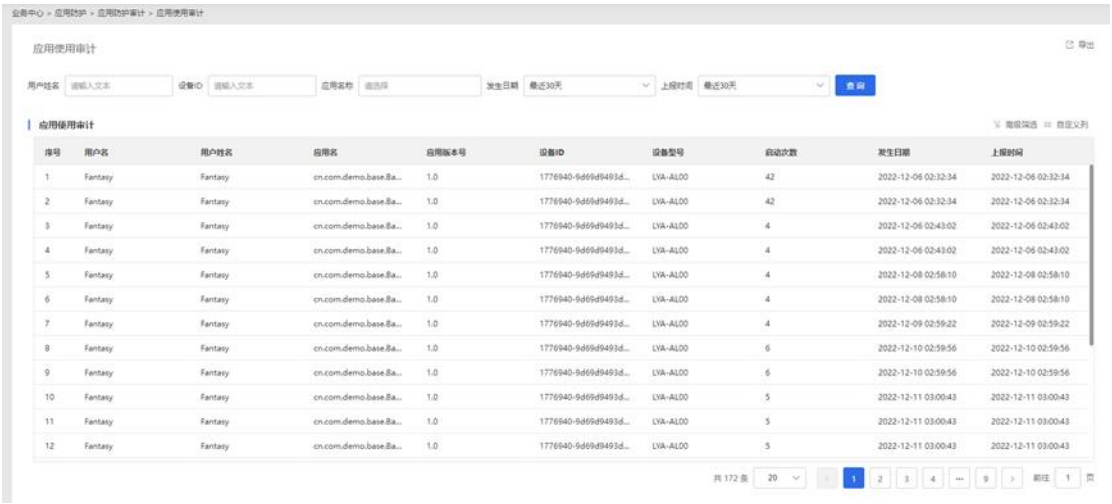
18.4.3.1. 应用使用审计

应用使用日志



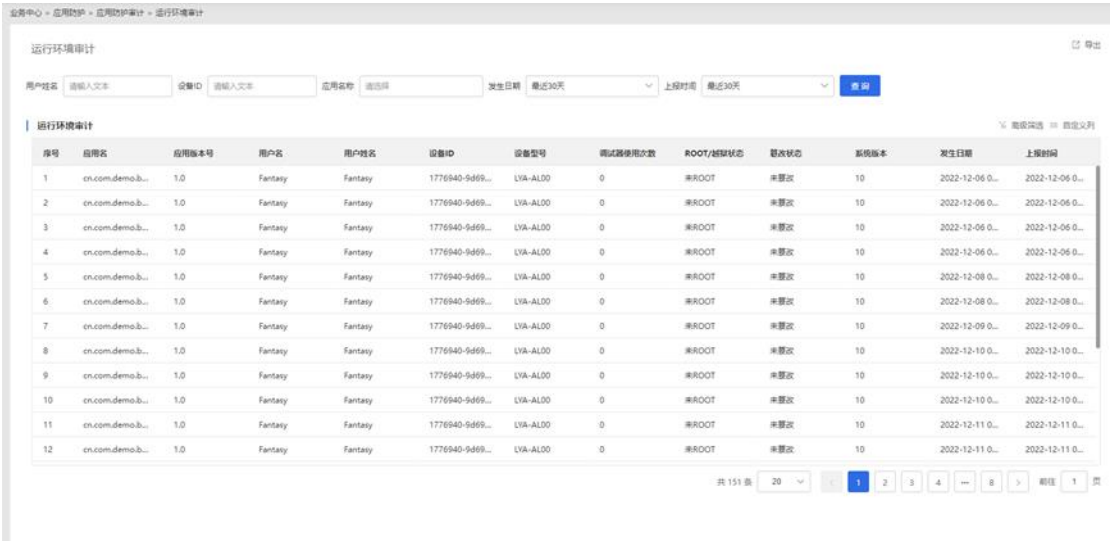
18.4.3.2. 应用加固审计

应用加固日志



18.4.3.3. 运行环境审计

应用运行环境日志

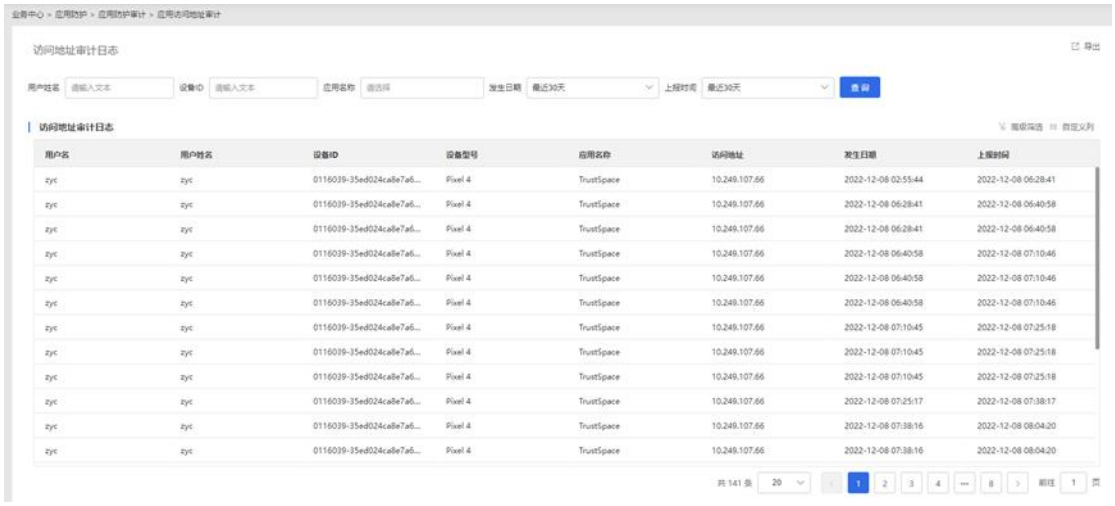


18.4.3.4. 敏感行为审计

应用触发敏感操作日志

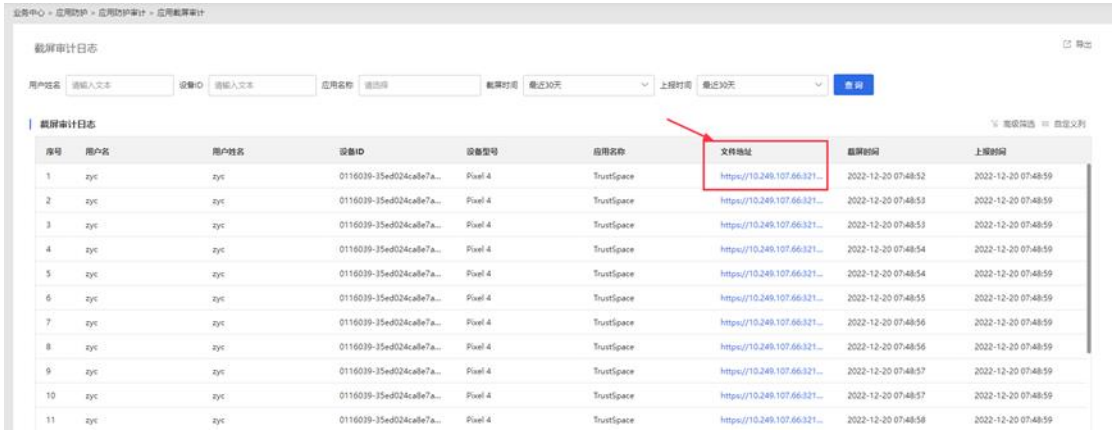
18.4.3.5. 应用访问地址审计

开启应用截屏策略后用户在使用应用时发生截屏，数据将上报管理平台，管理员可以在应用访问地址审计日志中查看，点击文件地址可查看截屏内容。



18.4.3.6. 应用截屏审计

开启应用截屏策略后用户在使用应用时发生截屏，数据将上报管理平台，管理员可以在应用访问地址审计日志中查看，点击文件地址可查看截屏内容。



18.5. 移动威胁感知

威胁感知是解决移动终端环境可信的重要组件工具，模块由风险感知、风险感知策略、风险感知配置、风险评估、风险感知日志五部分组成。

18.5.1. 风险感知

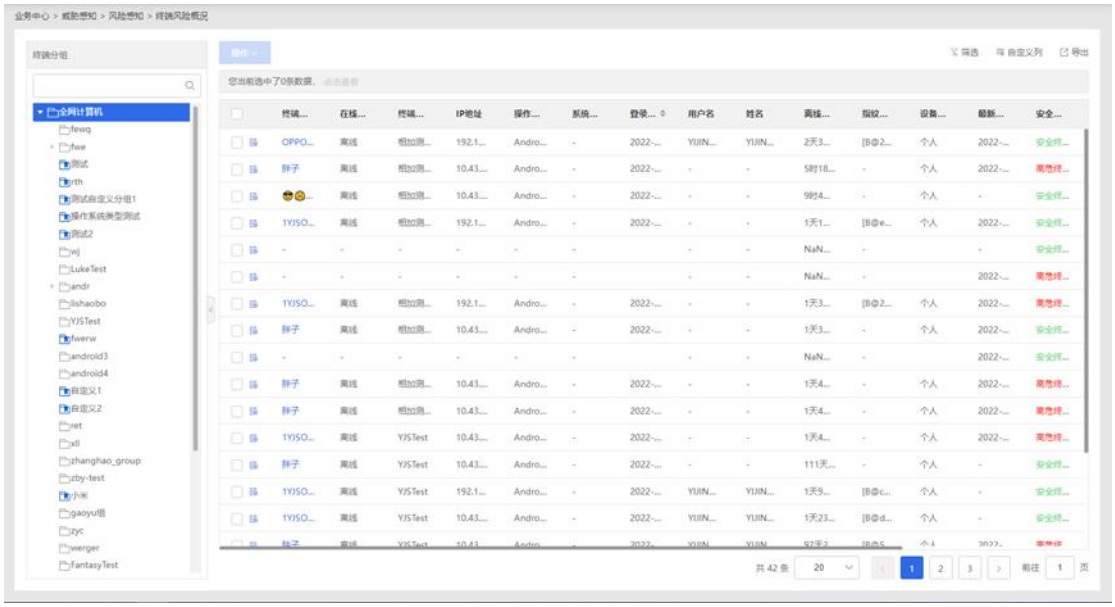
风险感知是对已接入终端设备的整体运行环境进行监测，通过对终端系统、网络、设备、应用、行为、位置等多维度进行监测，并对终端设备安全状

态进行评估，同时对全部终端存在的风险隐患提供界面化展示。功能模块包含：终端风险概况、应用风险概况。

18.5.1.1. 终端风险概况

终端风险概况可实现对已接入的全部终端运行状态进行实时监测，通过列表形式展示终端型号信息，包括终端联网 IP 地址、系统版本信息、登录时间、终端所属用户、指纹 ID、最新感知时间【感知项通过策略进行配置】、安全状态【通过对风险评估规则进行定义】、终端设备风险指数、当前存在风险【点击后可查看风险内容列表】、历史风险记录【点击查看历史风险记录信息列表】、病毒库版本信息。列表数据支持自定义展示内容与数据导出功能

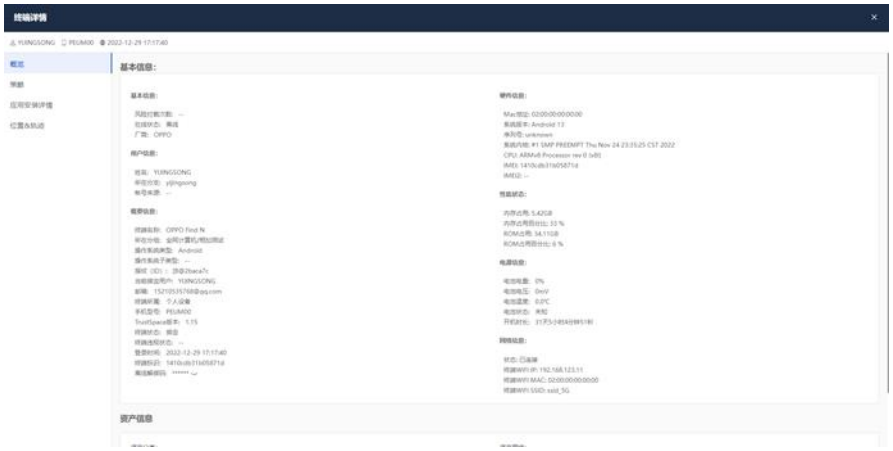
终端设备风险概况支持根据分组查找和自定义查找两种模式，用户可以在中部展示页点击左侧点击分组结构查看指定分组下的终端概况，或者输入分组名称进行精准查看。



终端详情

管理员可以通过点击终端名称查看终端设备详情概述，详情包括：终端概述、终端配置策略、应用安装详情、位置&轨迹

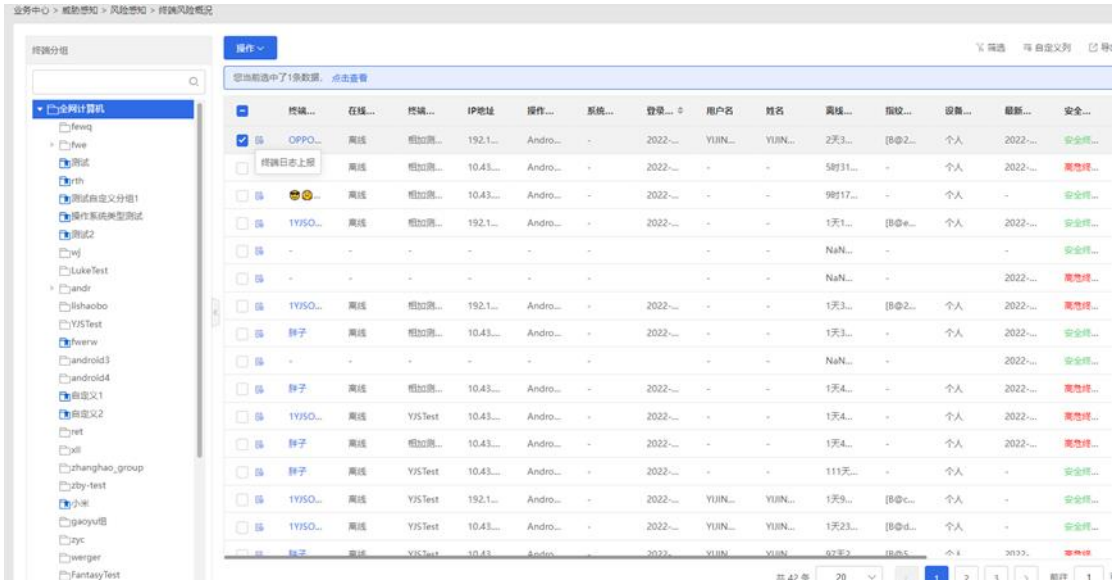
操作步骤：点击列表中终端设备名称



终端日志上报

管理员可以通过远程方式对制定终端进行日志上报操作。

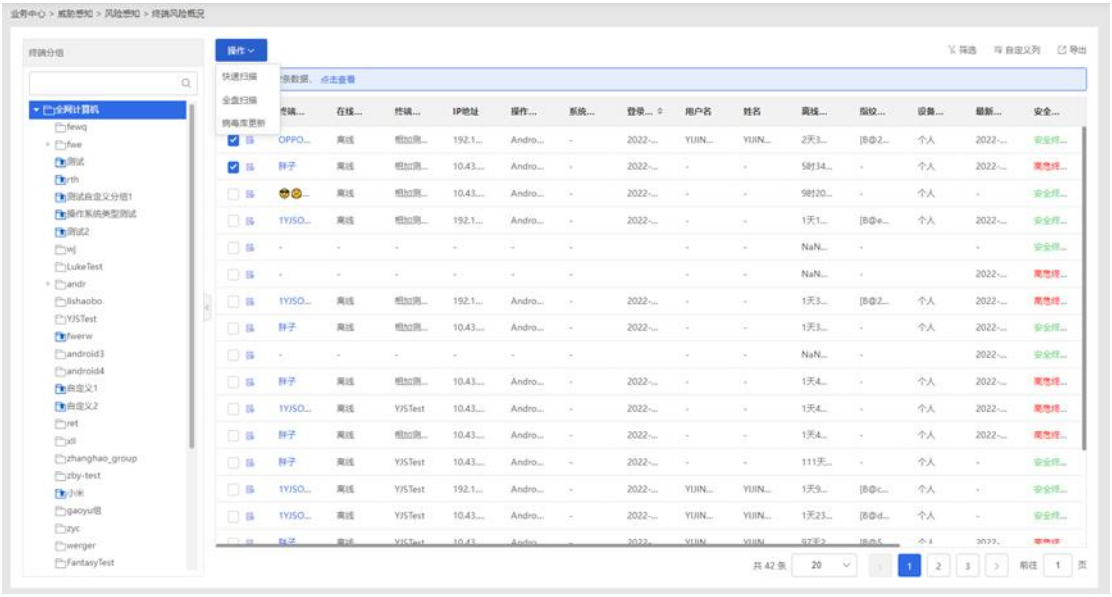
操作步骤：列表选择需要上报日志的终端，点击【 】-【终端日志上报】



快速扫描

快速扫描是对终端设备系统文件进行病毒扫描，管理员可以勾选指定（支持多选）终端设备远程进行病毒扫描。

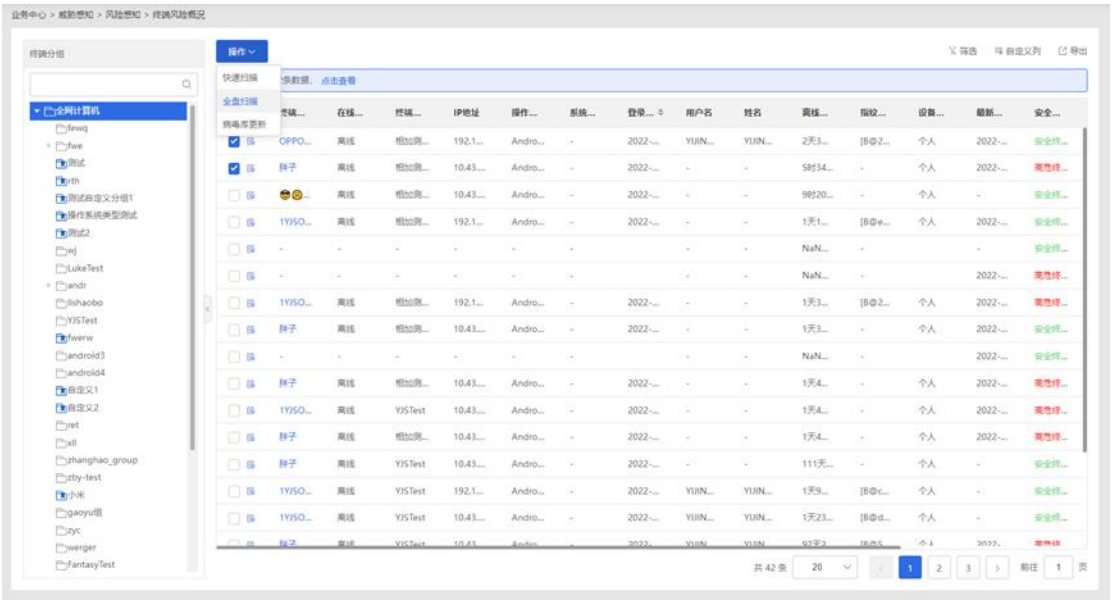
操作步骤：终端列表选择终端，点击【操作】-【快速扫描】



全盘扫描

全盘扫描是对终端设备各文件进行全量扫描。

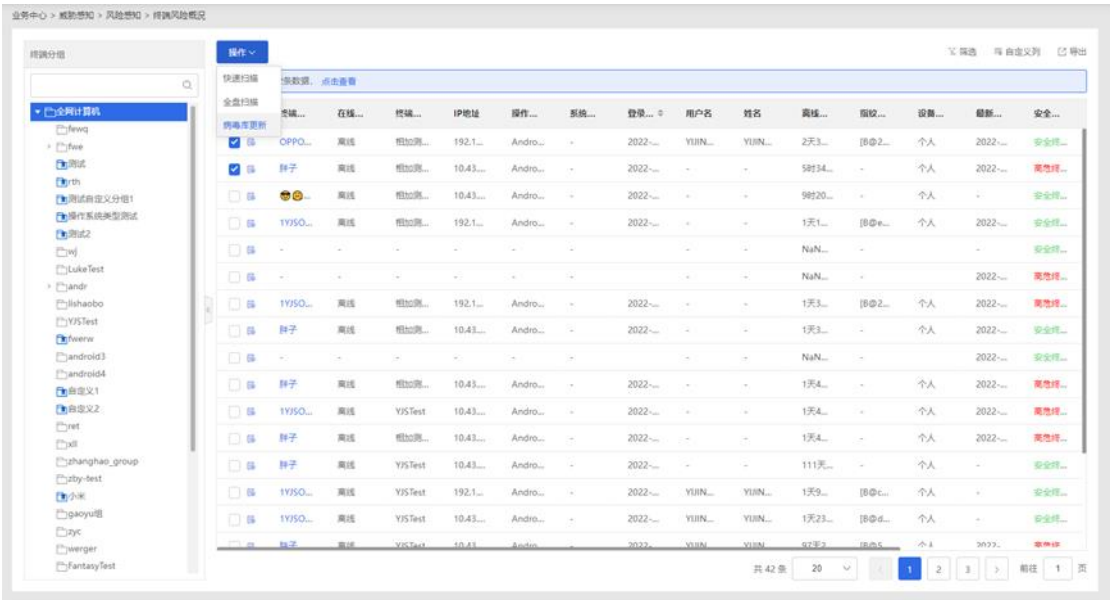
操作步骤：终端列表选择终端，点击【操作】-【全盘扫描】



病毒库更新

病毒库更新是对终端设备的病毒快进行远程更新。

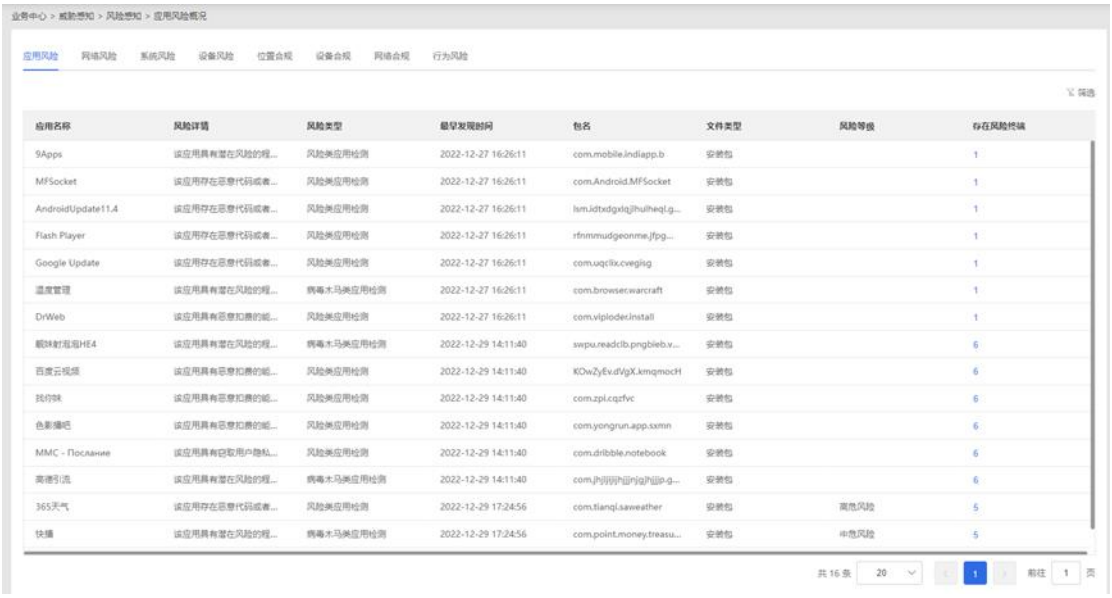
操作步骤：终端列表选择终端，点击【操作】-【病毒库更新】



18.5.1.2. 应用风险概况

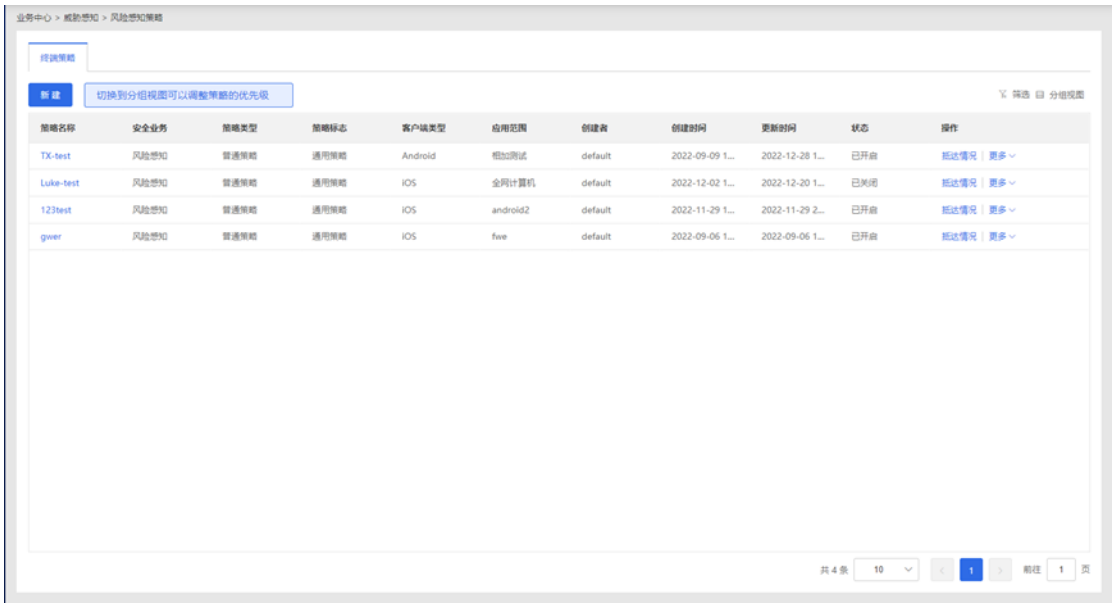
风险概况是风险、合规事件汇总展示模块，可实现查看已接入的终端发生的风险事件和触发合规事件的数据信息。风险事件包括应用风险、网络风险、系统风险、设备风险、行为风险、位置合规、设备合规、网络合规。

管理员可通过【威胁感知】-【风险感知】-【应用风险概况】页面进行查看



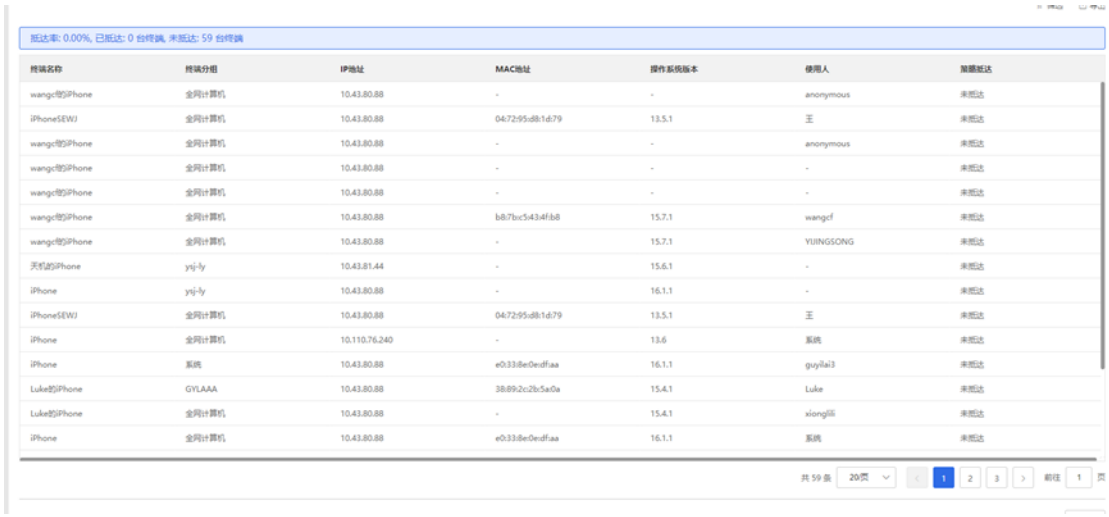
18.5.2. 风险感知策略

风险感知策略管理模块，管理员可以在该页面下创建应用防护策略，对已创建的策略进行查看与维护。

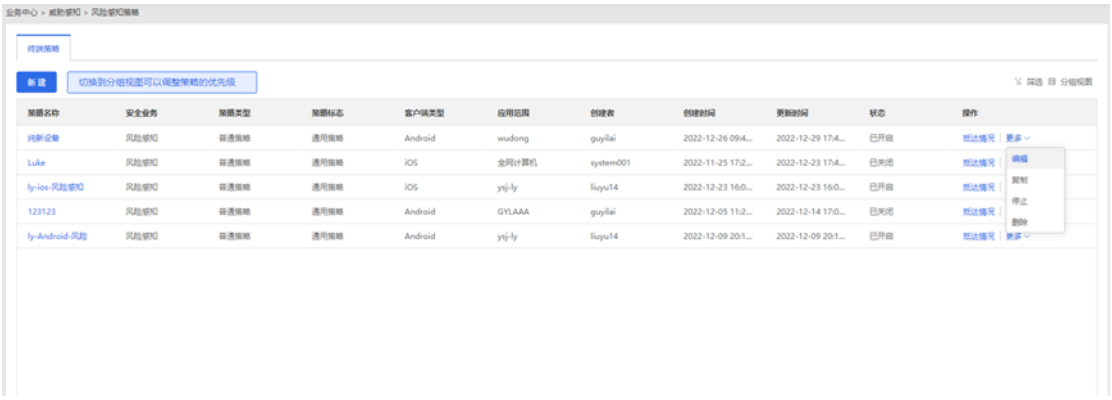


策略抵达情况

查看终端执行策略情况

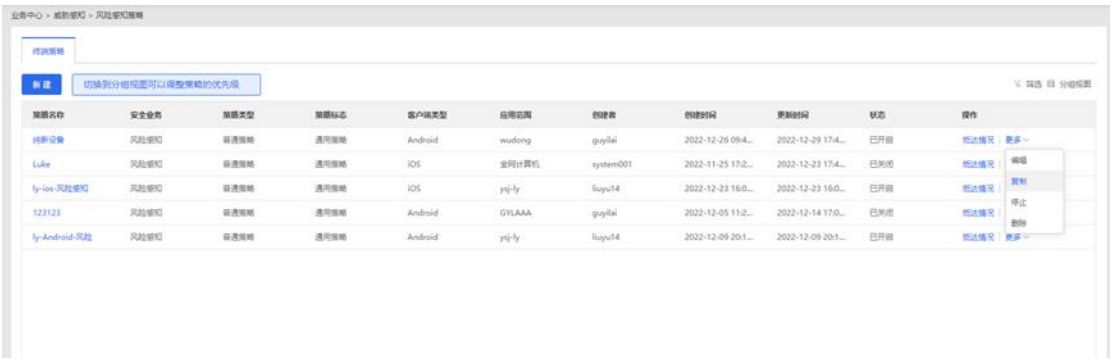


王有琦



策略复制

对指定策略进行复制生成新的策略

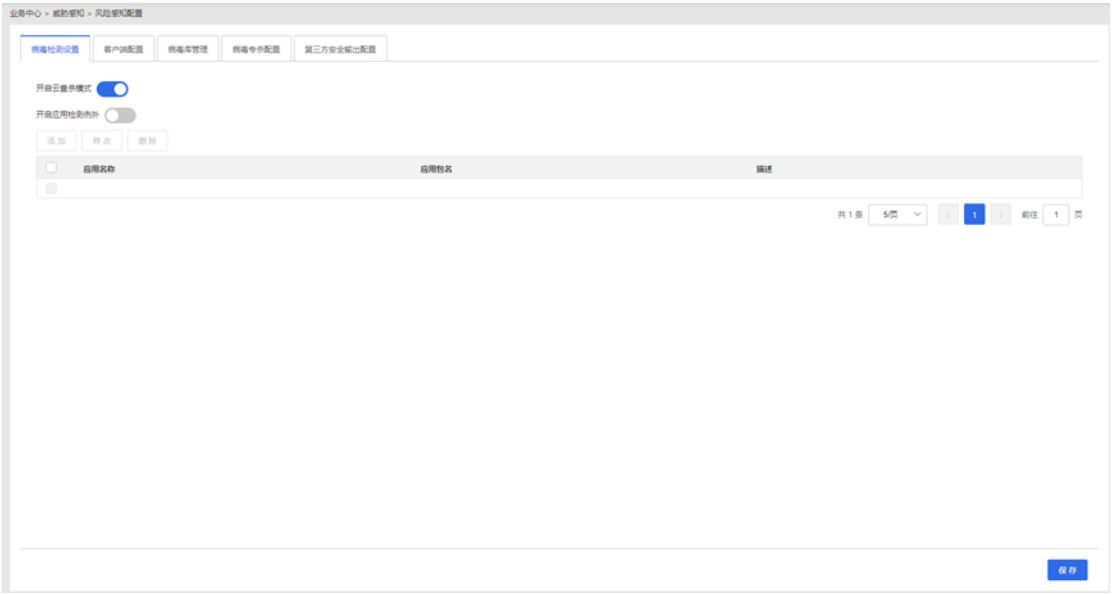


策略停止

对指定策略停止允许

18.5.3. 风险感知配置

管理可通过该模块设置病毒检测相关配置，模块包括病毒检测设置、客户端配置、病毒库管理、病毒专杀配置、第三方安全输出配置。

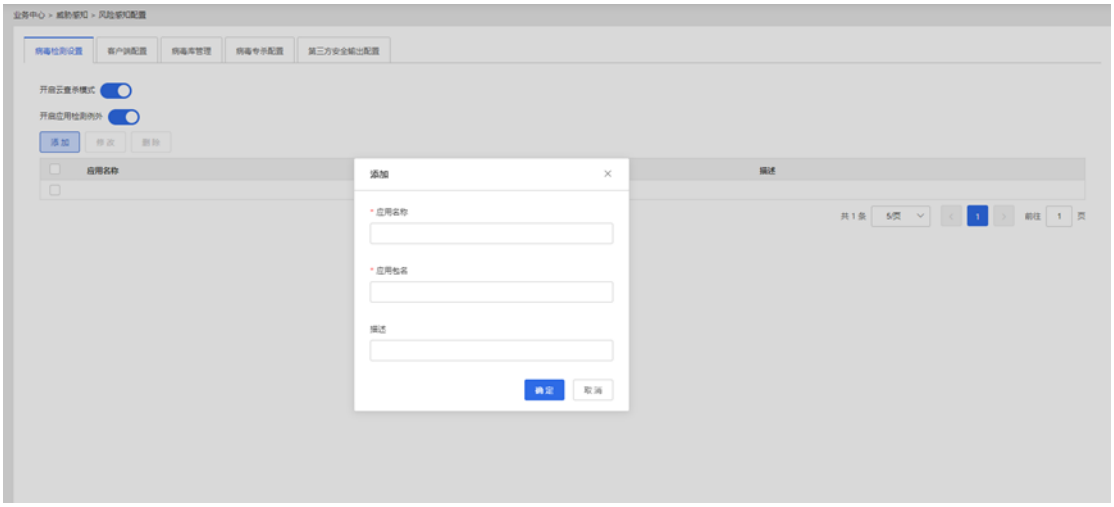


病毒检测设置

管理员可以通过该模块配置病毒检测模式和应用例外配置。

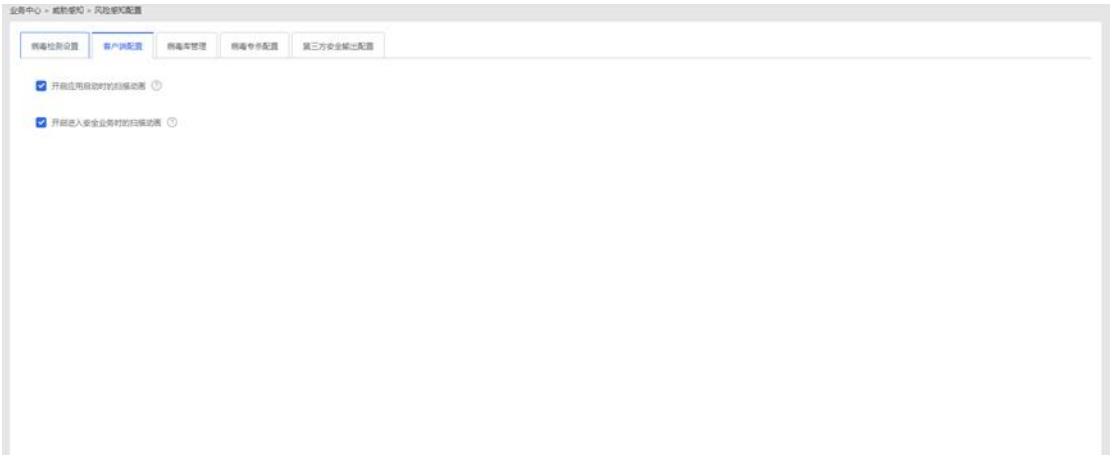
云查杀：开启后通过云病毒库进行病毒扫描，不开启时采用本地病毒库扫描。

应用检测例外：管理员可添加不需要检测的应用。



客户端配置

管理员可通过该模块配置进入应用或进入安全业务时显示检测界面。

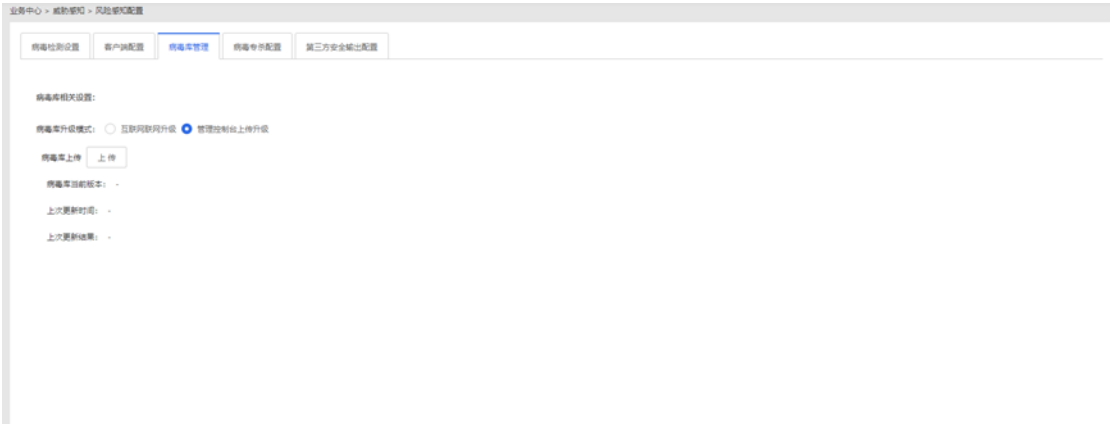


病毒库管理

管理员可通过该模块设置病毒库升级类型

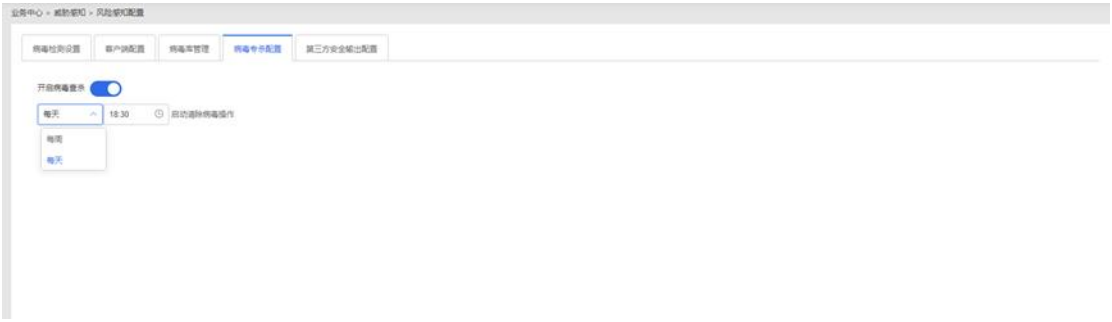
互联网联网升级：互联网升级病毒库，需要保证网络畅通。

管理控制台上传升级：服务端本地上传病毒库文件进行升级。



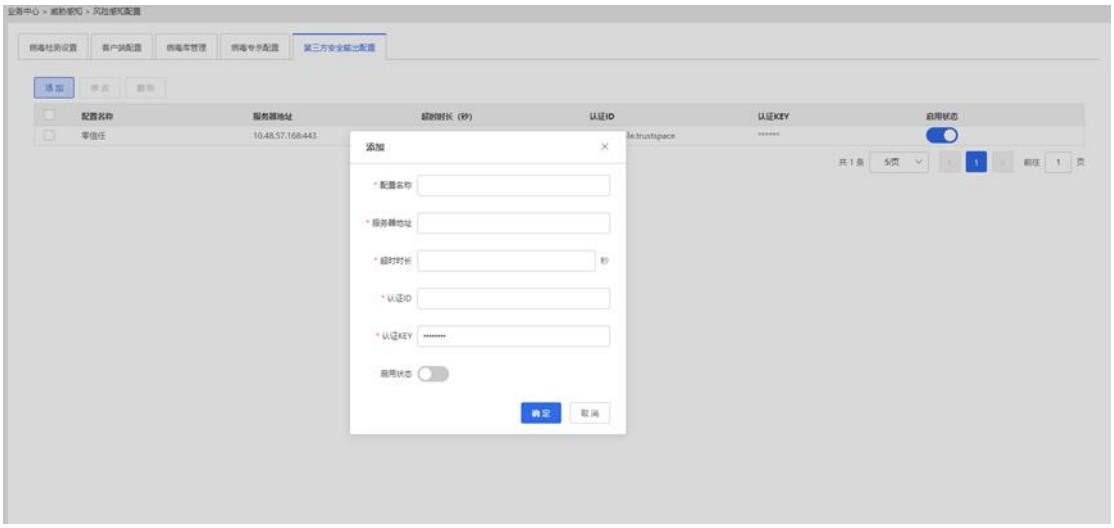
病毒专杀配置

设置病毒扫描任务



第三方安全输出配置

第三方安全验证地址配置



18.5.4. 风险评估

风险评估是对风险事件或者合规事件危险性进行定义的功能模块，可实现终端设备设备在触发风险后对该风险制定执行结构，用户可根据使用场景对风险项进行设置或者忽略风险行为，对不同风险类型可自定义评分规则。

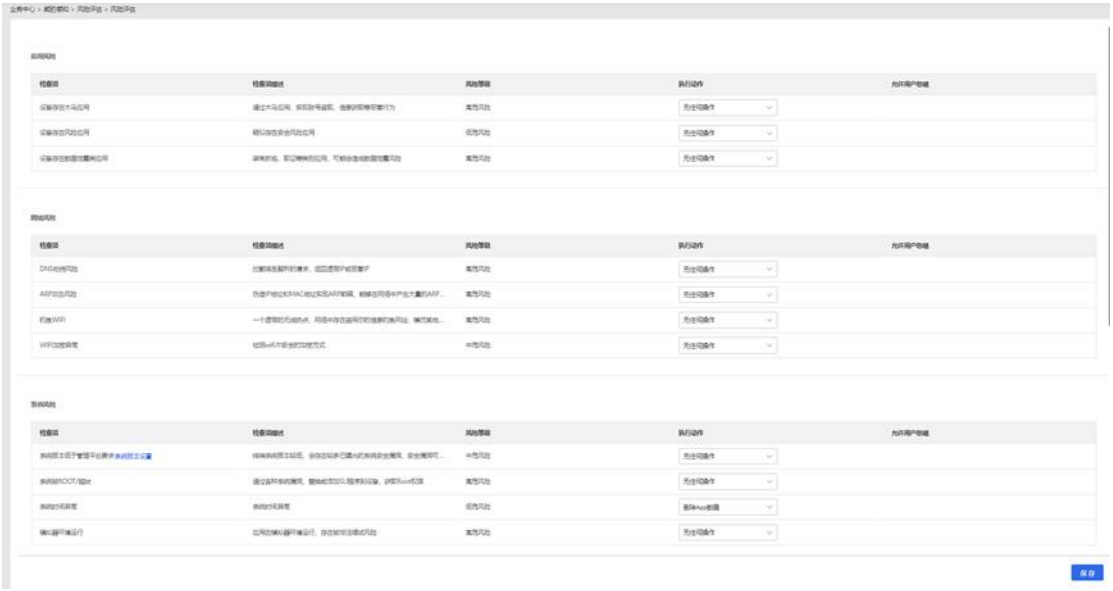
18.5.4.1. 执行动作

执行动作	描述
无任何操作	检测到风险项时不进行任何管控
阻止访问	检测到风险时阻止用户访问应用
删除 app 数据	检测到风险时清除应用数据信息
二次认证	检测到风险操作时需要进行二次身份认证
允许用户忽略	终端执行阻止访问风险应用时，用户可以忽略该提示

18.5.4.2. 风险评估

风险评估是对应用风险、网络风险、系统风险、设备风险、行为风险进行评估设置，用户选择后点击应用后生效。

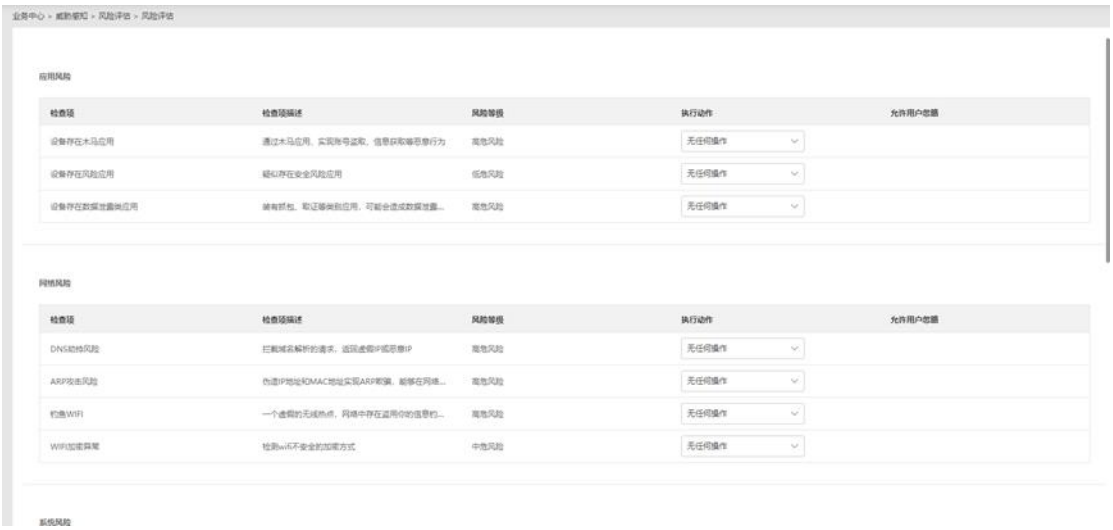
操作步骤：点击【风险评估】选择对应检测项目选择【风险等级】选择【执行动作】点击【保存】完成设置。



18.5.4.3. 合规评估

合规评估是对合规性进行风险等级和执行动作设置，可根据使用场景对合规项分别进行设置，当用户触发合规项时根据评估设置进行记录风险等级同时进行执行动作。

操作步骤：点击【合规评估】选择对应检测项目选择【风险等级】选择【执行动作】点击【保存】完成设置。

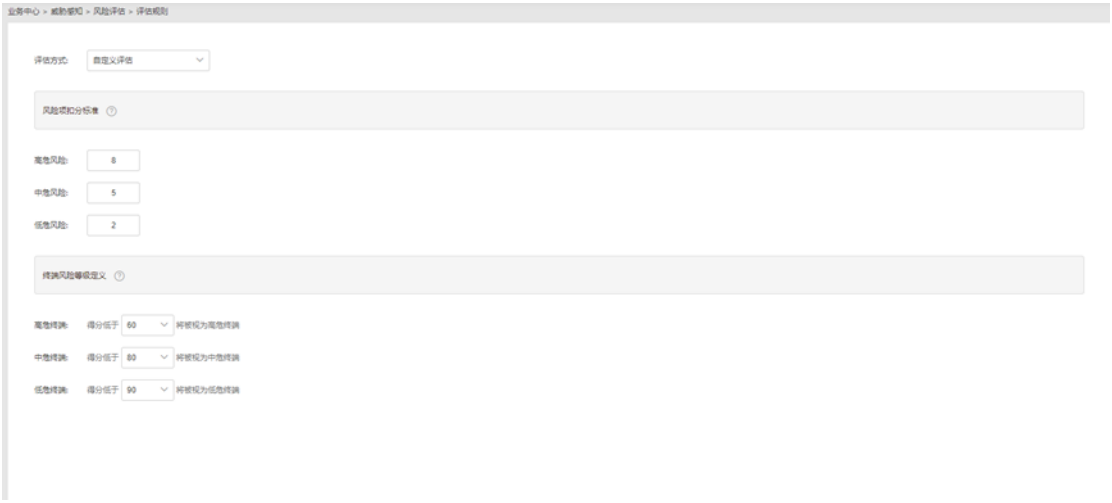


18.5.4.4. 评估规则

管理员可以通过过评估规则可以对风险等级进行扣分数值设定，并对高、中、低风险设置界限，终端设备在触发风险行为后会根据扣分数值进行记录，当数值达到某项风险等级时则在终端概况中对该终端设备的风险等级进行标注，并展示终端安全分数。

自定义评估：管理员根据业务场景自行设置评分规则

大数据智能评估：依托环境感知大数据设定的设备风险评分规则



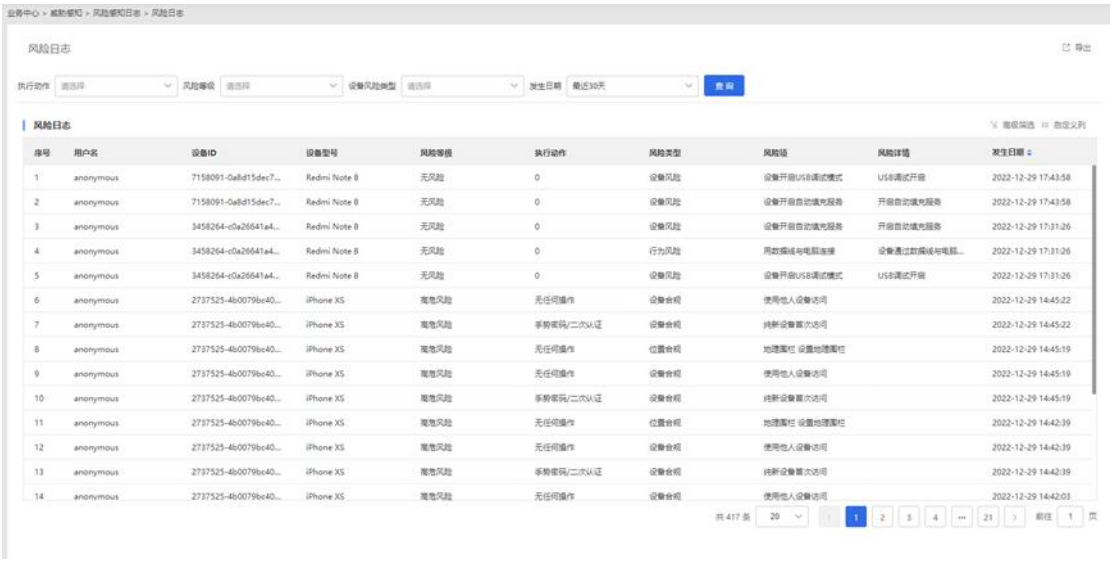
18.5.5. 风险感知日志

管理员可通过风险日志查看终端设备产生风险的详细数据，日志包括：风险日志、已拦截风险日志、已处理风险日志、专杀日志。

日志支持导出功能，管理员可点击导出选择对应的数据文件类型进行导出。

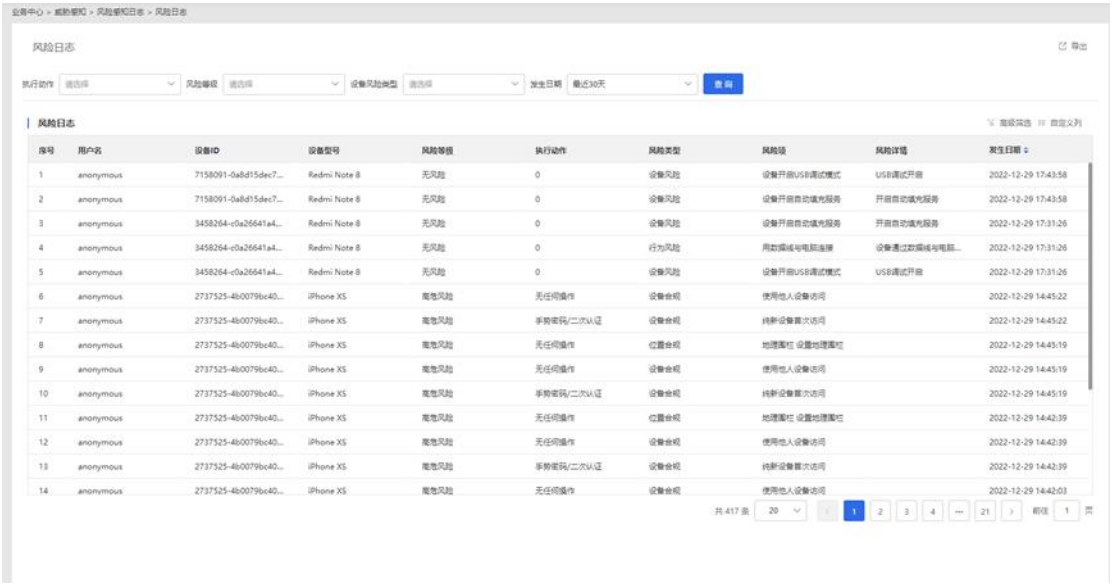
18.5.5.1. 风险日志

管理员可通过该模块查看终端设备发生风险的详细数据，风险日志数据为全量数据。



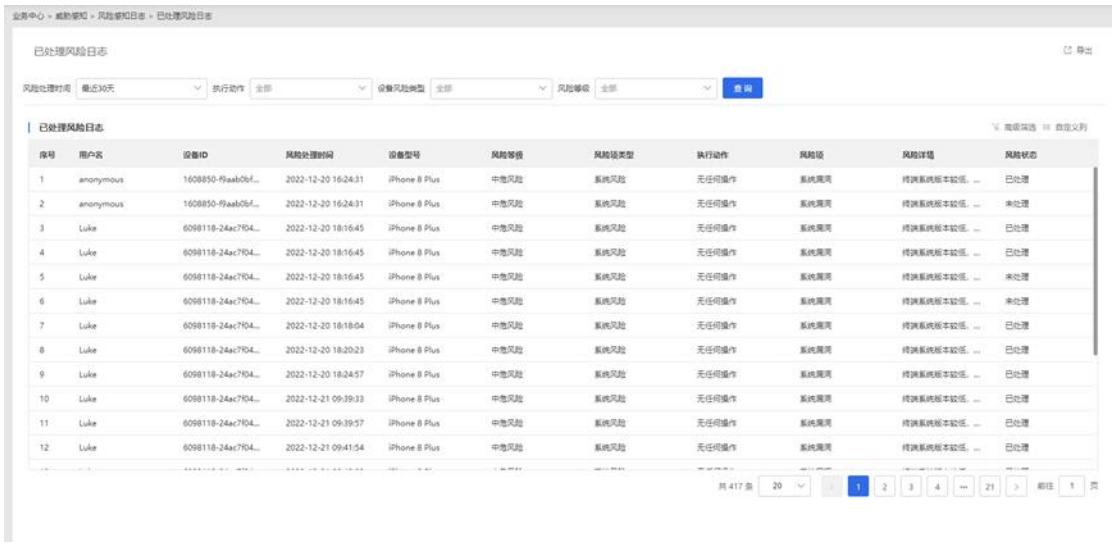
18.5.5.2. 已拦截风险日志

已拦截风险日志是查看终端设备触发风险项时被拦截的数据日志。



18.5.5.3. 已处理风险日志

管理员可通过该模块查看风险检测项处理情况。



18.5.5.4. 专杀日志

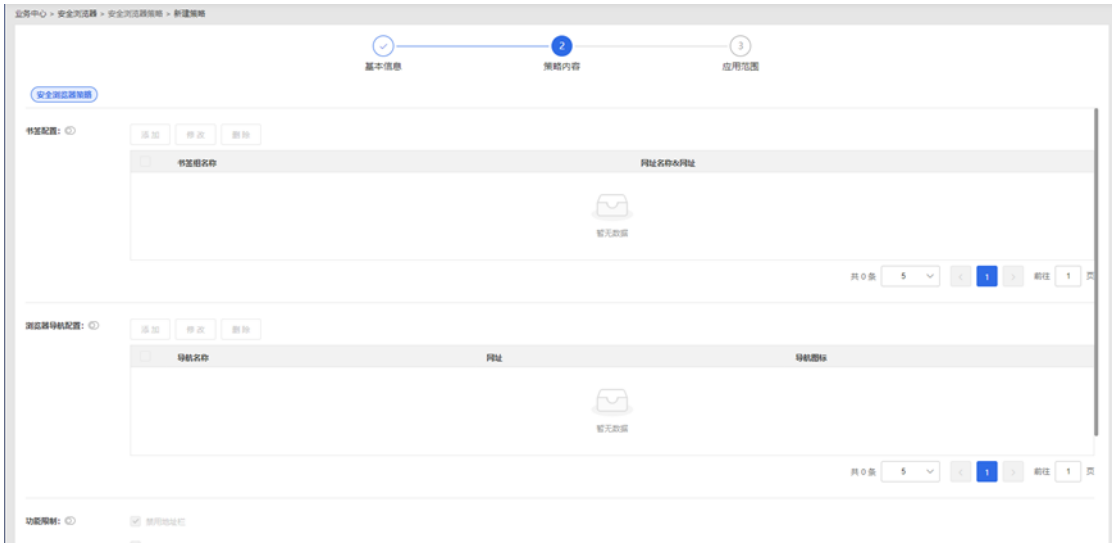
管理员可以通过该模块查看病毒查杀日志

18.6. 移动安全浏览器

该功能是通过管理平台设置终端安全浏览器访问功能、数据功能、浏览器功能的策略配置模块。

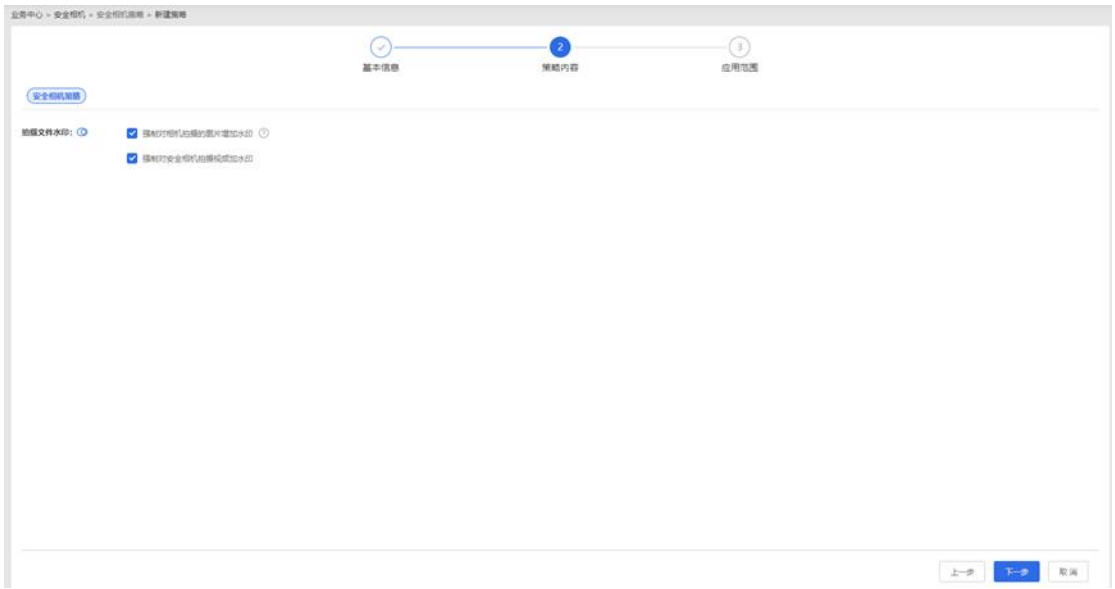
功能	描述
书签配置	配置浏览器书签
浏览器导航配置	配置浏览器导航标签
禁用地址栏	禁止使用浏览器地址栏功能
禁止打印	禁止打印浏览器访问页面

禁止保存网页	禁止保存浏览器访问网页
禁止查看网页源码	禁止操作查看网页源码功能
禁止开发工具	禁止使用开发者工具功能



18.7. 移动安全相机

该功能是对终端设备安全相机进行策略配置，管理员可通过管理平台设置安全相机在拍摄照片或视频时增加水印。



18.8. 移动业务配置

终端设备客户端版本上传功能，管理员可以在该页面下上传最新的客户端版本。

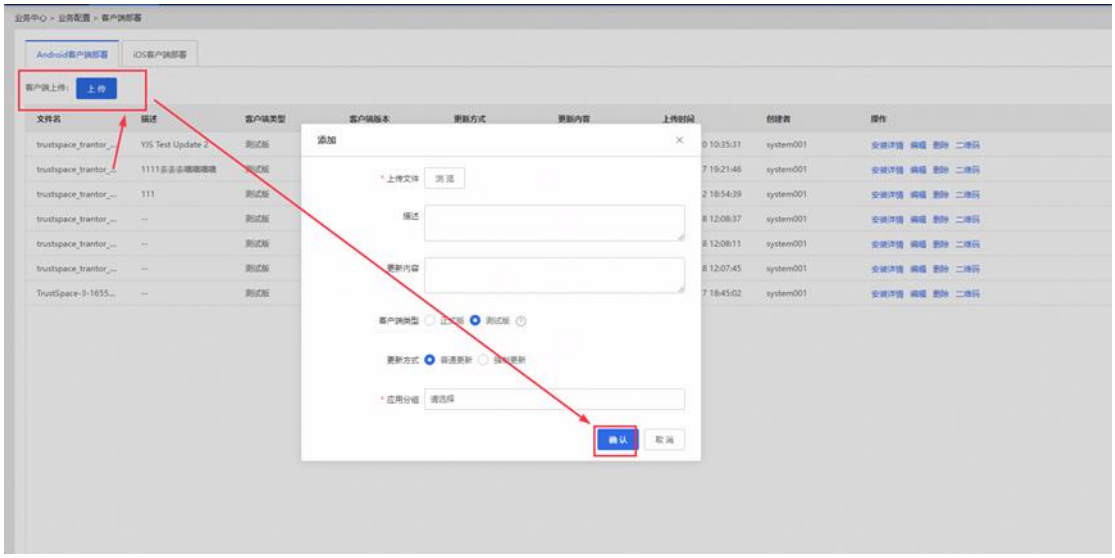
18.8.1. 客户端部署

18.8.1.1. Android 客户端部署

管理员可以在该页面下查看客户端上传历史详情，也可以在该页面下上传最新客户端版本，对已上传的客户端版本进行维护操作。

1）上传客户端

操作步骤：移动安全>业务配置>客户端配置>Android 客户端部署，点击【上传】按钮上传客户端文件，根据需要选择设置后点击【确认】完成上传。

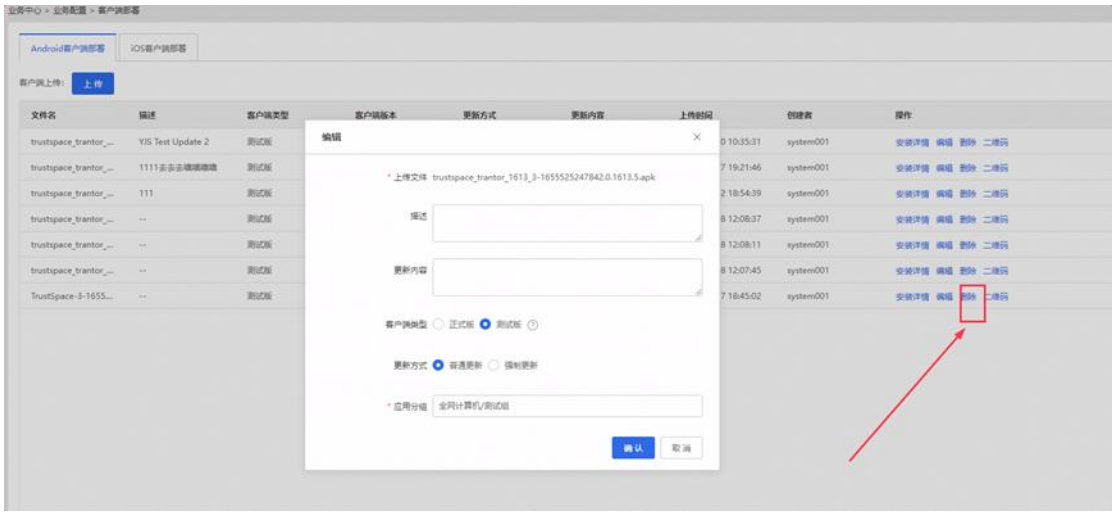


2) 安装详情

查看已安装客户端的端设备列表详情，未安装的客户端列表详情。

3）编辑

对已上传的客户端版本进行配置信息编辑。



4）二维码

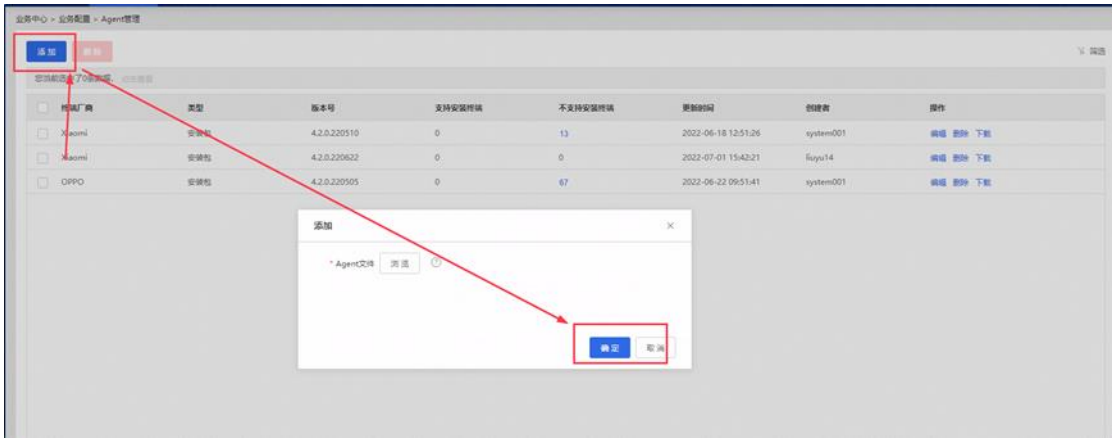
生成客户端安装二维码，终端设备可以通过扫码二维码进行安装。管理员也可以下载二维码图片或者复制下载链接发送终端用过户进行安装。

18.8.1.2. IOS 客户端部署

参考 18.8.1.1 章节

18.8.2. Agent 管理

管理员可以在该页面添加 Agent 安装包，同时在该页面对添加的安装包进行编辑、删除、下载操作。



18.8.3. 终端管理配置

终端管理配置是对终端所需设置进行配置，管理员可以在该页面配置终端管理配置、NAC 准入配置、ICG 准入配置、客户端界面配置、IOS 设备管理配置。

18.8.3.1. 终端管理配置项

终端管理配置项可以对客户端强制验证登录密码时间、客户端二维码分享、客户端用户反馈接收邮箱、客户端解绑配置进行管理。

操作步骤：【移动安全】-【业务配置】-【终端管理配置】-【终端管理配置】

客户端强制重新验证登录密码时间配置

设置客户端登录一定时间后强制客户端重新进行验证登录，时间可以自行配置

客户端二维码分享配置

设置客户端安装包下载二维码下载地址，用户可以访问地址下载安装二维码

客户端解绑配置

开启客户端切换，原登录用户自动解绑，新用户自动绑定

客户端用户反馈接收邮箱

客户端用户信息反馈接收邮箱

18.8.3.2. NAC 准入配置

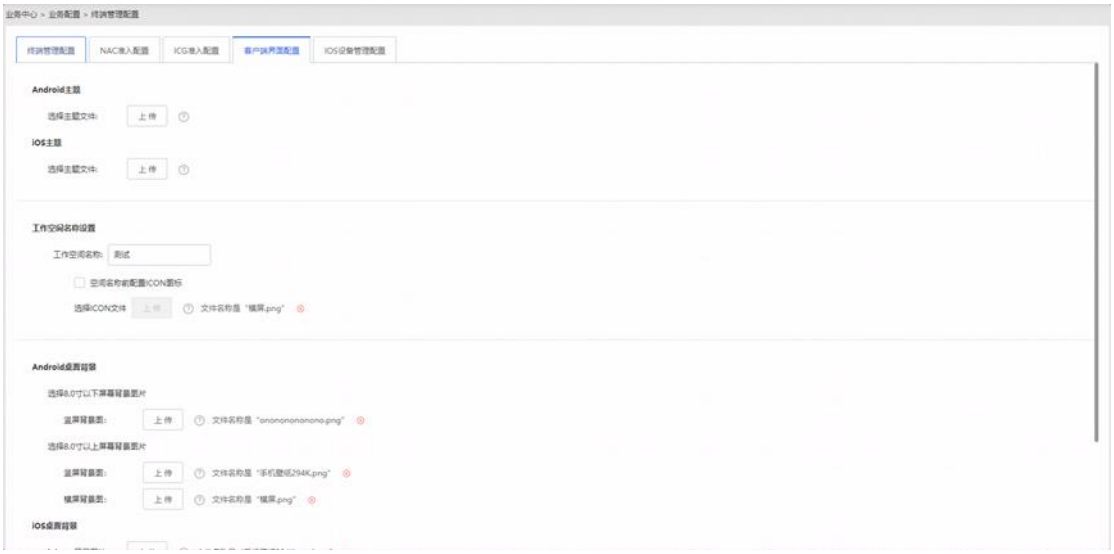
开启配置 NAC 网络准入。设置服务器地址与发送间隔时间。

18.8.3.3. ICG 准入配置

开启配置 ICG 网络准入。设置服务器地址与发送间隔时间。

18.8.3.4. 客户端界面配置

管理员可以在该页面根据终端设备激活方式，设置客户端界面。



19. 安全小助手

19.1. 基本概念

安全小助手，专为客户提供实用的系统、网络管理小工具。

19.2. 垃圾清理

垃圾清理软件是一款可以帮助用户，快速清理电脑上软件安装残留文件以及系统历史记录等垃圾文件的小工具，及时释放更多的磁盘空间，最大限度提升系统运行速度。具有安全快速地扫描，精准的查找并定位到需要清理文件的特点。

19.2.1. 基本功能

19.2.1.1. 扫描本地垃圾

入口：右键托盘>垃圾清理 或 客户端主界面>安全小助手。

右键天擎托盘，进入垃圾清理主界面。

点击“开始扫描”可进行本地垃圾文件的扫描。

点击‘取消扫描’，扫描停止，返回垃圾清理主界面。

扫描完成后，展示结果界面。

19.2.1.2. 清理本地垃圾

扫描完成后，将展示垃圾文件扫描结果界面。

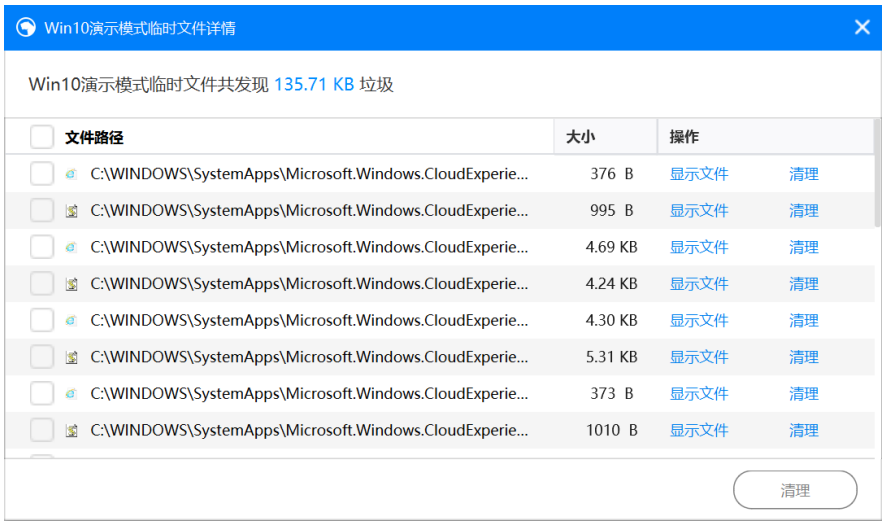
- 点击“重新扫描”，将进行垃圾文件的再次扫描；

➢ 点击“一键清理”，可进行垃圾文件的清理；

注意：默认仅勾选垃圾清理规则内匹配上的文件，其余文件的删除，需要用户手动选择并执行删除操作。

➢ 点击“⌄”，可查看对应文件目录下的子文件；

➢ 点击“ ”，可查看文件详情；



✓ 点击“显示文件”，直接跳转到文件所在目录；

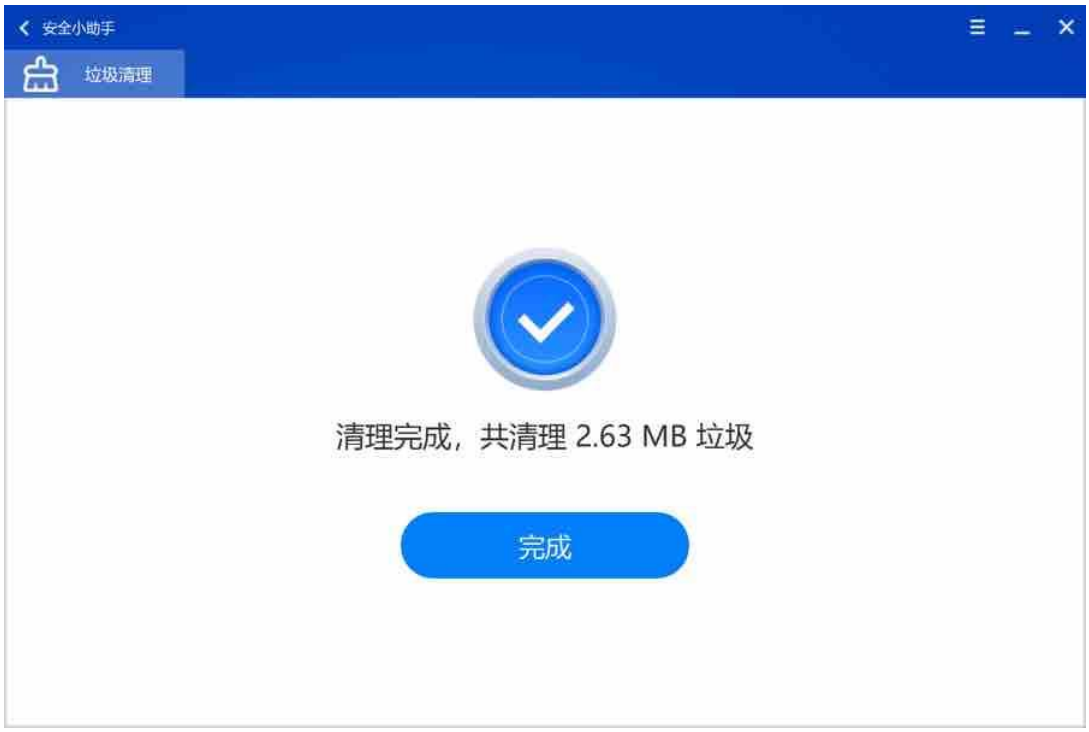
✓ 点击“清理”，可进行详情文件的清理（支持单一文件/多文件清理）。

➢ 点击“忽略”，可进行垃圾文件的忽略操作，对于忽略的文件，可在忽略区中进行查看。

备注：在垃圾清理的下一次扫描中，对于忽略区中的文件，将不再进行扫描。

对于风险文件执行删除时，将弹窗展示提示信息，由用户自主决定是否删除。

清理完成后，显示结果界面。



点击“完成”返回垃圾清理主界面，界面中将展示上次垃圾清理时间以及释放存储空间。

19.3. 垃圾清理库更新设置

19.3.1. 系统更新设置

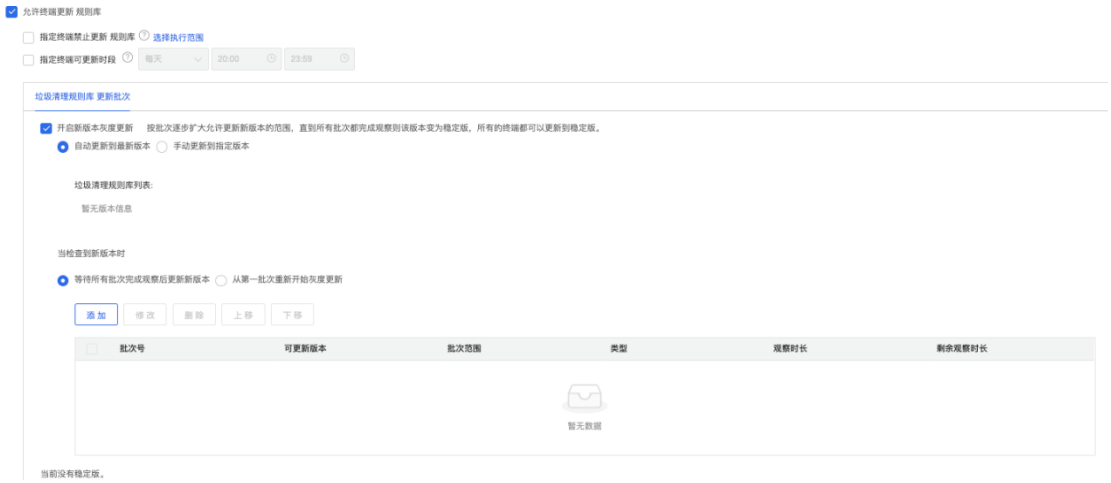
入口：系统管理>更新管理>安全小助手。

该模块设置垃圾清理规则库的更新时间，支持按月、周、天、小时周期性自动更新。

19.3.2. 终端更新设置

入口：系统管理>更新管理>安全小助手。

该模块设置全网终端更新垃圾清理规则库的时间，即清理规则库更新的灰度批次。



19.4. 启动项管理

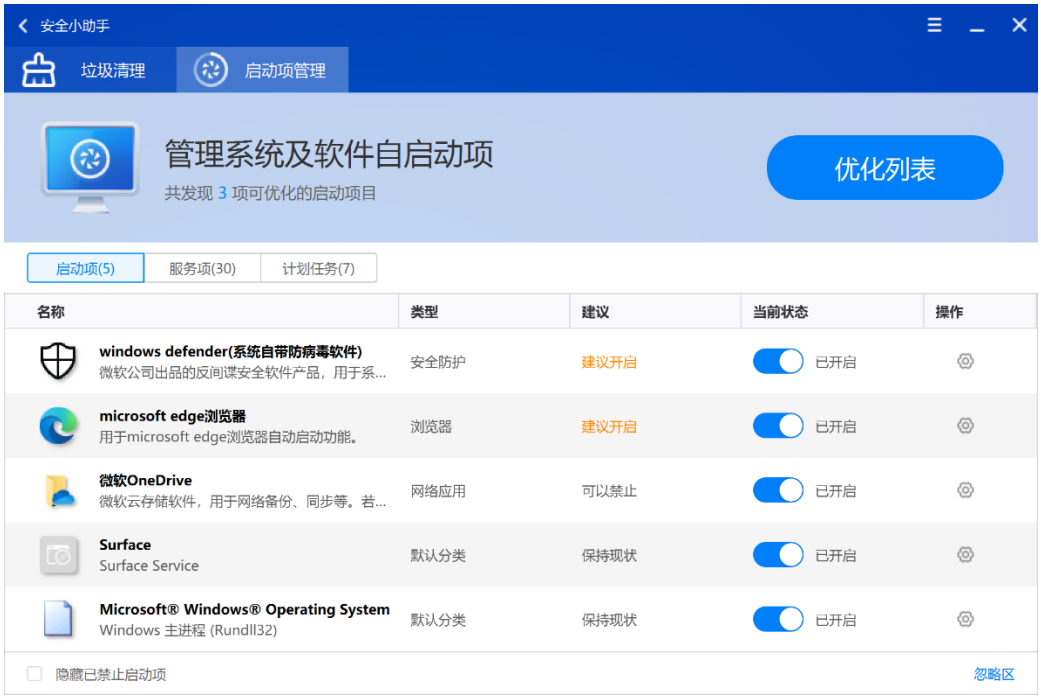
启动项管理工具可有效管理系统及软件的自启动项，提升开机速度，优化客户体验。

19.4.1. 基本功能

19.4.1.1. 检测系统启动项

入口：右键托盘>启动项管理 或 客户端主界面>安全小助手。

右键天擎托盘，进入启动项管理主界面，系统将自动检测出系统及软件启动项信息。



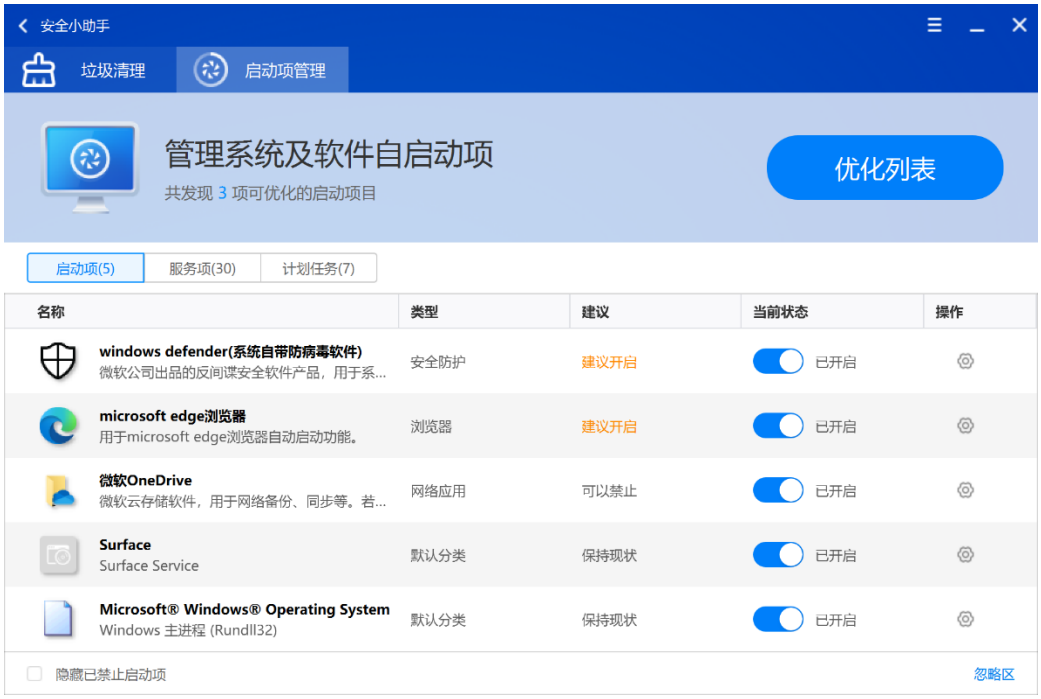
点击“服务项”可查看自启动的服务信息。

点击“计划任务”可查看自启动的计划任务信息。

点击左下角“ 隐藏已禁止启动项 “，可自动隐藏已设置为禁用的启动项。

19.4.1.2. 优化启动项

进入启动项管理界面，将自动检测出系统及软件启动项信息。



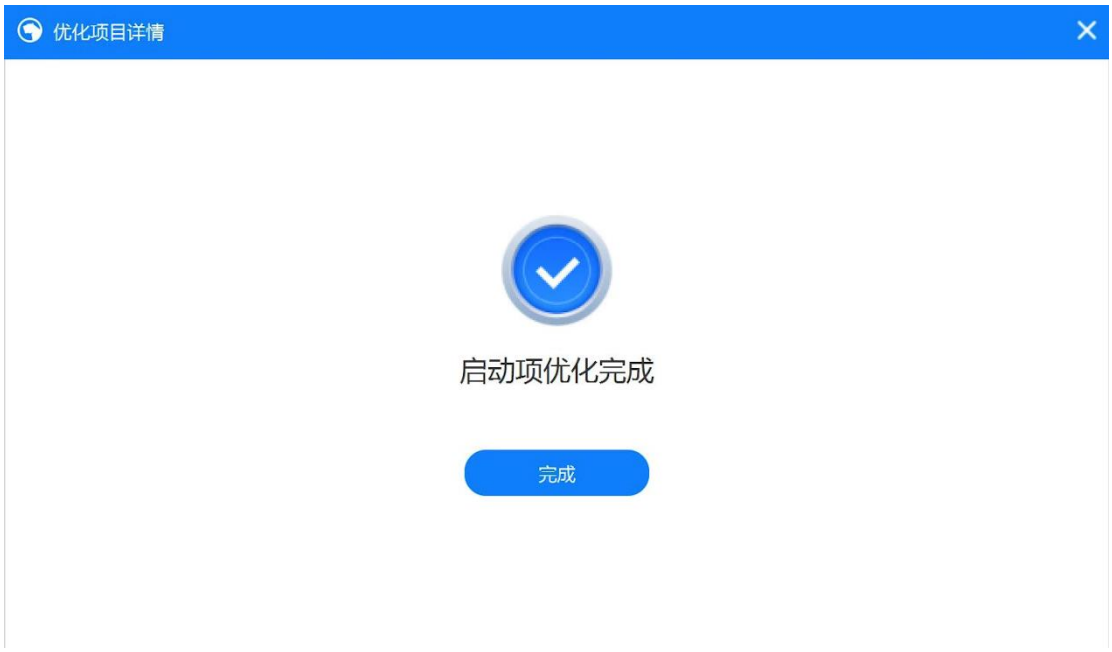
- 点击当前状态“ 已开启 ”，可直接进行当前启动项的关闭/开启；

- 点击“ ”，可展示当前启动项对应的操作菜单；
- 点击“打开目录”，直接跳转到文件所在目录；
- 点击“忽略此项”，可进行启动项文件的忽略操作，对于忽略的文件，可在忽略区中进行查看。

备注：在启动项管理的下一次检测中，对于忽略区中的文件，将不再进行识别。

点击“优化列表”，可展示推荐开启/关闭的启动项。

- 点击“忽略”，可针对当前的启动项进行忽略；
- 点击“优化”，可针对当前的启动项进行优化；
- 点击“一键优化”，可针对当前界面中所有启动项进行优化，优化完成后，弹出优化完成界面。



点击“完成”返回启动项管理主界面。

19.5. 启动项管理更新设置

19.5.1. 系统更新设置

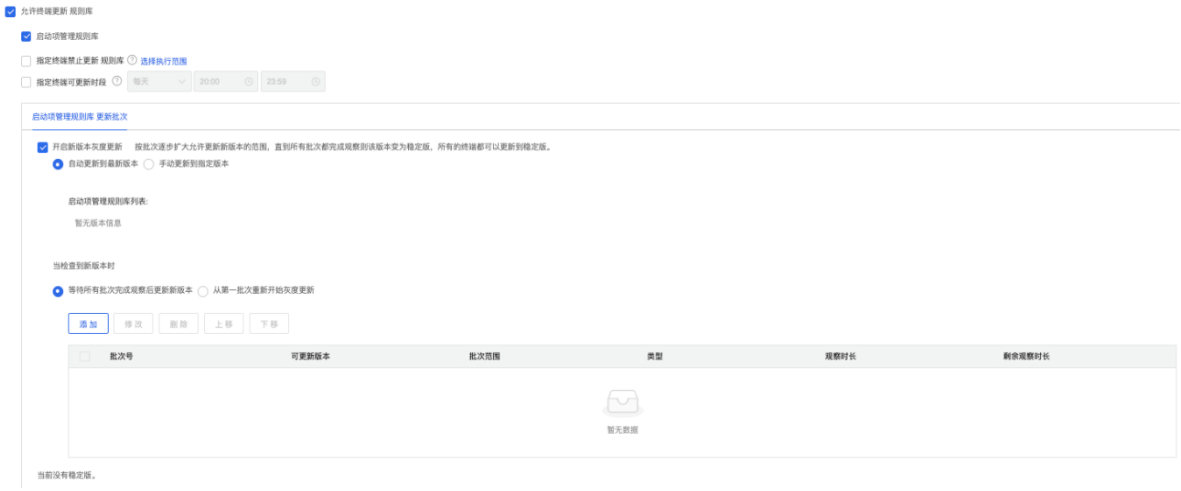
入口：系统管理>更新管理>安全小助手。

该模块设置启动项管理规则库的更新时间，支持按月、周、天、小时周期性自动更新。

19.5.2. 终端更新设置

入口：系统管理>更新管理>安全小助手。

该模块设置全网终端更新启动项管理规则库的时间，即清理规则库更新的灰度批次。



20. 文件分发

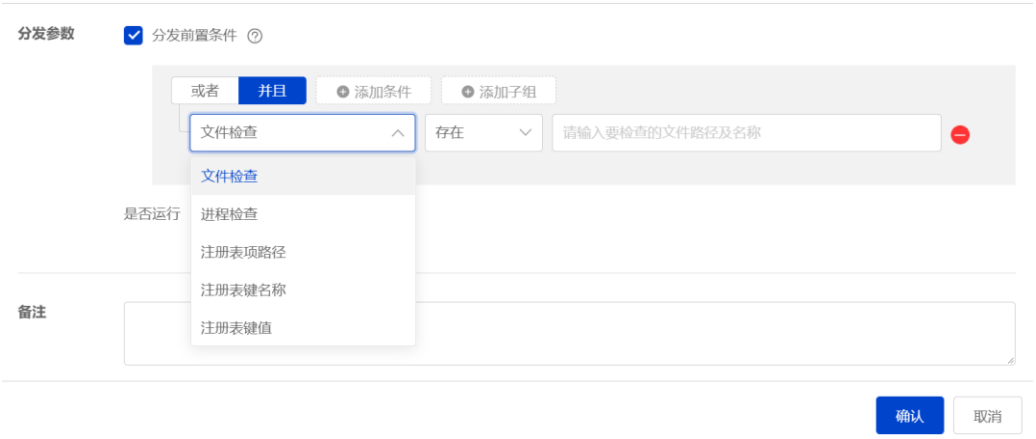
20.1. 基本概念

20.1.1. 文件分类

文件分类功能是按照文件或软件的不同用途对其分类，方便对同一类文件进行管理。对软件进行自定义分类。

20.1.2. 分发前置条件

分发前置条件是指对软件分发之前进行条件检查和判断，按照条件包括：文件检查，进程检查，注册表项路径，注册表键值，注册表名称。

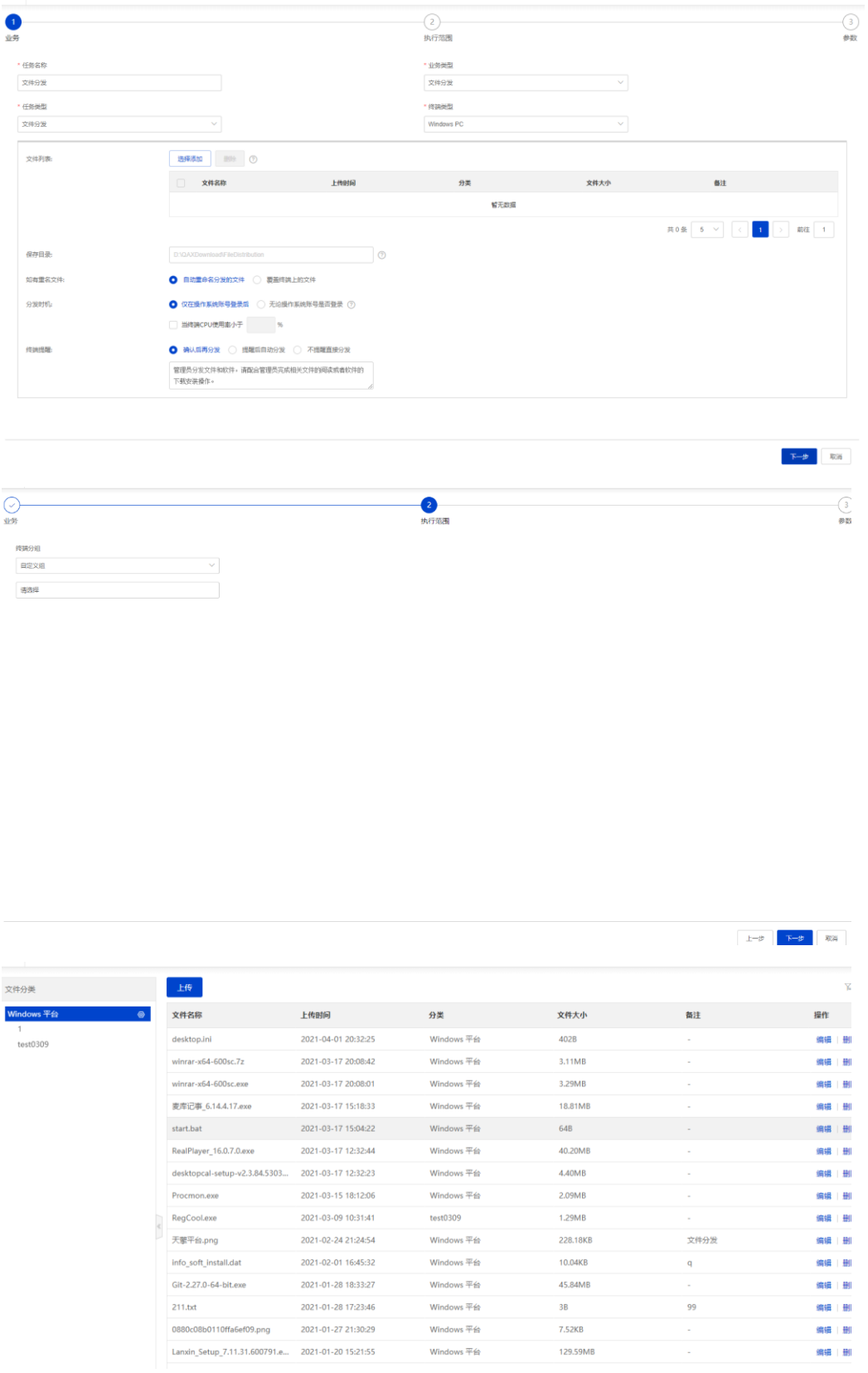


20.1.3. 筛选

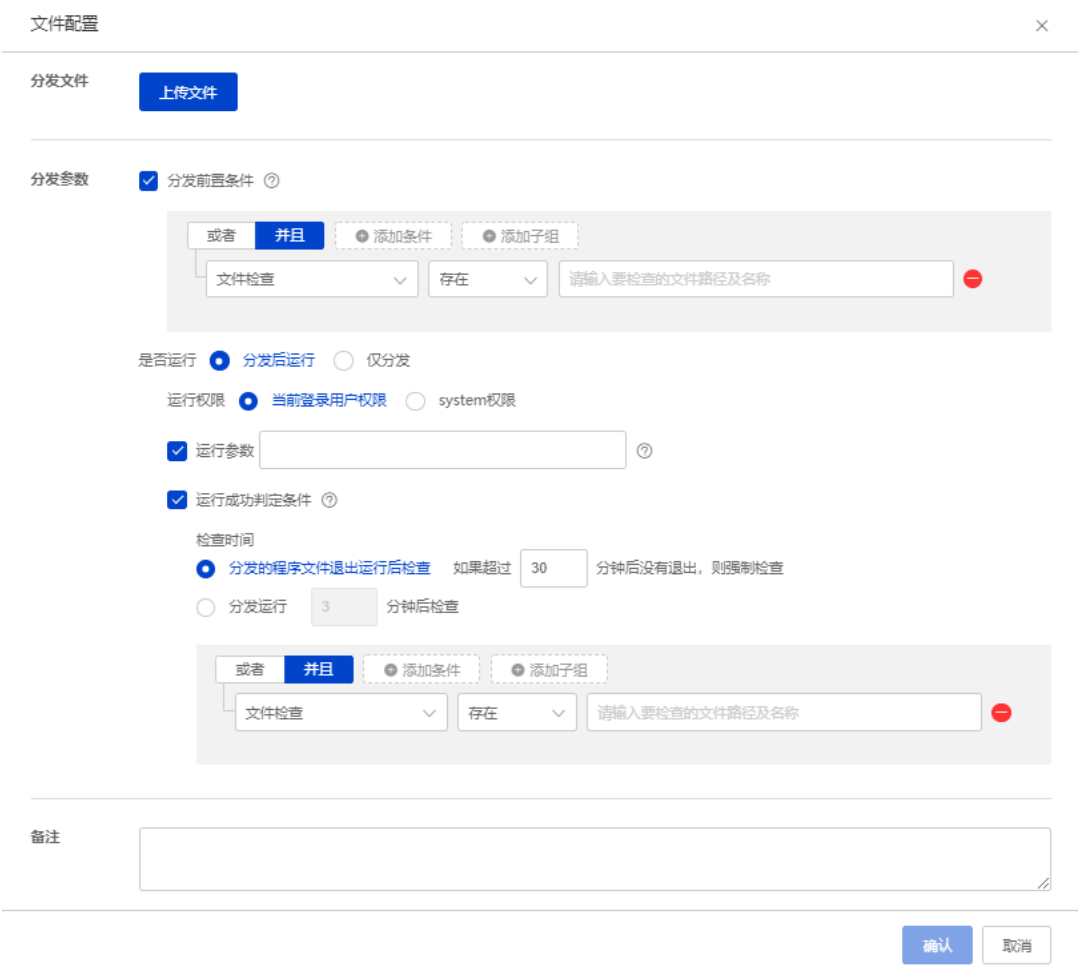
筛选是根据文件的文件名称，备注，文件大小，上传时间对当前分组中的文件进行筛选。筛选规则包括“包含”和“不包含”两种。

20.2. 文件分发策略

文件分发配置：在终端管理>终端任务中新建一个文件分发任务。在文件列表中添加已上传好的文件，设置保存路径和分发时间。最后选择需要下发的终端即可完成设置。



文件分发过程首先上传需要分发的软件，接着配置文件分发参数，分发参数包括软件运行参数，运行成功判定条件和文件检查频率。设置好下发范围进行文件的分发。



【注意】任务形式下发文件功能是为了方便管理员向终端快速分发各类文件，但在使用过程中可能因为配置检查不够或下发文件的兼容性或文件安全性问题导致出现无法预料的结果，分发文件的大小也可能会影响组织内网络流量占用。建议根据企业实际网络情况，操作时通过分组分批下发并随时观察文件分发任务的执行情况，以确保结果和预期一致。

21. 弹窗防护

21.1. 基本概念

终端启用弹窗防护功能可有效拦截第三方软件弹出的暴力、色情、游戏类的广告，避免日常工作或教学过程中出现软件弹窗受到影响。尤其在教学过程中弹窗会恶意转移学生注意力以及需退出全屏 PPT 关闭弹窗，严重影响教学质量，弹窗防护可直接阻止软件的弹窗，避免弹窗对终端用户造成影响。

21.2. 基本功能

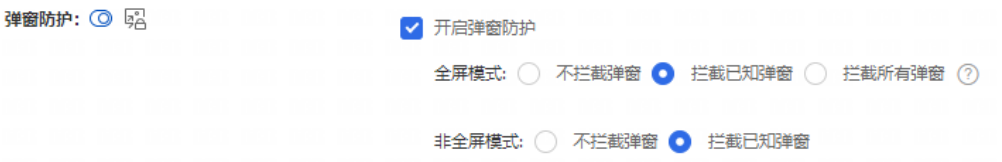
21.2.1. 策略配置

入口：安全小工具>弹窗防护>策略管理

21.2.1.1. 拦截模式设置

弹窗拦截分为全屏模式下拦截和非全屏模式下拦截两种模式，开启弹窗防护功能后，两种模式下均默认拦截已知弹窗。

- 全屏模式：全屏模式下启用的弹窗拦截模式
- 非全屏模式：非全屏模式下启用的弹窗拦截模式



注：仅在全屏模式下，支持拦截所有弹窗。由于此模式下，除当前全屏软件进程弹窗不拦截，其余进程的弹窗均会被拦截，请谨慎开启，推荐常规配置“拦截已知弹窗”。

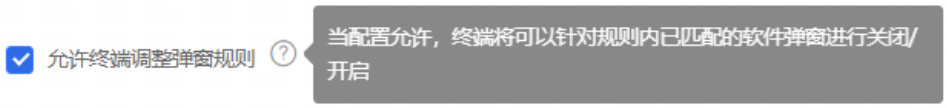
拦截询问设置

通过历史数据统计发现，终端用户对于部分弹窗的处理方式存在差异。针对此类弹窗，为避免误拦的行为，增加拦截询问设置，一旦开启后，由终端用户自主判断是否需要拦截。

注：询问窗口规则目前由独立团队持续运营，云规则中配置为需要询问的弹窗规则，终端识别后才会显示提示条。

21.2.1.2. 终端关闭软件拦截设置

通过此配置，可实现终端用户自主关闭/开启软件拦截的功能。



注：1）配置后，终端用户可在弹窗防护主界面中，在不同软件弹窗拦截记录的对应拦截设置上，支持进行开启/关闭配置；

2）云规则以及本地规则弹窗软件均支持；

3）仅支持规则库中适配过的软件。

21.2.1.3. 历史弹窗记录设置

目前终端支持用户主动触发弹窗记录的功能，一旦开启后，所有的弹窗信息将实时记录并保存在本地，此功能主要实现定期将本地弹窗信息进行清理的能力。

21.2.2. 弹窗防护本地规则

入口：安全小工具>弹窗防护>弹窗防护本地规则。

弹窗规则由云规则以及本地规则两部分组成，本地规则为云规则的补充，对于云规则中暂不支持的弹窗，企业内部管理员可自主增加。目前系统支持手动添加以及通过终端上报弹窗中添加两种方式实现本地规则的添加管理。

- 弹窗阻止规则：管理员添加发布后，终端将对此规则内的弹窗进行拦截；
- 弹窗例外规则：管理员添加发布后，终端将对此规则内的弹窗进行例外，此规则主要用于发生弹窗误拦截时的紧急加白。

  备注：弹窗例外规则优先级高于阻止规则。

21.2.2.1. 终端上报弹窗添加规则

目前终端主动捕获的弹窗将自动上报到管理中心，按照同一个规则上报的终端数量进行倒序展示，便于管理员通过弹窗的影响范围，将弹窗规则添加到本地规则中。

入口：安全小工具>弹窗防护>弹窗防护本地规则>终端上报弹窗。

注：

1、终端上报弹窗界面中展示为终端用户期望添加拦截的规则，推荐管理员采用此界面方式进行漏拦截的规则的添加。

2、终端上报弹窗界面仅支持阻止规则的添加，弹窗例外规则需要用户在弹窗例外界面中手动添加。

21.2.2.2. 手动添加规则

入口：安全小工具>弹窗防护>弹窗防护本地规则>弹窗阻止规则/弹窗例外规则。

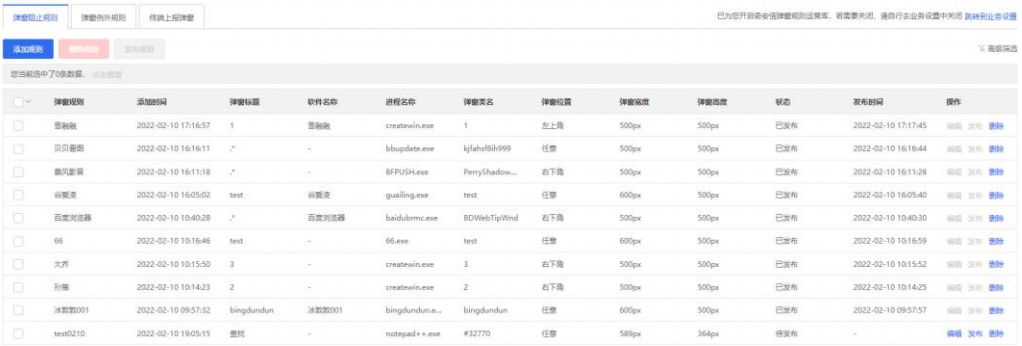
管理员可通过点击“添加规则”进行弹窗规则的添加。

注：1）弹窗阻止规则以及弹窗例外规则均支持手动添加；

2）弹窗信息的获取方式请联系奇安信技术人员支持。

21.2.2.3. 规则的发布

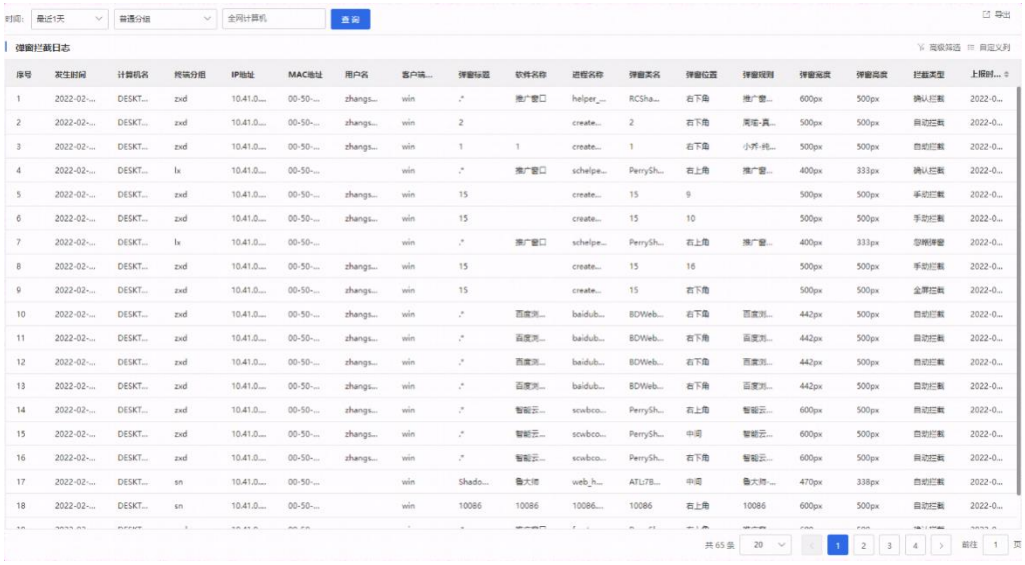
规则添加成功后，管理员需要针对已添加的规则执行发布操作。发布成功后，此规则将在终端立即生效。



注：未发布的规则支持编辑和删除，已发布的规则仅支持删除。

21.2.3. 弹窗防护日志

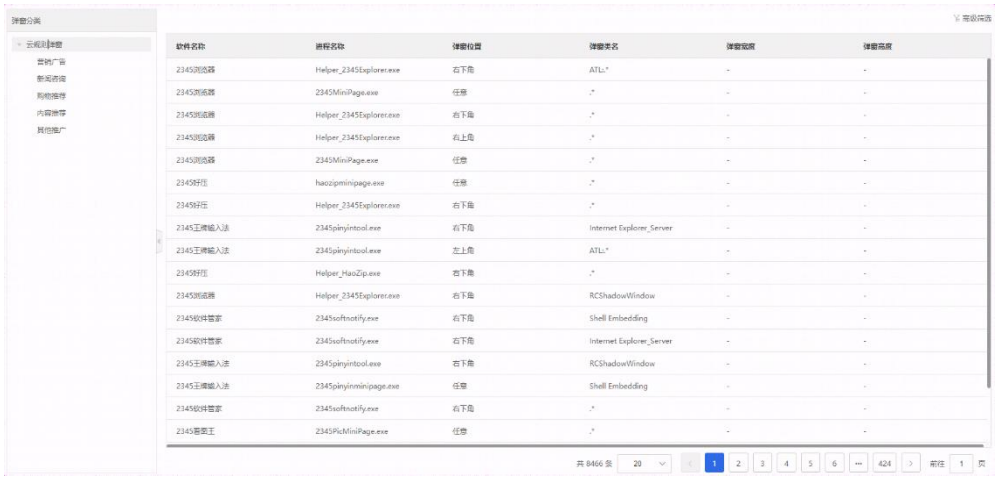
终端匹配相关弹窗规则进行拦截后，会上报被拦截弹窗相关信息，可按分组、按时间查询弹窗拦截日志，日志中详细记录被拦截弹窗的信息，如下图：



21.2.4. 弹窗防护云规则

入口：安全小工具>弹窗防护>业务设置。

管理中心支持进行云规则的查看，可按软件名称、弹窗位置、进程名称以及弹窗类名进行规则的查询，如下图：



注：管理中心支持关闭弹窗防护云规则，仅启用本地规则。

21.2.5. 捕获弹窗

入口：右键托盘>弹窗防护 或 客户端主界面>弹窗防护。

第三方软件广告弹窗未被拦截，终端用户可通过天擎主动捕获第三方软件弹窗规则并进行上报，管理员在管理中心的终端上报弹窗中查看到终端上报的弹窗捕获信息。

右键天擎托盘，进入弹窗防护主界面，点击捕获弹窗。

拦截后，捕获弹窗信息将添加到自定义弹窗列表中，如图：

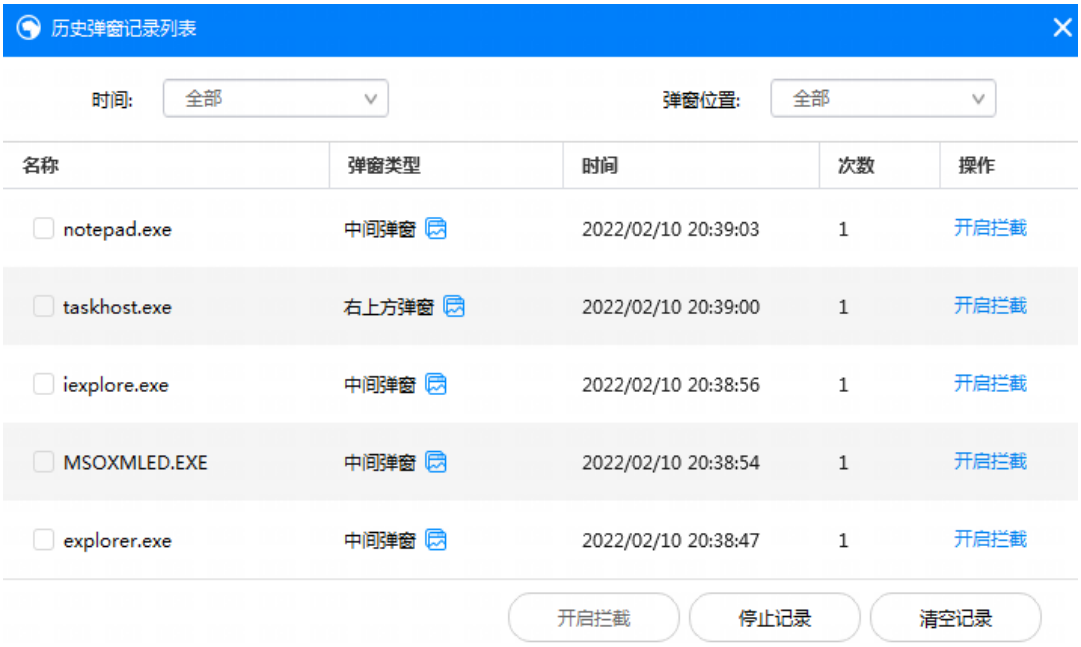
注：对于已添加的弹窗信息，支持查看和取消拦截。

21.2.6. 历史弹窗记录

入口：右键托盘>弹窗防护 或 客户端主界面>弹窗防护。

部分第三方软件广告弹窗停留时间较短，用户点击捕获弹窗去拦截时，弹窗消失。为避免此类弹窗未被及时捕获拦截，增加历史弹窗记录能力。

终端用户通过点击“开始记录”，自主启动历史弹窗的记录。



注：1）支持停止记录以及记录的清空；

2）支持历史弹窗图片的查看；

3）点击“开启拦截“后，弹窗被添加到自定义弹窗列表中。

21.3. 弹窗规则库更新设置

21.3.1. 系统更新设置

入口：系统管理>更新管理>安全小助手。

该模块设置弹窗防护规则库的更新时间，支持按月、周、天、小时周期性自动更新。

21.3.2. 终端更新设置

入口：系统管理>更新管理>安全小助手。

该模块设置全网终端更新弹窗防护规则库的时间，即弹窗规则库更新的灰度批次。

21.4. 典型场景

21.4.1. 如何处理软件弹窗未拦截的情况

软件弹窗规则库需要由奇安信运营团队持续运营，当出现弹窗规则库以外未知软件的弹窗时，管理员可通过自定义添加规则或终端用户上报规则对未知软件的弹窗进行拦截。

21.4.2. 如何更新弹窗防护规则库

- 管理中心可以连接互联网的用户场景，建议设置自动从奇安信云端更新弹窗防护规则库，可降低管理员的运维工作量，同时保证弹窗拦截效果最优。
- 管理中心不能访问互联网（纯隔离网）的用户场景，不能下载弹窗防护规则库，需使用离线升级工具定期导入弹窗防护规则库到控制中心。

21.4.3. 如何处理弹窗误拦截的情况

软件弹窗规则由云规则以及本地规则组合进行拦截，当出现规则添加错误导致终端部分软件弹窗被误拦截时，管理员可以通过自定义添加弹窗例外规则，进行误拦窗口的紧急加白。

22. 系统设置

22.1. 通用设置

通用设置：主要是用于联网状态、管理中心语言设置、资产登记定义、通知/外发服务、第三方联动设置、接入点设置、系统个性化设置等。

1) 通用设置：

a) 系统名称：支持自定义管理系统的名称，通常用于级联部署时区分多个管理系统。

b) 联网状态：是对管理中心是否允许联网的描述，可根据管理需求设置对应状态。决定了互联网资源文件的下载模式，如果是互联网模式则仅缓存文件、会按照一定机制清理缓存；如果是隔离网模式则需要使用离线工具导入文件，并且可以查看补丁文件是否已导入。

c) 管理中心的通信地址

管理中心支持配置多个通信地址，为了终端提供通信连接服务。例如，服务器采用单机部署，需要同时管理内网和外网的终端，如果服务器部署在内网，则需要额外再配置一个外网终端可以访问的通信地址。

d) 终端部署页面访问方式可以设定终端用户在线部署客户端时使用 http 或是 https。如果是 https 需要终端先安装证书才能访问下载页面。

e) 管理中心语言设置可以限制支持的语言类型，设定后会影响登录页的语言选择。

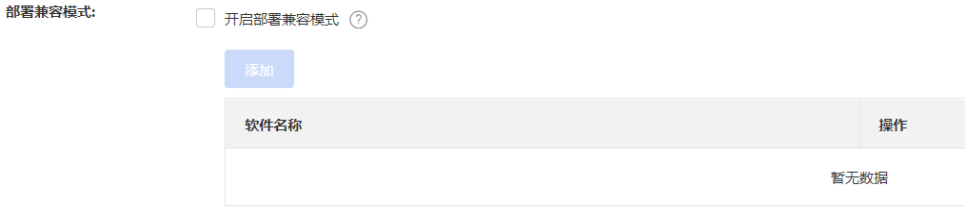
f) 文件限速。从管理中心下载文件，支持按照时间、终端 IP 地址网段、最大连接数限制下载/上传速度。最大下载/上传速度为所有连接数总和速度。

【注意】文件限速是为了方便管理员降低集中请求和文件下载对网络负载的影响，该功能设置会影响客户端部署、升级功能，建议该功能参数结合网络带宽负载情况逐步进行降低，以确保达到预期效果。

g) 互联网文件下载源：互联网文件指从互联网可以下载的文件，例如病毒库文件、主程序文件等。

h) 网络代理：管理系统通过代理访问互联网资源，例如云查杀、下载病毒库。

i） 部署兼容模式：用于部署客户端初期过渡，在未卸载指定软件时暂时不生效安全管理策略，以减少冲突。



j） 用户改善计划是为了持续改善奇安信天擎产品，会收集服务器的运行异常信息并反馈给奇安信集团官网。反馈信息严格遵守《奇安信用户体验改进计划》，绝不涉及用户任何隐私。此处可以选择是否参加改善计划。

2） 接入点设置：支持缓存文件、下载文件限速、预缓存文件、日志上传限速、选择终端上传文件存储位置，通过合理的配置可以有效保障企业工作所需资源并且可以提高企业网络带宽利用率。

支持通过最近的接入点获取互联网更新主程序、下载补丁文件等互联网资源文件，不用到上级下载互联网资源文件。同时支持配置网络代理。

特别说明：

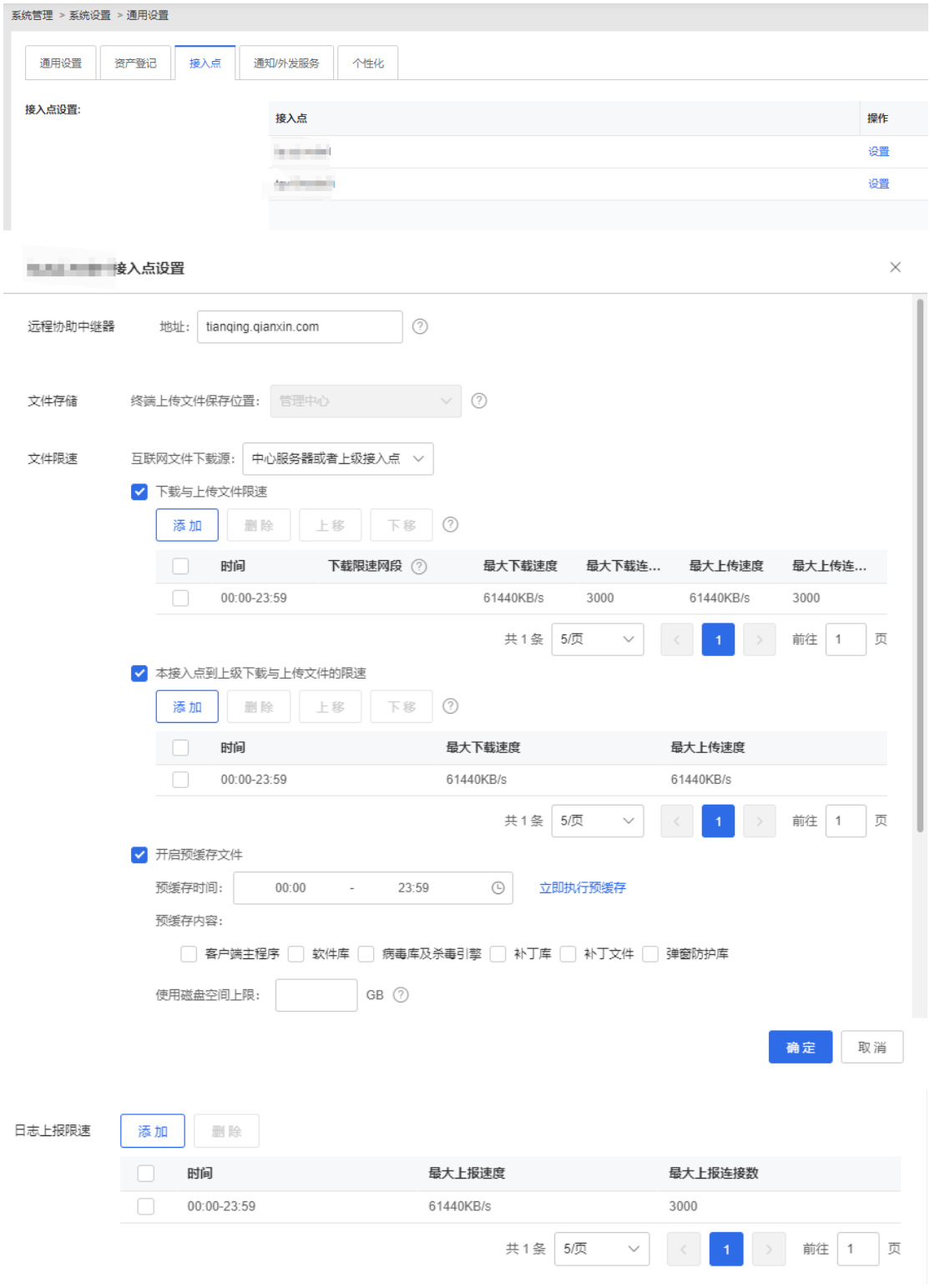
1、终端上传文件存储位置选择接入点时，需确保接入点与管理中心网络联通正常。接入点对管理中心只能单向通信时，此功能无法使用。

2、终端上传文件支持终端审计、数据防泄漏（DLP）、终端威胁检测与响应（EDR）三项业务。

3、接入点版本过低时，终端上传文件无法存储在接入点。

4、接入点预缓存开启后，不会缓存控制台上已经存在的内容。例如在开启预缓存配置之前，已经导入了 200G 的补丁文件，又在开启预缓存后再次导入了 300G 的补丁，此时接入点上只会缓存开启预缓存功能后的 300G 补丁；对于没有缓存到的 200G 补丁文件，当终端有请求到此内的数据，如 KB12345 这个补丁，接入点会检查发现自己没有 KB12345，此时接入点会代

理请求到控制中心，由控制中心返回给接入点，同时接入点对此补丁进行缓存，当其他的终端再次请求 KB12345 的时候，接入点就可以直接返回。

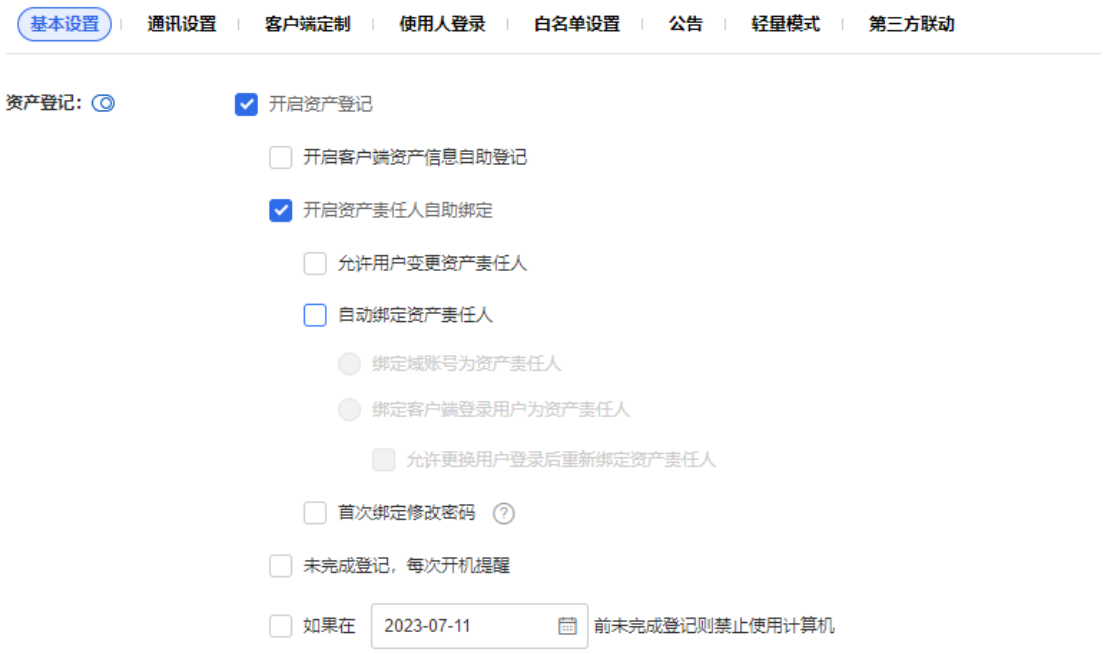


3) 资产登记：终端资产上报时展示的属性，便于企业识别和管理网内资产，支持自定义登记类别、必填项、输入类型，以及支持对已有的登记类别进

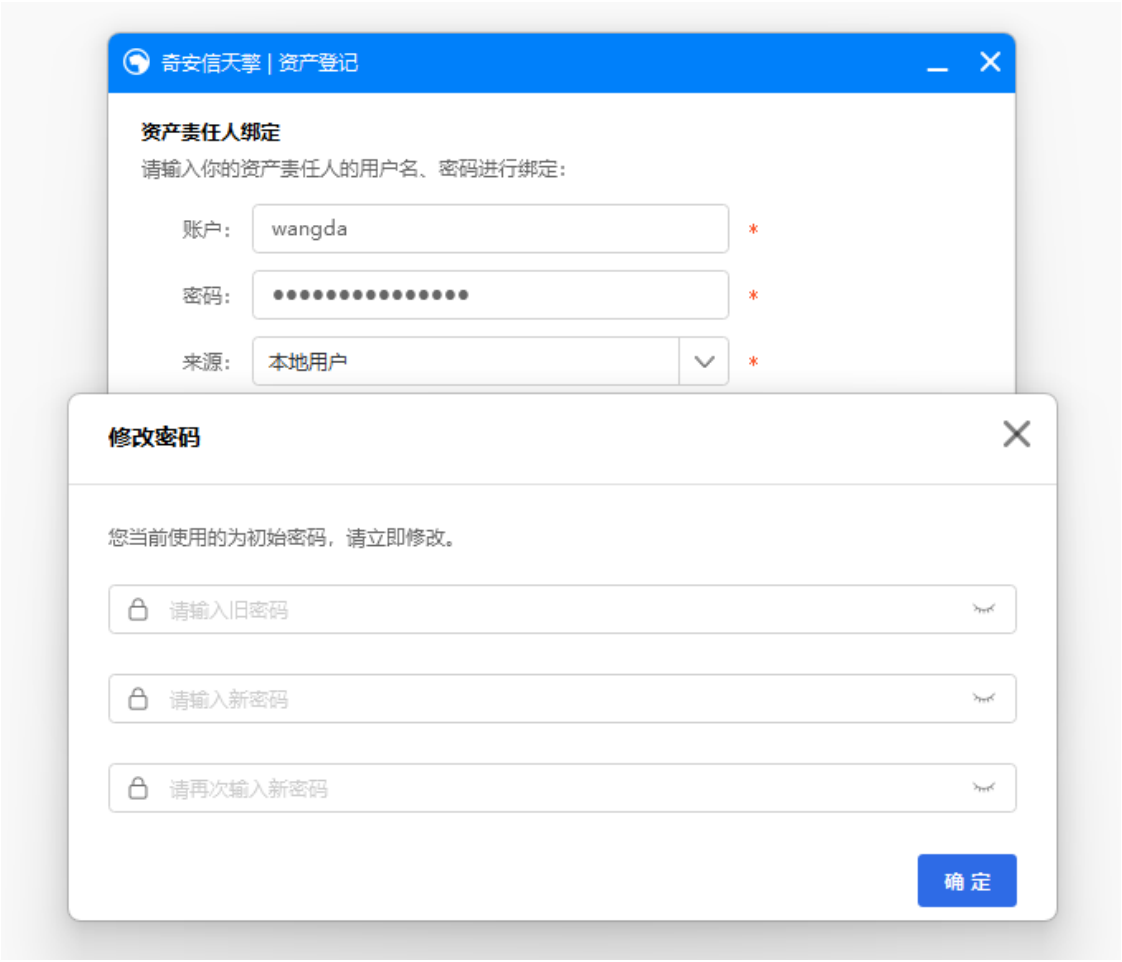
行编辑、删除和顺序调整；并且支持终端用户自助登记终端分组。支持客户端绑定资产责任人。

前置条件：添加资产类别。

支持首次绑定修改密码功能，入口：资产管理>终端管理>基础策略>资产登记


基本设置
通讯设置
客户端定制
使用人登录
白名单设置
公告
轻量模式
第三方联动
资产登记:
开启资产登记
开启客户端资产信息自助登记
开启资产责任人自助绑定
允许用户变更资产责任人
自动绑定资产责任人
绑定域账号为资产责任人
绑定客户端登录用户为资产责任人
允许更换用户登录后重新绑定资产责任人
首次绑定修改密码
未完成登记，每次开机提醒
如果在
2023-07-11
前未完成登记则禁止使用计算机

终端效果：



支持客户端首次登录强制修改密码功能，入口：终端管理>基础策略>用户登录

4） 通知/外发服务

a) SMTP 服务器设置模块用于设置管理中心相关事件的发件人邮箱，如果有相关业务订阅并设定了收件人，当事件触发后会向设置的收件人邮箱中发送相关邮件，以尽早通知相关管理人员进行查阅或处理；选择或输入邮箱的发件人邮箱地址、SMTP 服务器地址和端口、连接安全类型、验证方式、用户名和密码即可，发送测试邮件可验证联通性。

b) 短信网关设置模块用于设置管理中心下相关事件的发送平台，如果相关业务使用了短信通知功能，当事件触发后会向对应手机发送短信，以尽早通知相关人员进行查阅或处理；选择或输入短信平台类型、AccessKey ID、Region ID、AccessKey Secret、模板 CODE、签名、模板变量内容，然后输入手机号即可测试。

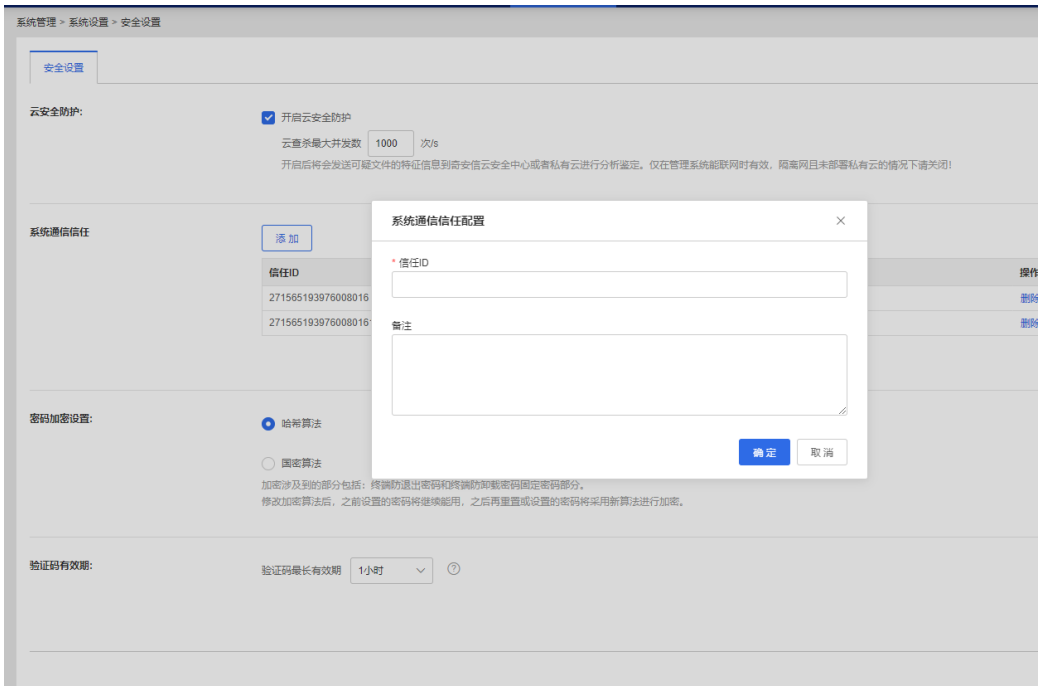
c) SYSLOG 服务器设置用于需要使用 syslog 的方式外发告警信息的场景下使用，完成告警服务器地址配置后，当事件触发后会向对应的服务器推送一条告警信息；发送协议支持 TCP 和 UDP2 种方式。

5） 个性化：个性化定制管理中心显示的产品名称和 Logo。

22.2. 安全设置

安全设置：云安全防护开关和并发云查数量限制、系统通信信任、密码加密设置、验证码有效期设置。

示例：系统通信信任在客户名称不一致的级联场景下使用，验证码有效期设置在客户端防退出等场景下使用。



在许可证管理中可查询客户的信任 ID。

22.3. 日志清理

清理管理中心存储的历史数据，节省磁盘空间，数据被删除后将不可恢复；可以根据需要勾选要清理的日志类型，并可设置日志保留天数和清理的时间段。

注：被清理的历史数据包括业务日志以及与日志相关的业务备份文件。

示例：添加病毒防护后，会定时清理病毒防护-病毒日志中的内容。

22.4. 数据外发

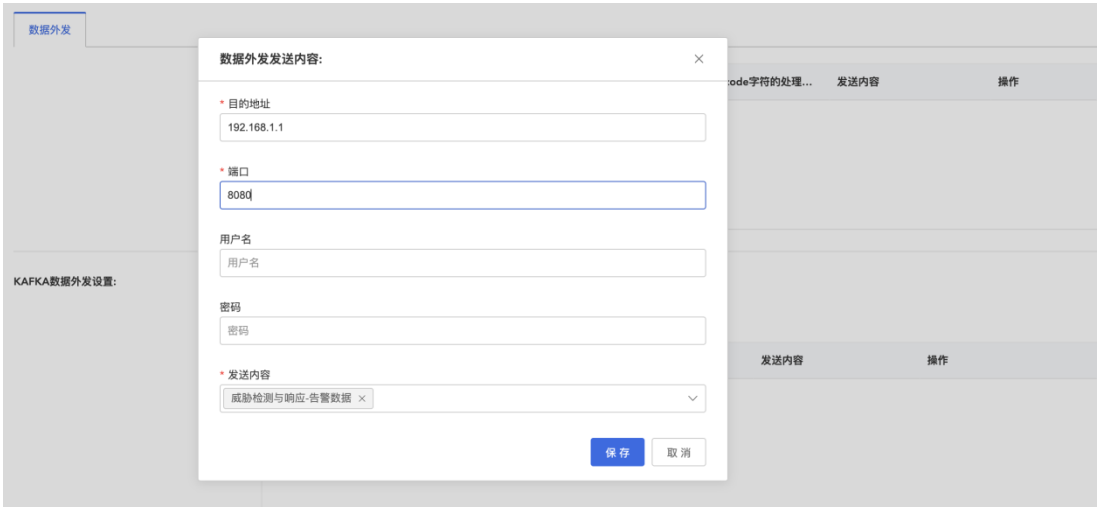
数据外发支持 syslog 数据外发和 kafka 数据外发。

1) Syslog 数据外发为 Soc 等第三方平台提供数据进行分析，支持同时向多个服务器发送数据。开启后，需填写目的地址、端口、发送协议、字符处

理方式以及发送内容；发送内容支持病毒防护、防火墙、补丁管理、终端管控等等，有对应业务许可时方可展示和选择。

- 当发送内容选择“终端概况”时，显示“终端概况发送频率”选择项，发送频率选项包含：1 小时/3 小时/6 小时/12 小时/24 小时。

2) Kafka 数据外发支持将终端采集到的终端行为数据，通过 Kafka 发送给第三方大数据分析平台。开启后，需填写目的地址、端口、用户名、密码以及发送内容；发送内容支持威胁检测与响应-告警数据，有对应业务许可时方可展示和选择。



23. 强制合规

23.1. 基本概念

奇安信天擎提供终端层面完整的一体化安全解决方案，但奇安信天擎的安装如果仅依赖管理手段或依赖人员自觉将无法有效提升网络整体安全水平。此时搭配“奇安信网神网络安全准入系统”强制入网终端进行身份认证，安装奇安信天擎客户端并强制终端进行基线合规检测，将有效提升全网终端奇安信天擎安装率、终端实名率及终端合规水平。

强制合规模块包括准入客户端及准入控制器两部分，准入控制器的提供资产识别、身份认证、终端推送等常用功能，需配套“奇安信网神网络安全准入系统”NAC-V 系列引擎使用，具体部署及使用可查看“奇安信网神网络安全准入系统管理员”手册。

奇安信天擎终端安全管理系统提供准强制合规的 Windows 和信创客户端模块，提供“准入认证客户端”及“安检合规”两个功能模块，用来支持 Windows 和信创终端的准入身份认证及终端合规需求。

23.2. 基本功能

23.2.1. nac 联动

23.2.1.1. 网络水印打点

在 NAT 网络下安装了天擎客户端的设备可以向准入系统服务器进行打点，即在网络通信数据包中加上含有准入系统可以识别的特殊标记，用于准入系统对其进行放行使用。

启用“开启 NAC 联动功能”，可以进行网络水印打点功能的配置。

下面是对于配置项的说明：

配置项	说明
心跳协议版本	选择用于打点的心跳协议版本。 注：v1.0 快但不安全，v2.0 兼具快速与安全性。
心跳间隔	天擎客户端向准入系统服务器进行打点的间隔，用于维持打点会话。
NAC 地址/端口	天擎客户端打点的目标准入服务器地址和端口。 注：默认情况下，心跳协议版本 v1.0 对应准入服务器端口为 80，v2.0 对应端口为 443。如果准入控制器注册时使用的端口发生了变更，这里填写的端口应为注册时的端口。

23.2.1.2. 网络水印例外

对网络水印进行自定义与例外。

下面是对于配置项的说明：

配置项	说明
IP 白名单	向 IP 白名单内的地址访问时，不会加上网络水印值。 有部分软件系统，可能会因为自定义网络水印引起崩溃。

23.2.2. 准入认证客户端

授权启用“强制合规>准入认证客户端”模块后，终端将自动安装准入认证客户端，准入认证客户端支持通过有线/无线 802.1X 协议或 HTTP 协议向网络安全准入设备（NAC-V）发起入网身份认证，支持用户密码方式、证书方式、Ukey 方式、超级 SIM 方式或双因素方式（用户密码+证书）验证终端使用人身份或终端身份。身份认证成功后，准入设备将允许合法终端接入网络。

23.2.2.1. 认证类型与方式

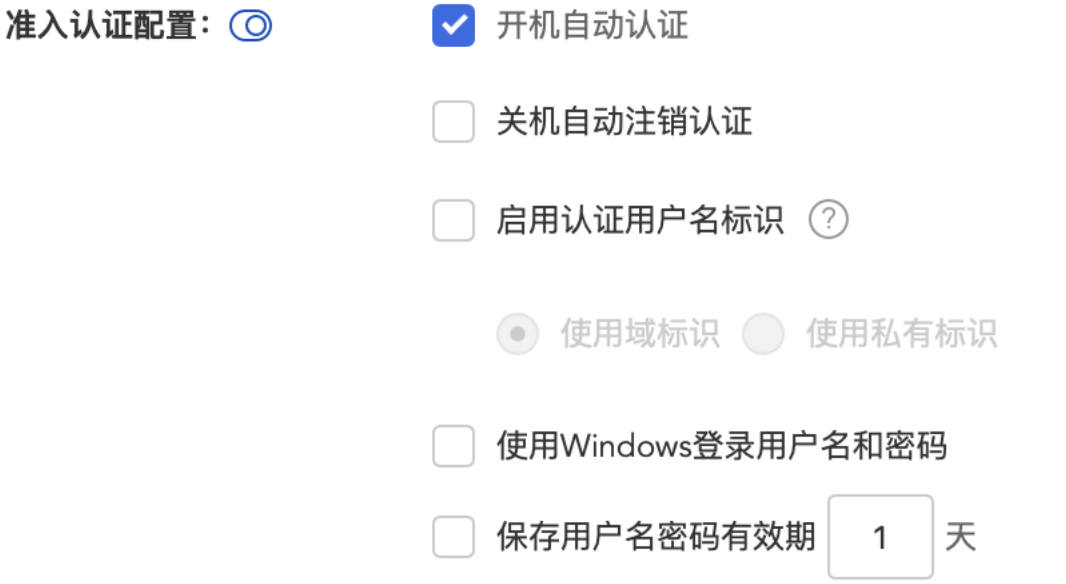
自定义客户端上的认证类型和认证方式。

下面是对于配置项的说明：

配置项	**说明**
默认认证方式	客户端默认采用的认证方式。 注：选择的项必须在“客户端可选认证方式”处勾选同名项。
客户端可选认证方式	可供用户在客户端自定义选择的认证方式类型。

23.2.2.2. 准入认证配置

自定义认证相关的一些配置。



下面是对于配置项的说明：

配置项	说明
开机自动认证	操作系统开机时，客户端自动自行认证。
关机自动注销认证	关闭操作系统时，触发客户端注销当前认证会话。
启用认证用户名标识	认证时，自动在用户名后面加上标识。可采用域标识或自定义标识。
使用 Windows 登录用户名和密码	使用用户名密码登录 Windows 操作系统后，客户端将登录时使用的用户名密码用于准入认证。
保存用户名密码有效期	客户端允许保存密码的有效期。 超过有效期后，会取消勾选【保存密码】。

23.2.2.3. 执行动作配置

自定义认证时与认证后执行的动作。

下面是对于配置项的说明：

配置项	说明
认证联动安检	认证时会触发安全检查。
认证成功后执行更新 IP 动作	认证成功后，重新获取当前终端的 IP 地址。
注销联动安检	客户端注销认证时触发安全检查。
认证成功后，客户端启用网络水印	认证成功后，客户端启用网络水印功能。 网络水印概念参考本文档【强制合规/基本功能/nac 联动/网络水印打点】。
认证成功后，同步登录天擎	认证成功后，使用准入认证的用户身份自动单点登录天擎客户端。
认证成功后，打开 url	认证成功后，打开管理员指定的网址。

23.2.2.4. 无线认证选项

自定义无线认证配置项。

23.2.2.5. 显示选项

自定义客户端界面显示的项。

下面是对于配置项的说明：

配置项	说明
全静默运行	不显示客户端界面、托盘、桌面图标，准入客户端对于用户是无感知的。 注：选择全静默运行时，其他的显示选项不会生效。
认证成功最小化	认证成功后，认证界面窗口最小化。
启动时最小化	启动操作系统后，认证界面不显示。 注：常与开机自动认证配合使用，实现开机后台自动认证。
显示记住密码	显示认证界面的“记住密码”开关。
显示自动登录	显示认证界面的“自动登录”开关。
显示修改密码	显示托盘右键的“修改密码”菜单。 注：一些版本的信创客户端显示
显示认证客户端托盘	显示客户端的托盘。

23.2.2.6. 高级配置

自定义断网提示时间和是否恢复网络自动认证。

23.2.2.7. 其他配置

自定义证书认证采用的证书服务器地址与协议。

23.2.3. 安检合规

奇安信天擎合规检查策略会检测终端入网安全状态，能快速定位发现入网计算机终端的安全合规情况，并通过与“奇安信网神网络安全准入系统”联动将未合规终端进行网络隔离，只能够访问自定义的隔离修复区或修复服务器，同时依照策略进行引导式修复或一键修复。对于已确认合规终端，也可调用周期监测或定时监测引擎，对该终端的安全状态进行多次评估，如发现运行阶段又不符合安全检查策略，进行再次隔离或提示，这种具有安全隐患的终端禁止其访问企业核心资源，保证入网终端的安全基线是标准的、可控制的，可修复的，并提供一系列入网安全状况统计和终端合规性详情等报告。

23.2.3.1. 检查设置

对准入客户端安检和通知的时机进行配置。安检合规检查项与基线合规检查策略一致，支持系统配置安全检查设置、系统状态安全检查设置、系统运行安全检查设置三个大项下面的几十项内容进行配置并未这些安检项配置自定义提示内容，同时支持引用基线模板进行入网安全检查，方便管理员对部门安全基线进行统一运维。

下面是对于配置项的说明：

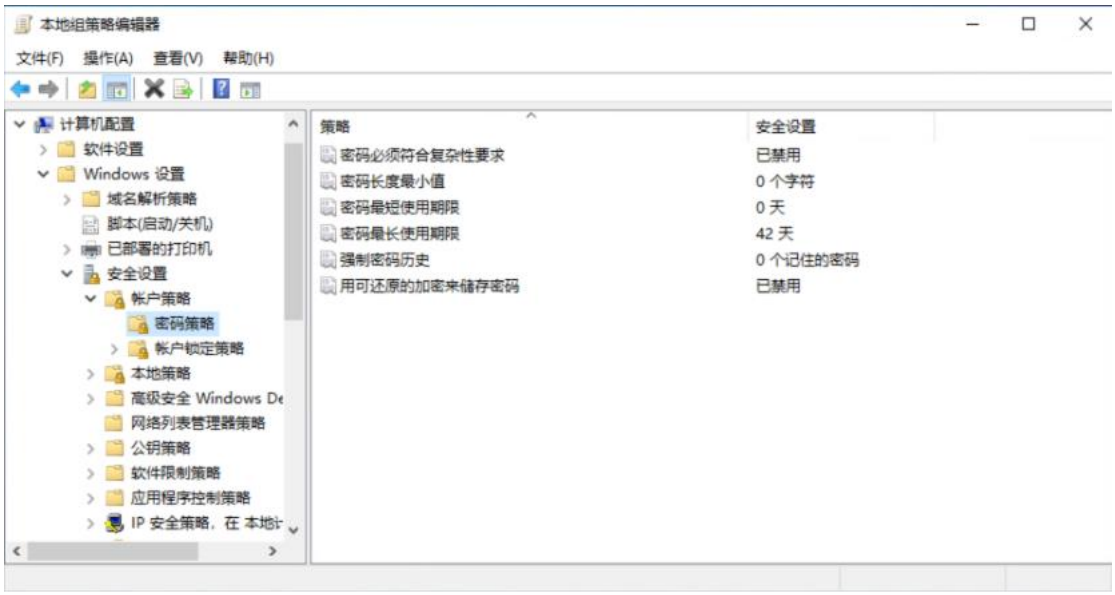
配置项	说明
开机默认阻断	打开操作系统后安检结果默认阻断。仅在执行安检并通过后解除阻断状态。

打开安检界面后自动执行安检	用户打开客户端安检界面后会立刻自动执行安检。
启动客户端后开始检查	打开准入客户端后开始执行安检，支持自定义延迟时间。
周期检查	每隔一段时间执行安检，周期单位可以设置为分、小时、天、周或者月。
通知模式	安检结果通知用户的方式，可设置为一律弹窗显示、仅安检不通过时显示或者一律不显示。
检查标准	设置安检不通过的标准，可设置为否决项不通过或分数低于指定值时安检不通过。 注：否决项代表关键的安检项。
检查不通过处置动作	设置安检不通过时的处置动作，包含告警、断开网络、注销认证。 注：微隔离会限制安检不通过的终端仅可以访问有限的网络资源。

23.2.3.2. 系统配置安全

系统配置的安全检查规则自定义。

这些安检项对应 Windows 组策略中的配置，组策略配置与安检规则不一致时，安检不通过。



23.2.3.3. 系统状态安全

系统状态的安全检查规则自定义。

下面是对于安检项的说明：

安检项	说明
补丁检查	检查是否存在指定安全级别或补丁号的补丁。

防病毒检查	检查是否安装了指定名称的防病毒软件，同时检查病毒库的更新时间是否在指定时间内。
杀毒软件保护检查	检查是否启用了杀毒软件保护。
工作组命名检查	检查是否加入了指定名称的工作组。
域检查	检查是否加入或登录指定名称的 AD 域。
计算机命名检查	检查计算机名是否符合制定的名称规范。
系统备份还原点检查	检查是否存在系统备份。
账户权限检查	检查当前登录操作系统的用户是否属于指定名称的用户组。
系统中重要目录对 Everyone 或 Guests 来宾账户开放检查	检查系统中的重要目录是否对 Everyone 或者 Guests 账户开放访问权限。
空口令检查	检查当前登录账户的密码是否为空。
操作系统是否开启 Hardware DEP Available 保护检查	检查是否启用了 Hardware DEP Available。
系统隐藏用户检查	检查操作系统中是否存在隐藏用户。

23.2.3.4. 系统运行安全

系统运行时的安全检查规则自定义。

下面是对于安检项的说明：

安检项	说明
进程检查	检查是否存在指定名称的进程，
端口检查	检查是否存在禁止启动的指定的端口号。
软件检查	检查是否存在指定名称的软件。

23.2.4. 准入概况与设备合规

安检合规的结果可以在安检合规概况和安检合规日志中查看。安检合规概况以终端分组视图可以查看到计算机的合规情况，包含：安检得分、不合规项、检查结果、最近一次检查时间、合规项。

安检合规日志可以将时间和安检行为进行关联展示。支持展示最近 1 天、最近 7 天、上周以及自定义时间的终端安检情况。也支持筛选某个分组、某个计算机来进行安检操作的审核。安检合规日志支持导出。

23.2.5. 天擎与准入同台

终端管理在天擎控制台上操作，入网管理在准入控制台上操作。如果用户对这两个功能都有需求的情况下，切换两个控制台不方便。为此，同台功能可以实现将准入控制台所具备的功能内置在天擎控制台上进行展示的功能。

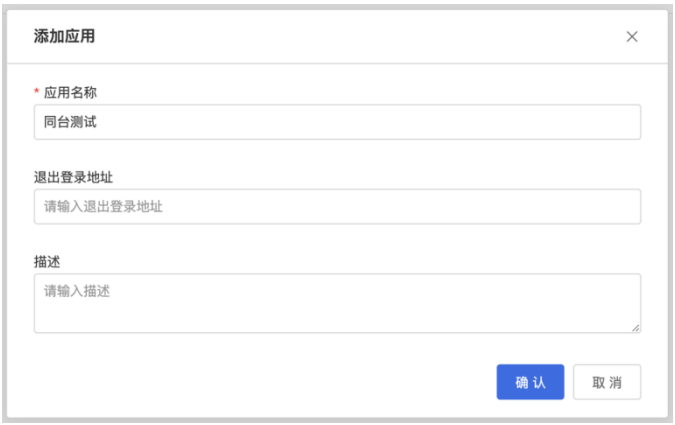
注：同台功能需要准入控制台版本在 8.6.0.3100 以上。

下面是配置步骤：

- **新建应用**

入口：用户管理>应用

添加一个新的应用，填上名称。



创建完成后，查看刚刚新建的应用详情。将应用凭证里的 AppKey 和 AppSecret 提前复制好。

- **开启联动**

入口：系统管理>强制合规>NAC 设置

填上对端准入控制台的地址，格式如下图所示，点击[连接]按钮。

在弹窗准入联动中输入准入控制台的管理员账号密码。

同步 appkey 与 secret 来源于刚刚创建的应用（【用户中心-应用】下点击创建的应用，如上文所说）。grpc 网关端口在天擎单机版默认 36781，集群版默认 30081。tcp 网关端口天擎单机版默认 6785，集群版默认 30080。点击“激活”完成同台的初始配置。

配置完成后，可以在天擎的网络准入菜单下查看到准入控制台的页面而无需再输入准入控制台的管理员账号密码。

24. 多级级联

24.1. 基本概念

24.1.1. 级联部署

级联部署即将多个独立的奇安信天擎终端安全管理系统按照上下级关系连接起来，用于拥有需要独立安全运营的分支机构的政企单位，以实现独立运维和统一安全管理。

24.1.2. 级联策略

管理系统级联部署下的策略管理，支持分发强制策略强制管理下级终端，也支持分发普通策略作为安全兜底，分支机构可根据自身情况调整安全策略。同时支持终端策略和用户策略。

24.1.3. 级联报表

管理系统级联部署下的日志报表管理，汇总下级管理系统的终端日志和统一报表分发，为管理员提供全网的终端安全状态数据。

24.1.4. 级联更新管理

管理系统级联部署下的更新管理，支持全网所有管理系统统一灰度更新，也支持下级管理系统各自从互联网更新。

24.2. 基本功能

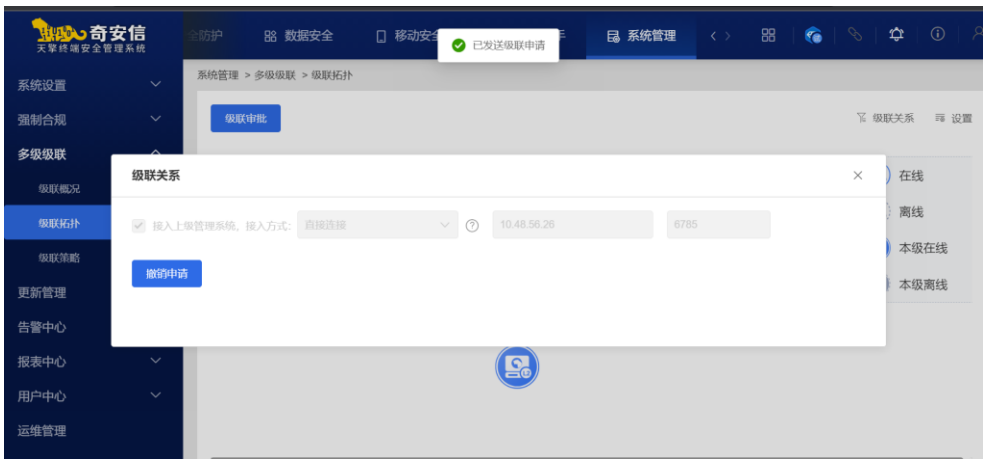
24.2.1. 级联关系

支持5级级联部署，支持单机和集群部署混合级联，如果终端数量较多，通常一级采用集群部署服务器，下级采用单机部署。

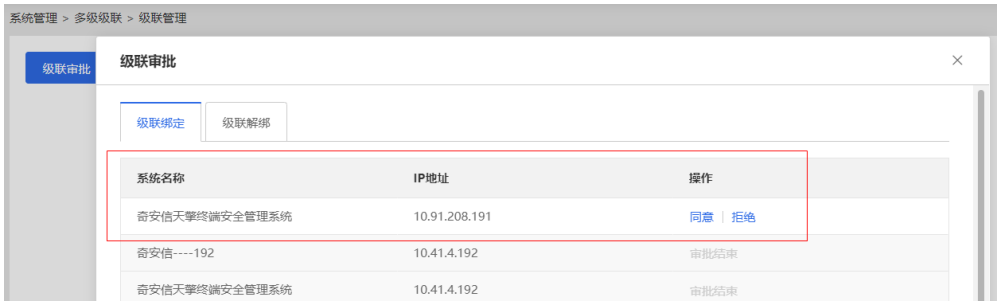
建立级联：

1) 独立部署各个管理系统。

2) 登录作为下级的管理中心，导航到“系统管理>多级级联>级联拓扑”，填写上级管理系统的地址和端口（Windows单机部署的默认端口是6785，Linux/ARM单机部署和集群部署的默认端口是30080），申请级联，并联系上级管理员审批。



3) 上级管理员导航到“系统管理>多级级联>级联拓扑”中，同意接入级联，建立级联关系。



4） 完成级联关系建立，上级管理员查看和管理下级管理系统。

解绑级联关系：

1） 登录下级管理系统的管理中心，导航到级联管理，在“级联关系”设置中发起“解绑”。并联系上级管理系统的管理员审批。

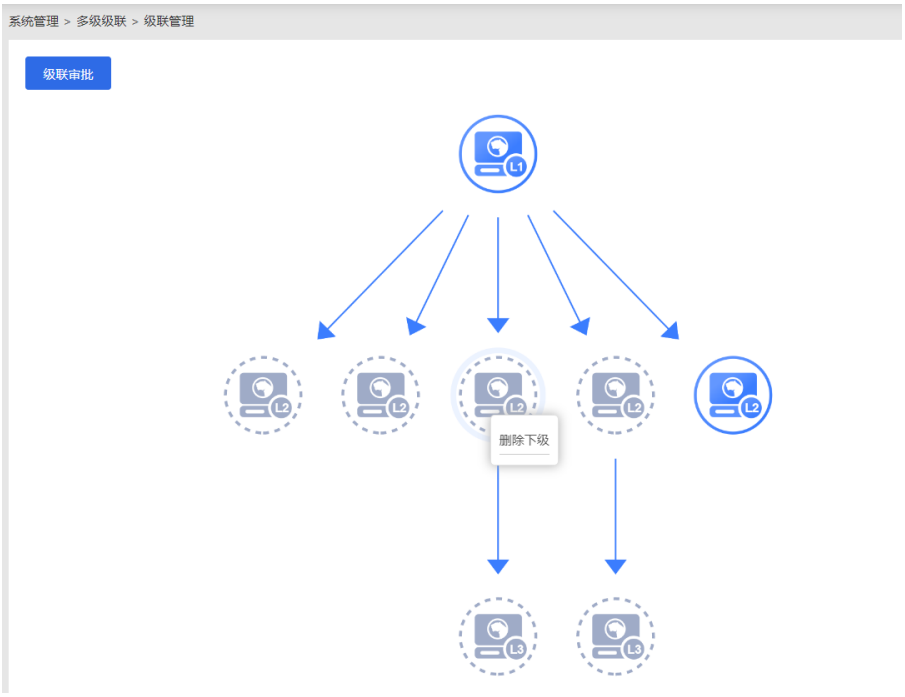
2） 上级管理系统的管理员同意解绑则可以完成解除级联关系。

重置级联关系：

在上级管理系统异常损坏等情况而不能正常的解绑的情况下，“重置”功能强制解除级联关系。重置功能仅在上级管理系统损坏时可用。

删除下级管理系统：

在下级管理系统异常损坏等情况而不能正常的解绑的情况下，上级管理系统的管理员可直接在级联拓扑中删除下级系统，如果下级系统只是临时掉线，恢复在线后级联关系会自动恢复。删除功能仅在下级管理系统离线时可用。



24.2.2. 级联策略

功能入口：系统管理>多级级联>级联策略。

1) 级联策略支持分发终端策略和用户策略。

2) 级联策略支持停止/开启。

3) 级联策略仅作用于下级系统，不影响本级的终端/用户。当级联关系解除后，下级系统接收到的级联策略自动失效，并且自动删除策略。

4) 级联策略支持强制策略和普通策略。

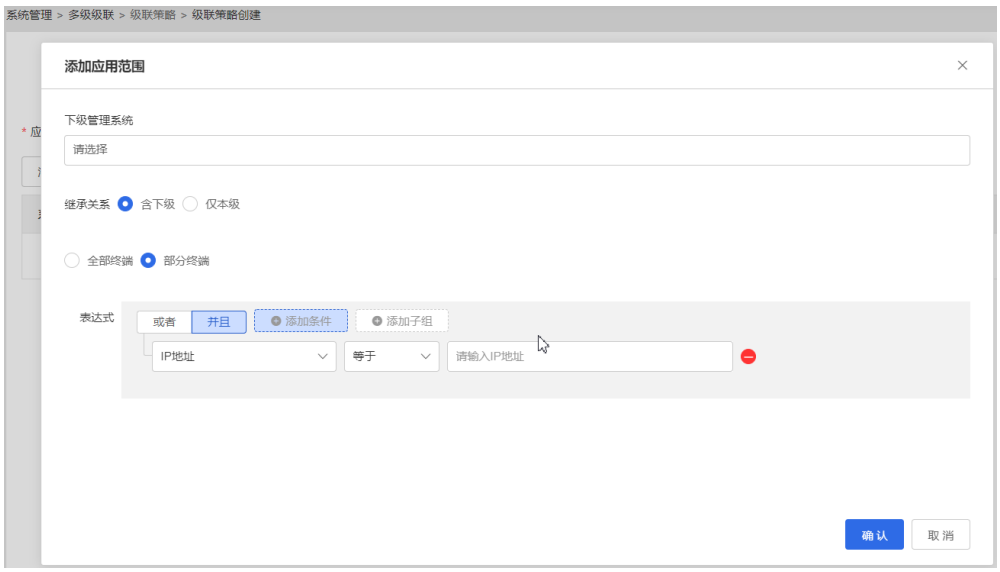
   a) 级联强制策略的优先级高于下级系统的所有策略。

   b) 级联普通策略的优先级低于下级系统的所有策略。

5) 级联策略支持分发给指定的下级系统并且包含子孙系统、指定的下级系统但不包含子孙系统。

6) 级联策略支持分发给下级系统的部分终端/用户，可通过“表达式”或者分组描述部分终端/用户。

7) 级联策略配置方法与本级策略一致。



【注意】策略批量下发下级控制台时，建议优先选择1个控制台应用策略并密切关注策略生效效果，确认符合预期后再扩展策略应用范围到更多控制台。

【注意】由于不同控制台部署地址不同，如策略项中涉及到地址相关内容时，需确定具体配置项内容与策略下发范围匹配。

24.2.3. 级联报表

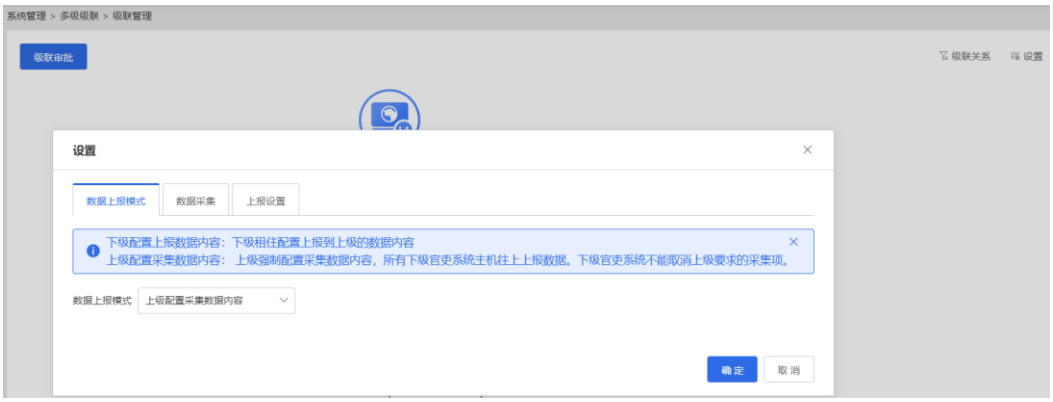
管理系统级联部署下的日志报表管理，汇总下级管理系统的终端日志和统一报表分发，为管理员提供全网的终端安全状态数据。

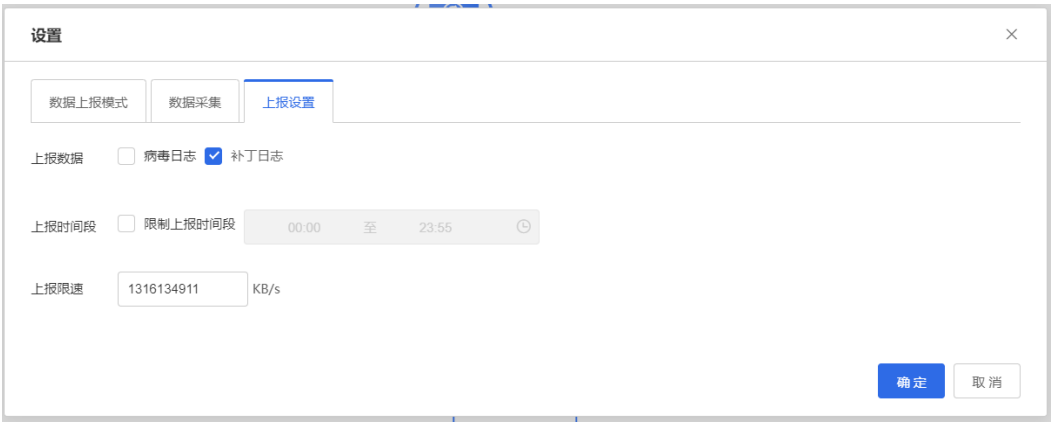
1) 一级系统的管理员导航到“系统管理>多级级联>级联拓扑”，配置级联日志报表的上报模式，可配置为“由上级配置采集数据内容或下级配置上报数据内容”。

2) 如果是上级配置采集数据内容，则一级系统的管理员配置全网统一上报哪些日志内容。

3) 如果是下级配置上报数据内容，需要通知下级系统的管理员各自配置上报内容。并根据各个分支机构到上级的带宽情况配置上报时间段。

特别说明：本版本仅支持病毒日志和补丁日志及报表。



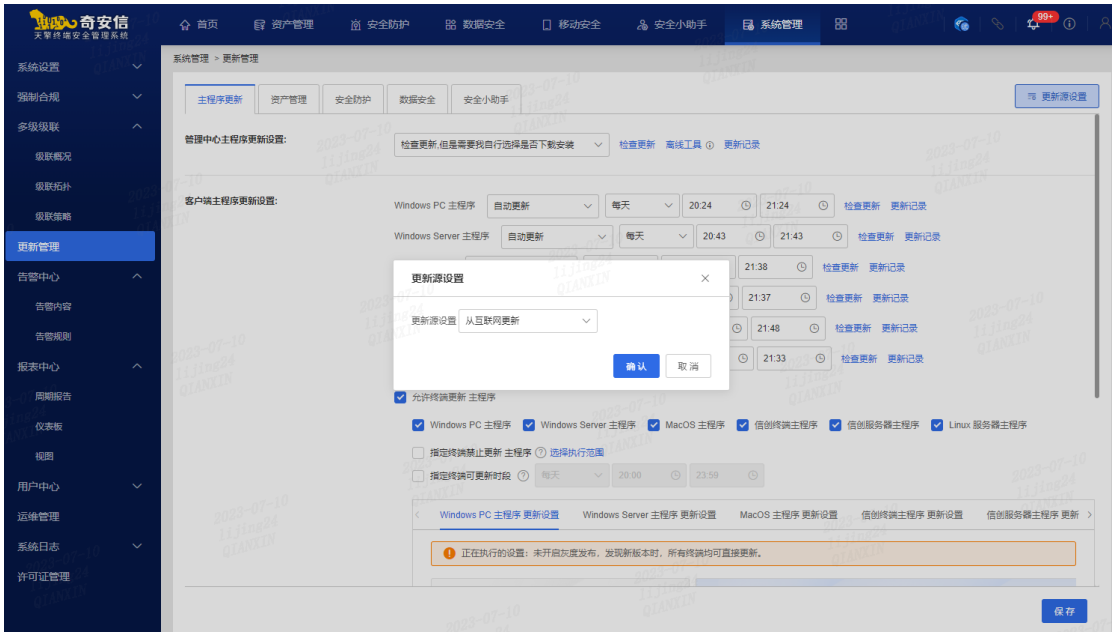


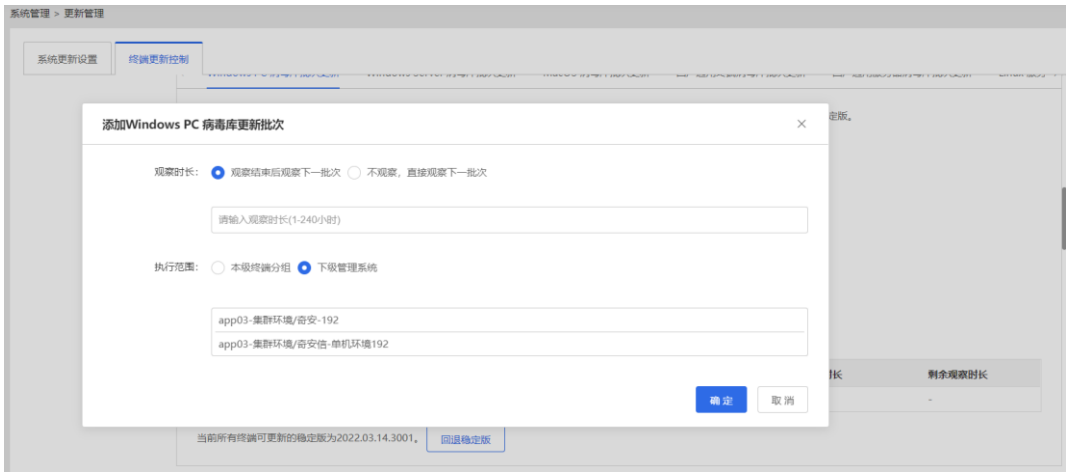
24.2.4. 级联更新管理

管理系统级联部署下的更新管理，支持全网所有管理系统统一灰度更新，也支持下级管理系统各自从互联网更新。

1) 下级管理系统配置更新源。

2) 上级管理系统配置灰度批次。

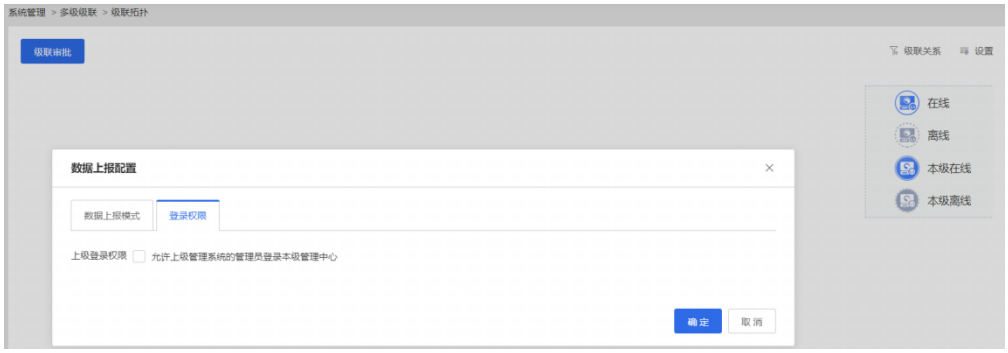




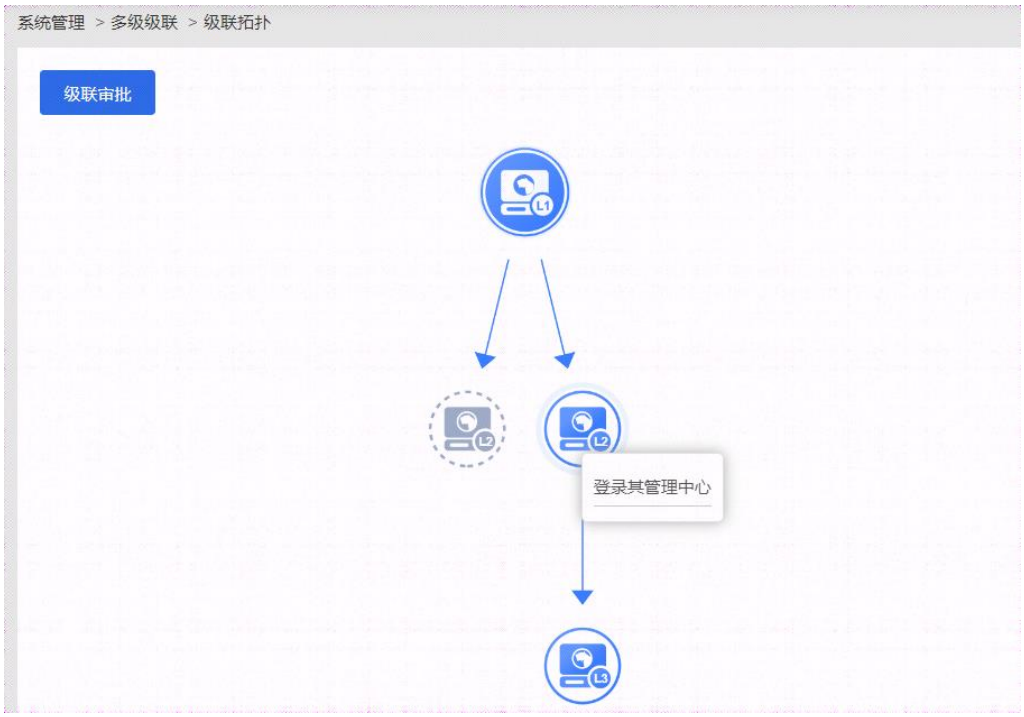
24.2.5. 登录下级管理中心

上级管理系统的管理员在下级系统授权后，可以免密登录到下级系统的管理中心管理终端、策略、任务等操作，但不支持查询下级系统的日志。

1) 下级管理系统管理员在级联设置中配置登录权限，允许上级管理系统的管理员登录本级管理中心。



2) 上级管理系统管理员导航到级联拓扑中，选择要登录的下级系统，点击其图标则发起登录。



25. 更新管理

25.1. 基本概念

25.1.1. 版本号

用于表示奇安信天擎管理中心版本，包括提供的安装包文件名中的字串和安装后在管理中心界面上展示的部分。

◆ 文件名部分：

QI-ANXINTianqing-server-[版本信息]_[系统平台 Windows/Linux]_[文件MD5]

✓ 版本信息中包含 VRP 或 Hotfix 两种格式：

V 指产品版本，整体架构和设计有较大调整，例如 V10.0。

R 指 Release 小版本，为维持产品的功能有效性或增强竞争力而做的功能新增或者改进的版本。

P 指 Patch 版本，为修复产品缺陷或小规模改进产品功能而定期发布的针对特定版本区间的更新包。

Hotfix 指 hotfix 版本，为修复特定的一个或多个关联性产品缺陷的专用性的更新包，针对特定的单个版本或版本区间发布。

✓ 系统平台，表示此交付包运行的平台

Windows:Windows 系统。

Linux:Linux 系统。

✓ 文件 MD5：

安装文件的 MD5 哈希，用于校验文件传输是否正确。

◆ 管理中心展示：

管理中心展示版本号的地方如下图所示，其中管理中心版本号展示分为两行。

产品版本，表示奇安信天擎终端安全管理系统产品版本号。

产品批次，标明了当前管理中心所属的 Release 版本和对应的 Patch 版本。

◆ 客户端展示

通过点击客户端任务栏图标右键菜单中的关于项，可以看到当前客户端的版本信息，其他平台客户端操作相同。

也可以打开客户端主界面点击左上角箭头图标可以在弹出框中查看 Build 版本号、病毒库等版本。

◆ 其他库的版本展示

对于购买的模块需要云端持续运营更新的会有对应的规则库，也会存在对应的版本用于查看、管理和更新；版本号根据业务不同有所区别，具体登录管理中心查看。

25.1.2. 在线更新

在线更新指已经部署的奇安信天擎终端安全管理系统通过互联网获取奇安信公司云端最新版本的更新操作。

此操作主要对应奇安信天擎终端安全管理系统管理中心上系统管理>更新管理菜单下服务器更新部分，具体操作可参考 25.2.1 章节。

25.1.3. 离线更新

离线更新是指利用离线工具从互联网下载更新数据然后同步到隔离网下的管理中心。具体操作可参考 25.2.2 章节。

25.1.4. P2P

P2P 是一种点对点的网络传输方式，P2P 下载是指终端下载文件的同时作为同网段内其它终端的下载源，以减少主干网的带宽占用。奇安信天擎为了减少企业带宽压力，提供了终端 P2P 下载文件功能。通过终端管理>基础策略>终端策略>通讯设置中开启。开启 P2P 功能，终端将会打开侦听端口 9522 和 9521。

25.1.5. 版本更新

版本更新是指同一产品版本不同批次之间的更新行为；更新版本包括有较大功能变更的放量版本（Release 版本）、Bugfix 的 Patch 迭代版本，以及定向修复的 Hotfix 版本。

25.1.6. 自动更新

自动更新包括奇安信天擎终端安全管理系统管理中心和终端两部分。

管理中心的自动更新需要连接互联网，有“从不检查更新”和“检查更新，但是需要我自行选择是否下载安装”两种选择。管理中心会根据设置定期到奇安信公司云端检查是否有可用的新版本。相关设置在系统管理>更新管理菜单下，具体操作可参考 2.2 章节：

终端的自动更新是指终端从管理中心根据设置主动定时获取新版本程序或病毒库等。相关设置在系统管理>更新管理菜单下，具体操作可参考 25.3 章节。

25.1.7. 手动更新

手动更新是指在未进行自动更新时，通过点击相关更新按钮主动触发更新的操作，同样包括奇安信天擎终端安全管理系统管理中心和终端两部分。

管理中心：通过点击系统管理>更新管理菜单下，各类型更新配置选项后方的“检查更新”或者管理中心右上角 对应版本或批次，具体操作参见 25.2.1 章节。

终端：通过点击界面左上角的白色箭头或者主界面右上角菜单下“更新检查”完成手动更新，具体操作参见 25.3.2 章节。

25.1.8. 定时更新

定时更新与自动更新相辅相成，当设置为自动更新时，需要设置具体的时间来自动触发检查更新的相关动作，具体操作参见 25.2.1 章节。

管理中心的默认设置为“检查更新，但是需要我自行选择是否下载安装”，此时系统会自动定时去云端检查更新，不支持设置定时时间。

其它相关程序及病毒库和补丁库等文件的更新，可以根据安全运营需要设置定时检查更新的时间。

25.1.9. 覆盖安装

覆盖安装是指使用同版本或高版本的奇安信天擎终端安全管理系统安装包在本地再次执行安装过程。

25.2. 管理系统更新

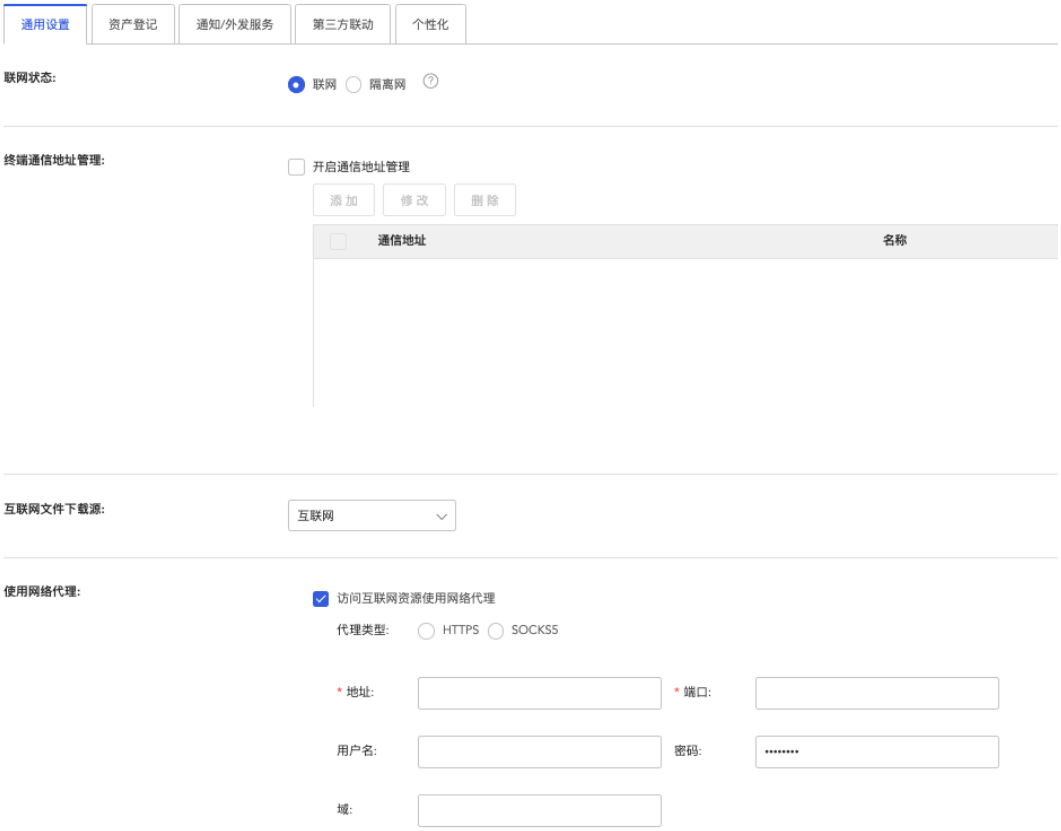
奇安信天擎终端安全管理系统支持对管理中心自身以及病毒库、补丁库等库信息和文件更新，更新方式分为在线更新、离线工具更新和覆盖安装更新三种。

25.2.1. 在线更新

在线更新是指在联网情况下的更新，支持手动检查更新、自动检查更新，同时也支持使用网络代理联网下载更新文件,并支持断点续传，也可以设置定时自动更新，具体操作步骤如下：

1) 打开奇安信天擎终端安全管理系统管理中心并登录，点击右上角信息按钮，查看并记录当前管理中心的版本。

2) 确保当前管理中心可以连接互联网。在系统设置-通用设置-通用设置处确认联网状态为“联网”。并且支持使用网络代理访问互联网更新资源，如下图：



3) 自动更新。自动更新时，则在系统管理>更新管理>主程序更新，分别配置“管理中心主程序更新设置”和“客户端主程序更新设置”。

4) 检查更新。可以在系统管理>更新管理>主程序更新，手动检查更新。

5) 下载更新。管理员手动检查更新时，当检查到有更新后，则可点击“下载更新”，会进行更新包的下载，并展示进度，也可以后台下载文件。

6) 更新并展示版本号。下载完成并更新，更新完毕后会更新管理中心版本，其他如主程序、病毒库等更新完成后同样展示更新的版本号。

7) 更新记录。可展示管理中心更新自身以及病毒库、补丁库等库信息和文件更新的记录。包括版本号、更新的时间、更新说明。

25.2.2. 离线工具更新

离线工具更新支持管理中心在无法连接互联网的情况下，使用“离线更新工具”将互联网数据更新至管理中心。具体操作步骤如下：

1) 打开奇安信天擎管理中心并登录，点击右上角信息按钮，查看并记录当前管理中心的版本。

2) 下载离线工具。打开奇安信天擎管理中心，进入系统管理>更新管理菜单，在“管理中心主程序更新设置”行尾点击 “离线工具”超链接下载。

3) 配置相关信息。双击运行离线工具，点击窗口左下方“配置”开始对管理中心地址、服务接入端口（Windows 单机部署默认：36781，Linux 集群部署默认：30081）、下载代理设置、补丁设置以及下载数据等进行配置，完成后点击保存。

4) 获取管理中心的信息。可以选择获取需要更新的信息，不需要的可手动取消勾选。

5) 从互联网下载更新数据。将离线工具及同步的管理中心数据拷贝至能连接互联网的环境，然后运行工具并点击“从互联网下载更新数据”，然后待检查完毕后选择需要下载的数据进行下载。

6) 将更新的数据同步至管理中心。将下载好的数据连同工具一并拷贝回能访问管理中心的设备并运行工具，更新时确认提示后即可更新数据。

25.2.3. 覆盖安装更新

覆盖安装更新是指使用符合覆盖安装升级条件的新版本安装包进行覆盖安装操作，以完成对管理中心自身的升级和相关库文件和信息的更新（根据安装包的发布时间不同，其携带的库文件和信息相比安装时间具有一定滞后性）。具体操作步骤如下：

1) 打开奇安信天擎终端安全管理系统管理中心并登录，点击右上角信息按钮，查看并记录当前管理中心的版本。

2) 比对安装包文件名中标识的版本号。根据安装包名称或者安装包属性查看要进行安装的包是否高于当前已安装版本，如果版本低于当前已安装版本则无法安装，具体需参考新版本的产品发布说明书中的支持覆盖安装说明。

3) 运行安装程序，对管理中心进行覆盖安装更新。

25.3. 终端更新

终端需要从管理中心获取主程序、病毒库等数据进行更新，完成终端功能及防护能力的提升，其主要特点：

1) 更新方式支持在线更新和离线更新，为了减小服务器压力也可以在策略中开启 P2P 下载功能；

2) 支持设置需要更新的终端类型或数据类型，并支持对终端的更新设置例外（即禁止指定终端更新）；

3) 支持指定终端更新的版本，并且支持对网内允许更新的终端分批次进行灰度更新和观察，对于存在问题的版本可以切换至其他版本；

4) 支持当检测到新版本时，在上一个版本观察结束后重新从第一批次开始观察，对于批次外的终端可以禁止自动更新。

本节主要介绍终端更新配置、在线手动更新和离线更新。

25.3.1. 终端更新配置

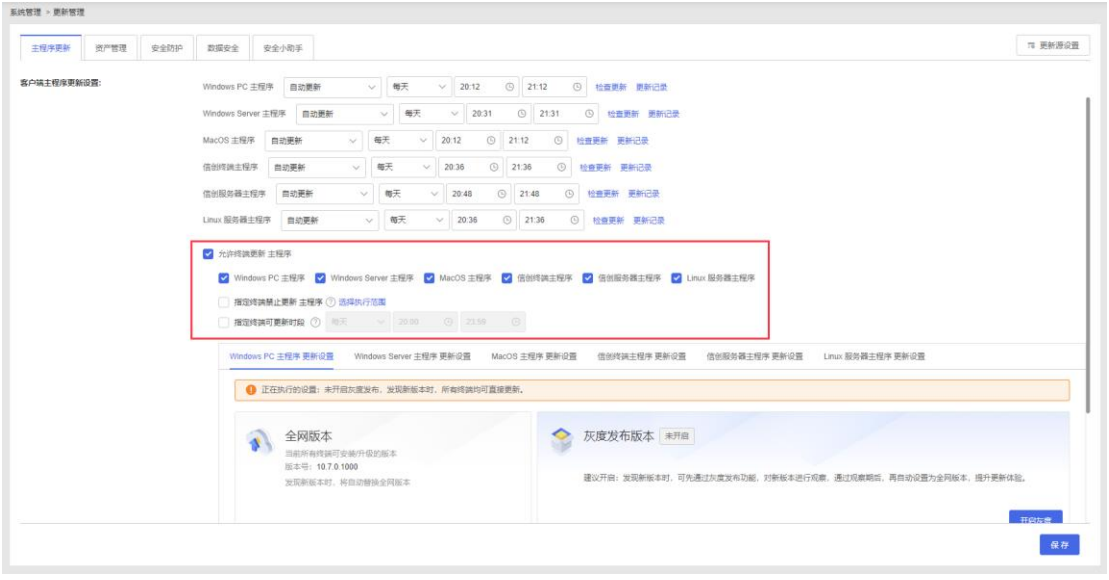
终端更新配置步骤和说明（以主程序更新为例，补丁库、病毒库等同理）：

1) 开启终端更新主程序并开启某类型的终端更新。

a) 进入“系统管理>更新管理”，然后切换至“主程序更新”页面。

b) 勾选允许更新终端主程序，并勾选允许更新的终端类型。若不开启终端更新，或不开启某系统类型的终端的更新，则终端将不可升级，仅可通过在线部署和离线更新安装最低版本（底包）。

c) 此次，还可以配置指定终端禁止更新的组织结构或自定义组和更新时段。



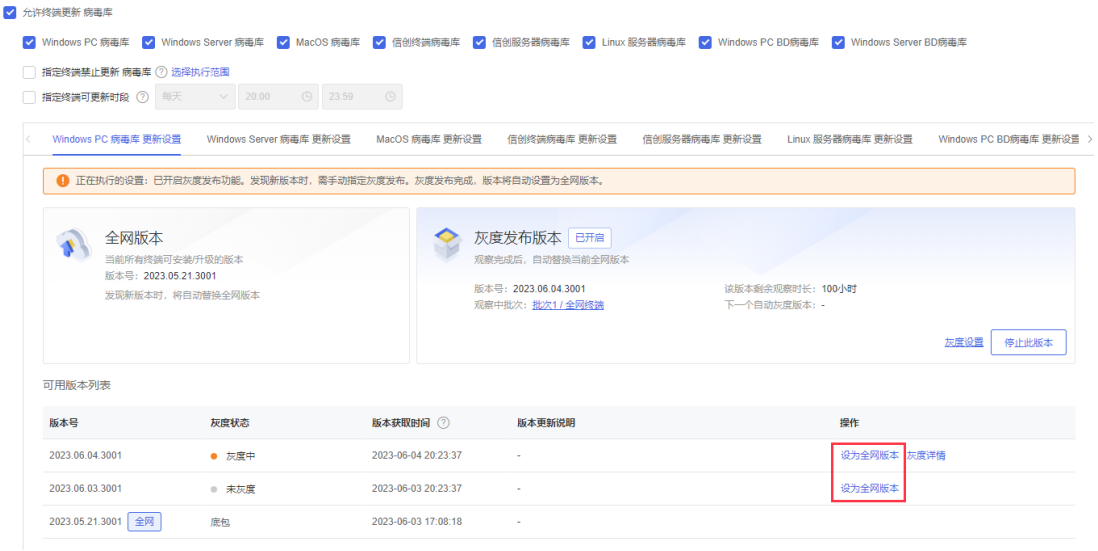
2) 切换终端类型更新设置 tab，可以进入不同类型终端的更新设置。

3) 全网版本，是全网的终端，新安装或升级时，使用的版本。其变化的逻辑为：

a) 不勾选允许更新终端主程序，或不勾选允许更新的终端类型。则该类型终端将不可升级，仅可安装最低版本（底包），全网版本将自动变为最低版本（底包），不能进行设置。

b) 勾选允许更新终端主程序，并勾选允许更新的终端类型。不开启灰度更新功能。则每次管理中心更新了新版本后，将自动更新全网版本。所有终端可以更新到全网版本。

c) 勾选允许更新终端主程序，并勾选允许更新的终端类型。开启灰度更新功能。此时用户可以手动指定全网版本。当有灰度版本灰度完成以后，会自动替换当前全网版本。（该图为在管理中心里设置病毒库在终端中设置全网版本的示意图）



4) 灰度版本，管理中心发现终端客户端主程序新版本时，可先通过灰度发布功能，对新版本进行观察，通过观察期后，再自动设置为全网版本，提升更新体验。

a) 灰度版本必须在勾选允许更新终端主程序，并勾选允许更新的终端类型后。功能才会正常生效。否则即使开启灰度，功能也无法生效。

b) 点击开启灰度功能，可以打开灰度的设置弹窗。灰度功能已开启时，可通过该卡片上的“灰度设置”按钮打开。

c) 灰度设置弹窗中，可以配置灰度发布的方式。该弹窗的设置需在弹窗中点击确认后，再在整体更新管理页面中点击保存后才生效。

i. 设置项，灰度发布功能：开启/关闭

ii. 设置项，新版本出现时。

1. 若选择自动灰度发布，则当管理中心获取新版本时，会对其向终端进行灰度发布，发布后将替换全网版本，达到自动灰度，自动推送全网终端的能力。

2. 若选择不自动灰度发布，管理中心不会自动不对版本向终端进行灰度发布。需用户手动指定灰度版本

iii. 设置项，新版本自动灰度处理方式。此项仅在选择“自动灰度发布”时，可设置。

1. 等待已有灰度发布完成后再进行最高版本灰度发布。设置此项后，某版本正在灰度时，管理中心获取新版本时，该新版本将排队。待正在灰度的版本灰度完成后，再进行灰度。

2. 终止当前的灰度发布，直接进行最高版本灰度发布。

iv. 设置项，灰度发布范围设置。

1. 对灰度发布的终端范围进行设置，以批次的维度进行管理，观察的顺序按批次号排序，如，批次 1 结束后再进行批次 2 中终端的灰度发布。可对每个批次观察的时长和终端范围进行设置。

2. 周六日不计入观察时长。灰度观察的方式主要为通过每个批次的终端按顺序安装/升级版本后，再观察特定的时间，周六日通常为非工作日，并没有观察的价值。勾选此项，在灰度时，计算观察剩余时长时，可跳过对周六日的计算。

灰度功能其他操作

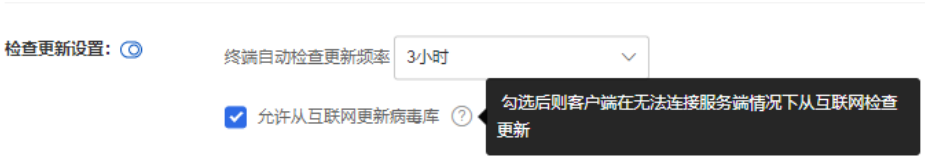
1） 停止当前灰度版本。点击后可以停止当前版本的灰度发布。

2） 查看当前灰度中版本的灰度的进度。点击可用版本列表中的灰度详情，或灰度发布卡片中的观察中批次，可以查看当前灰度的详情。

更新源及下载源配置：

1) 终端更新源设置，当前允许离线终端从互联网检查更新，仅对病毒库生效。

配置入口：终端管理>基础策略>通讯设置>检查更新设置；



2) 终端下载源设置，当终端根据上述配置检查到可更新的版本后，根据定义的下载源进行更新文件下载(此设置仅涉及文件下载，不涉及更新检查)，当前支持“仅内网”、“内网优先”、“仅互联网”、“互联网优先”，如果是“仅内网”则需要保持终端与管理中心的连通信。

配置入口：终端管理-基础策略-通讯设置-下载源设置；

25.3.2. 在线更新

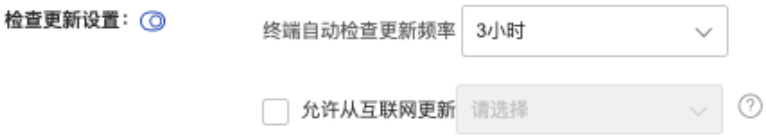
在线手动更新步骤：

1) 在终端手动点击更新。在终端主界面左上角箭头图标或终端主界面右上角菜单下的“检查更新”触发更新；如果开启了优先升级分组，此终端须在分组内，否则只能等待观察结束。

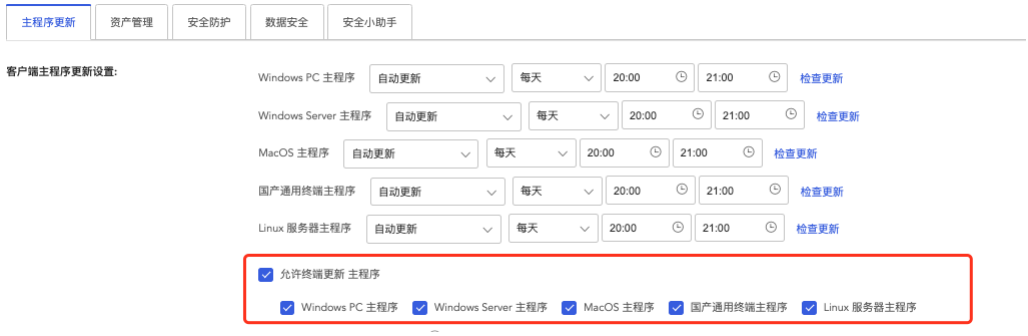
2) 触发更新后会弹出升级进度对话框，无更新则直接提示，有更新则等待更新完成即可。

在线自动更新步骤：

1） 在资产管理>基础策略>通讯设置中，设置终端自动更新检查频率；



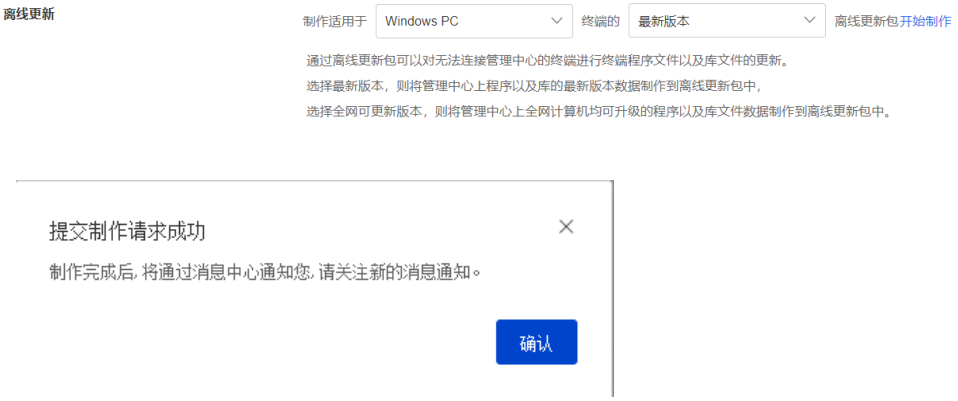
2） 在系统管理>更新管理，开启“允许终端更新主程序”等配置；



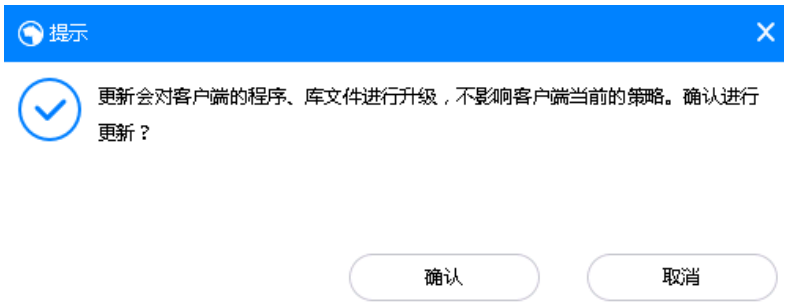
25.3.3. 离线更新

离线更新步骤：

1) 在管理中心制作离线更新包。打开奇安信天擎终端安全管理系统并进入终端管理>终端部署页，切换至更新包部分并选择离线更新的客户端类型和版本后点击“开始制作”，而后等待通知。



2) 下载离线更新包拷贝至终端更新。离线更新包制作完成后，从右上角的消息中心获取下载地址，然后拷贝至对应的终端双击更新，确认提示后即开始更新；



3) 更新完成后显示完成，主程序版本、各种库版本将更新。

25.4. 典型场景

25.4.1. 隔离网部署的管理中心如何更新

请参考 **错误!未找到引用源。** 章节。

25.4.2. 孤岛终端如何更新

请参考 **错误!未找到引用源。** 章节。

25.4.3. 如何降低更新带来的风险

终端会根据策略中设置的检查更新时间自动触发检查更新，如果管理中心开启了允许更新主程序、病毒库等，在奇安信天擎管理中心更新后，为了验证新版本终端对既有终端版本的更新稳定性和兼容性，可以在管理中心开启新版本灰度更新来设置优先更新的分组，同时对特定的终端也可以设置禁止更新，具体步骤如下：

1) 打开奇安信天擎终端安全管理系统管理中心，系统管理>更新管理，主程序更新菜单下。
2) 勾选对应终端的类型保证更新通道开启，然后设置需要禁止更新的终端范围。
3) 勾选对应的灰度更新的开关，并选择终端将要更新的版本，默认更新至最新。
4) 点击添加，并选择希望优先更新的分组，选中并输入观察时长后保存会添加至下方优先分组列表。

设置后，以后每次管理中心更新版本后，终端主程序批次内终端都会优先进行更新，30 小时后会转为对全网终端端自动更新，如果设置了终端例外，则例外终端不能更新。

如果在观察期间发现严重问题，应停止终端更新，待解决问题再打开更新。如果是全网终端自动更新期间发现有严重问题，应回退到上一个稳定版，并酌情调整批次内的分组。待问题解决后重新选择版本进行灰度更新。

灰度更新，可参考终端灰度发布实践案例

25.4.4. 如何减小更新时占用带宽对业务的影响

更新对网络带宽的影响主要为奇安信天擎管理中心更新后，全网终端进行更新时产生的流量对企业业务网络带宽造成的影响。

对于网络带宽小，网络覆盖范围大，但是终端开机时间又相对统一的情况，可以部署接入点缓存文件，终端从接入点下载文件，接入点没有缓存时会回源到管理中心服务器下载，减少对业务网络造成压力。

同时，终端更新时可在策略中的资产管理>终端管理>基础策略>通讯设置>下载设置中开启 P2P 下载，利用同网段中正在更新的其它终端更新，能减少更新对服务器的压力（说明：开启 P2P 下载会增加 ARP 广播数量，请按分组分批设置）。

25.4.5. 如何在更新管理中心后暂不更新终端

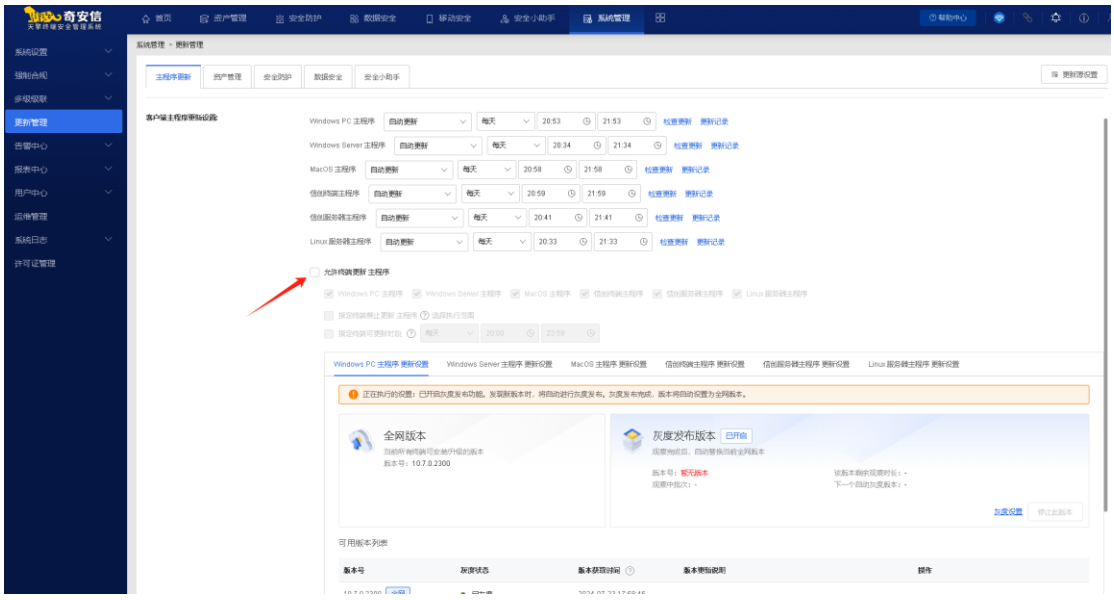
管理中心更新后，如果暂时不希望终端更新至对应版本，打开管理中心，系统管理>更新管理菜单并切换至主程序更新页面，取消勾选“允许终端更新主程序”即可。

25.4.6. 终端灰度发布实践案例

建议天擎在首次安装后，立即做好灰度发布的配置，如果还未配置，请先配置好后再执行天擎管理中心的更新操作。以下为天擎的灰度发布推荐流程及灰度配置示例：

步骤 1：在控制台版本更新和客户端程序版本更新前，先关闭“允许终端更新”的功能

以客户端主程序为例，在“系统管理>更新管理>主程序更新”中，取消勾选“允许终端更新主程序”，避免灰度生效前，全网终端触发了更新。



步骤 2：创建优先更新的分组，并筛选出相应终端

用于更新观察的分组，推荐至少完成 3 个批次下的终端更新，再全网终端更新（如果企业规模小，也可以设置 2 个批次），这样需要准备 3 个分组来观察更新。

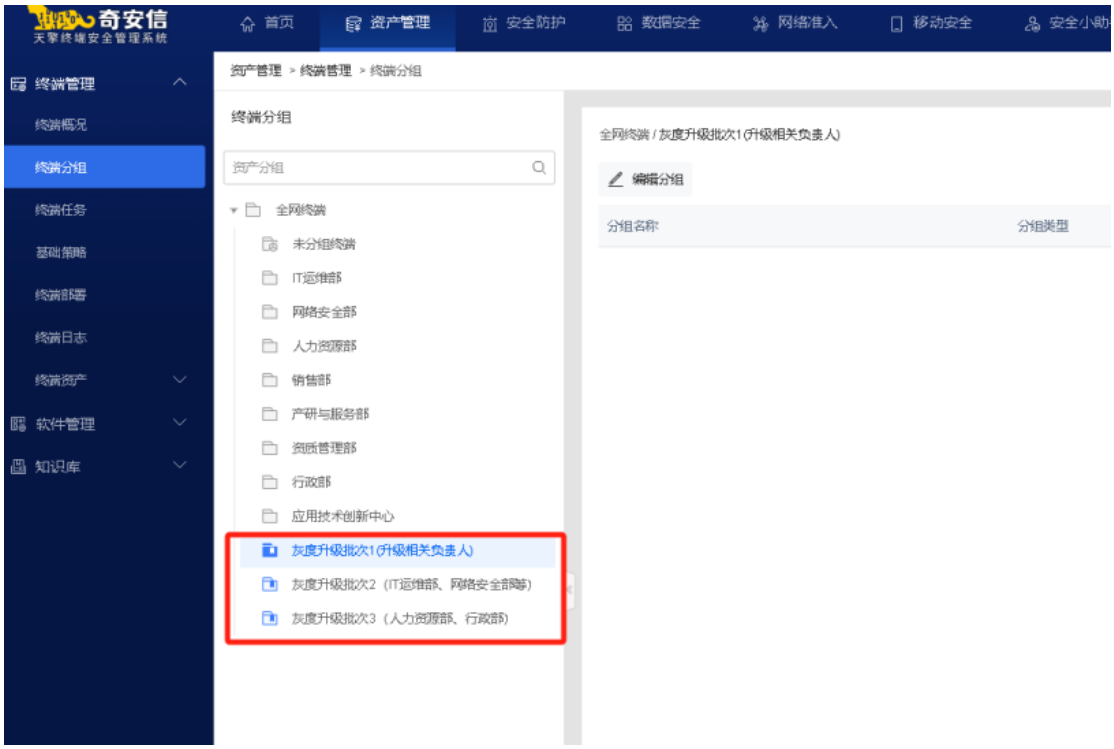
分组，建议创建专门用来观察、优先更新的自定义分组，并添加一定数量的终端：

批次 1 对应分组 1 下终端 10 台；推荐将操作此次更新相关的运维、研发、测试人员的终端（主要是操作此次更新相关的人员，可以在客户端主界面左上角人工点击更新，直接更新到最新版本，用来验证此次更新流程是否正常）；

批次 2 对应分组 2 下终端 100 台；推荐选定“IT 运维部/网络安全部/信息管理部”等运维使用天擎的相关部门终端。一旦有问题，部门内部可以立刻知晓，停止后续批次的更新；

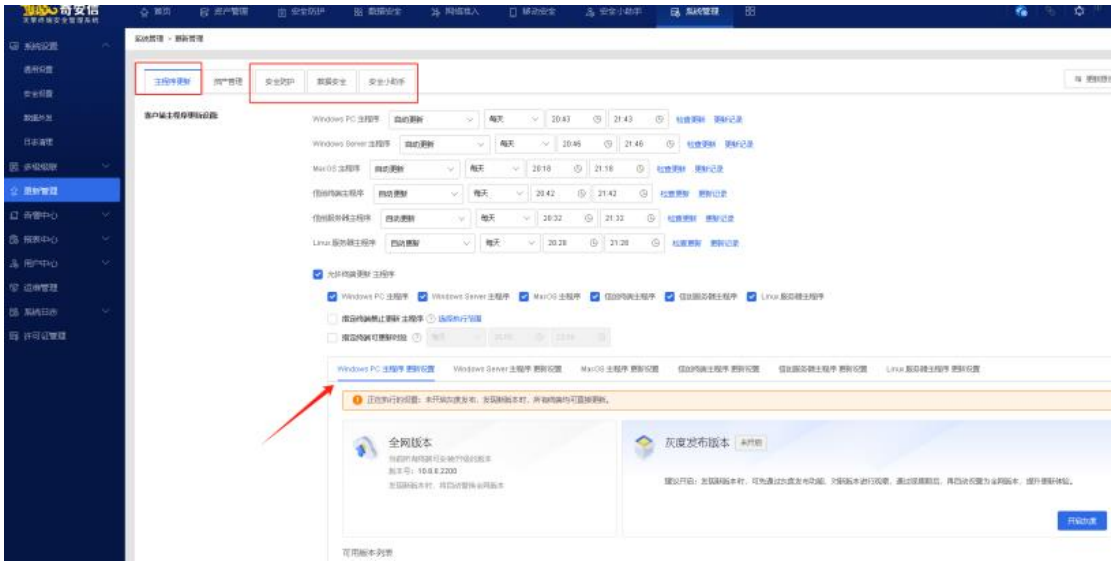
批次 3 对应分组 3 下终端 200 台，推荐再选定一些非核心业务部门终端做第三批次灰度更新。

如下截图，分别创建了灰度升级批次 1(更新相关负责人)、灰度升级批次 2（IT 运维部、网络安全部等）、灰度升级批次 3（人力资源部、行政部），三个自定义分组用来优先更新。



步骤 3：开启灰度发布，并创建批次

下面以主程序更新中的 Windows PC 主程序更新设置为例说明，其它安全防护、数据安全、安全小助手，以及对应的每个终端类型也建议开启灰度发布



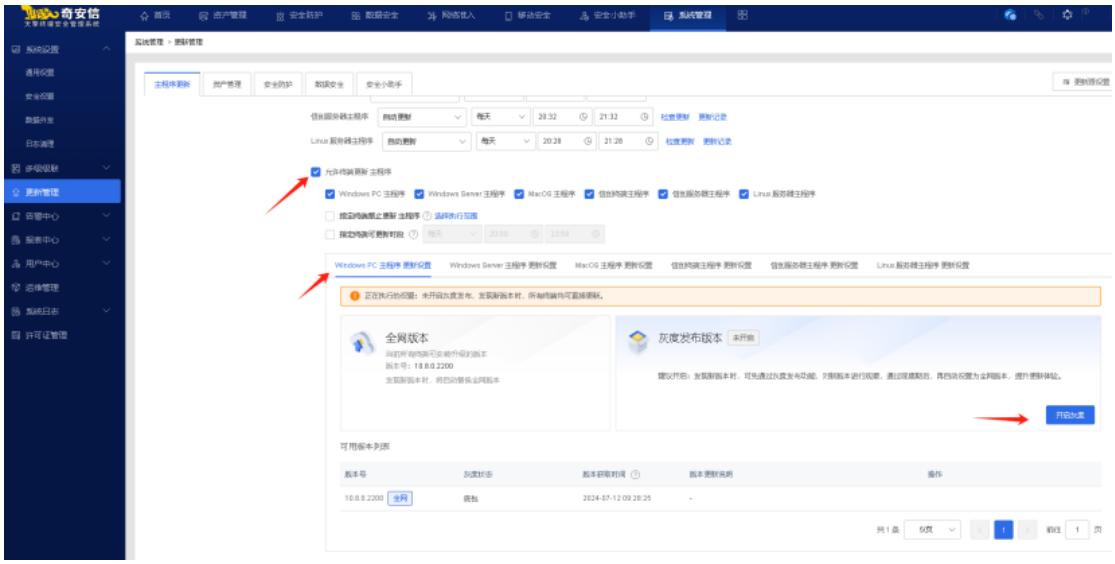
1）进入“系统管理>更新管理>主程序更新”，在客户端主程序更新设置里，开启允许终端更新主程序，在 Windows PC 主程序更新设置里，点击【开启灰度】

2）灰度发布设置，新版本出现时、新版本自动灰度处理方式，推荐默认设置。灰度发布范围设置，具体配置可以根据企业实际情况自行规划，下面提供一套主程序更新的推荐配置：

批次 1，选择上述灰度升级批次 1，观察时长设置 24 小时；

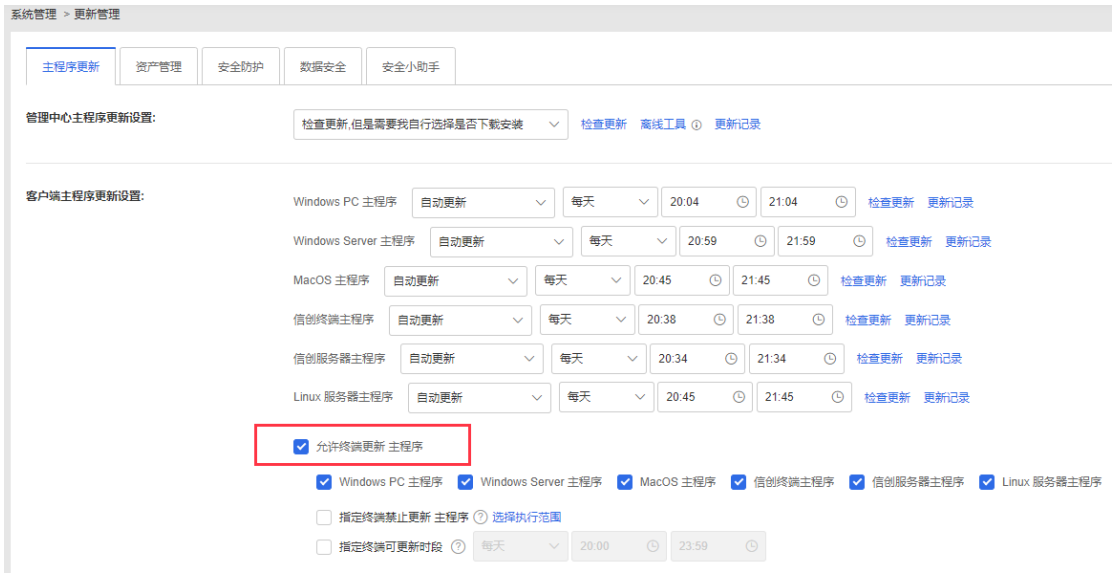
批次 2，选择上述灰度升级批次 2，观察时长设置 48 小时；

批次 3，选择上述灰度升级批次 3，观察时长设置 120 小时。



步骤 4：确保配置了灰度发布批次后，再开启“允许终端更新”的功能

以客户端主程序为例，在“系统管理>更新管理>主程序更新”中，勾选“允许终端更新主程序”



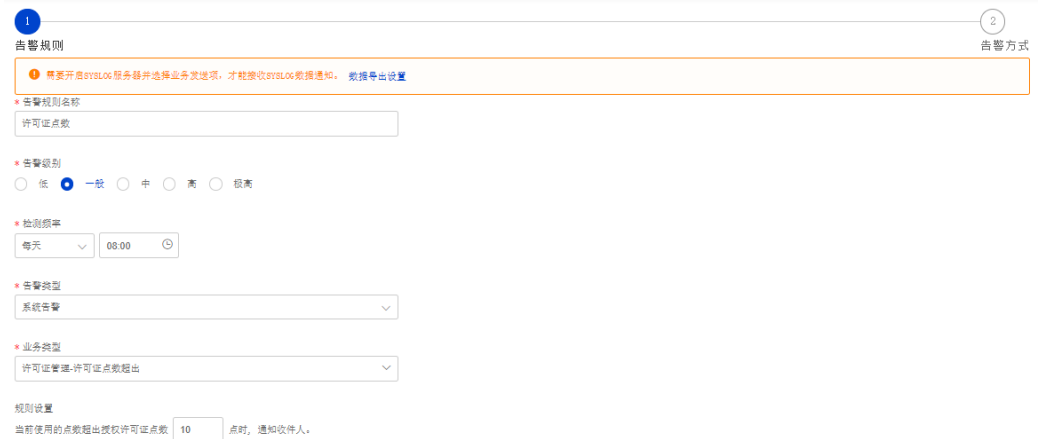
26. 告警中心

告警中心通过“邮件、短信、SYSLOG 告警”三种告警方式按照预先配置的告警规则通知管理员终端的各种安全状态或者风险，帮助管理员及时处理安全风险。

告警配置：

- 配置规则

基于告警级别、检测频率、告警类型、业务类型和规则设置定义一个告警规则，然后选择告警方式，比如“邮件告警”、“SYSLOG 告警”、“短信告警”，选择对应告警方式前需在系统设置中相应配置对应地址才可使用。



- 告警规则管理

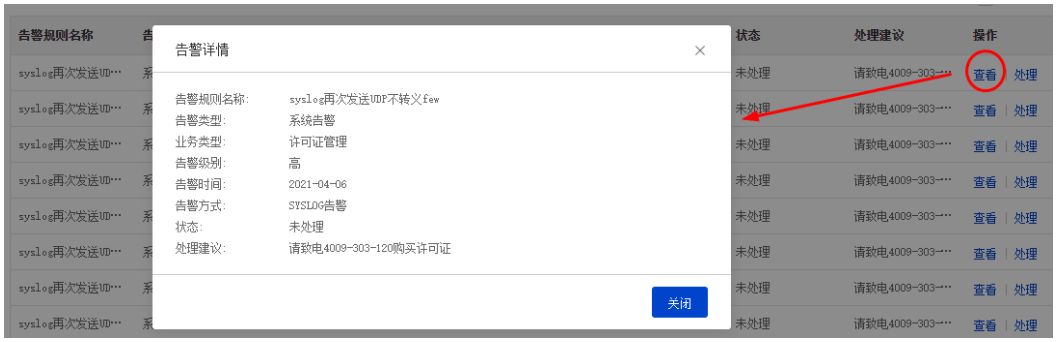
新建完告警规则后可以进行启用、停用、编辑和删除，点击名称可以查看告警详情，支持通过“高级筛选”筛选规则。

告警列表：

- 告警列表展示当前的告警信息，左上角汇总有当前待处理告警数、急需处理告警以及已忽略告警。

- 可以基于条件筛选告警信息，筛选可以保存便于下次直接使用。

- 可以查看告警详情。



◆ 可以对告警进行处理。

27. 报表中心

报表中心提供了自定义报表的能力，并将自定义的报表定时生成周期报告，管理员可登录管理中心查看、下载周期报告，周期报告可配置发送邮件，可通过发送邮件方式周知管理员来查看周期报告。

27.1. 视图

一个视图对应一个图表类型，对某业务数据可自定义图表类型进行统计。

入口：系统管理>报表中心>视图

1) 视图展示样式支持卡片模式、列表模式，默认卡片模式，点击右上角的“显示列表”可切换列表模式。

2) 视图支持根据视图名称进行模糊搜索。

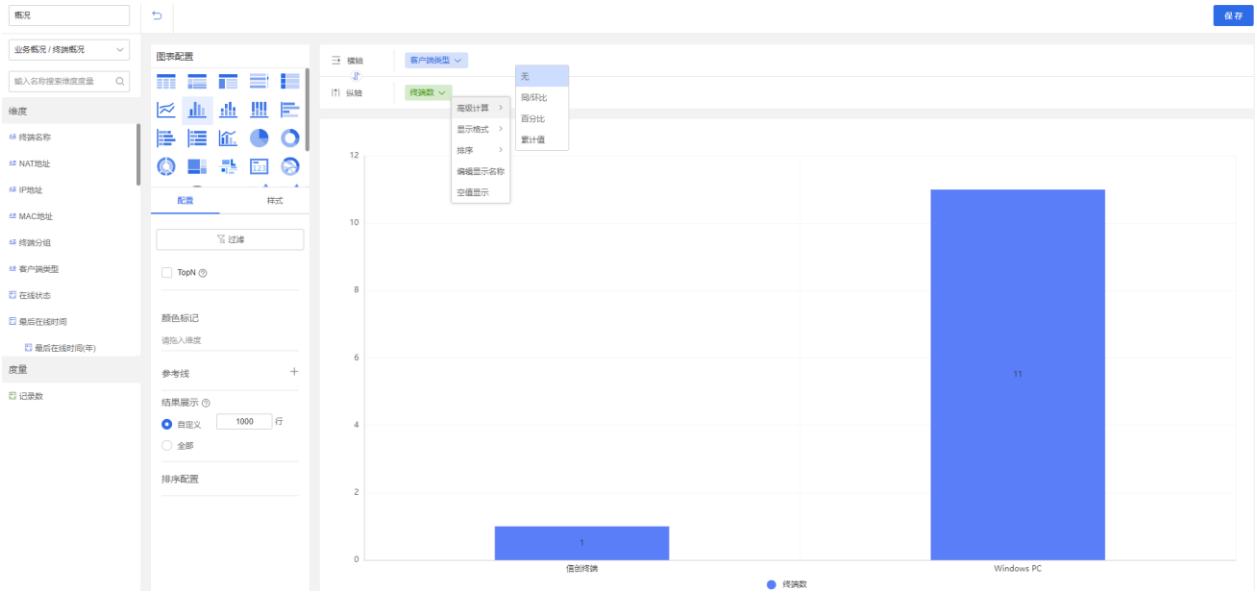
3) 通过目录树可对视图进行分类管理。

4) 在列表模式下，可对视图进行批量移动到某一目录下，可对视图批量复制视图、批量删除。

5) 对单个视图支持编辑、重命名、移动到、删除操作。

6) 点击[编辑]进入编辑视图界面：

- 在左上角选择业务数据集
- 选择业务数据集后，在业务数据集下方展示该数据集下的维度字段和度量字段
- 在图表配置区域，选择图表类型后，在右侧区域上方展示该图表涉及的字段分类，将维度字段、度量字段拖拽到图表的字段分类后，在右侧区域的下方展示图表
- 在图表配置区域，可对图表进行配置、样式设置。
- 图表选择的字段，支持设置：显示格式、排序、显示名称，数值类型的字段支持设置高级计算。



27.2. 仪表板

可在仪表板画布上添加多个视图，并自定义视图的大小和位置，可对仪表板的样式进行配置。

入口：系统管理>报表中心>仪表板

1) 仪表板展示样式支持卡片模式、列表模式，默认卡片模式，点击右上角的“显示列表”可切换列表模式。

2) 仪表板支持根据仪表板名称进行模糊搜索。

3) 通过目录树可对仪表板进行分类管理。

4) 在列表模式下，可对仪表板进行批量移动、批量删除的操作。

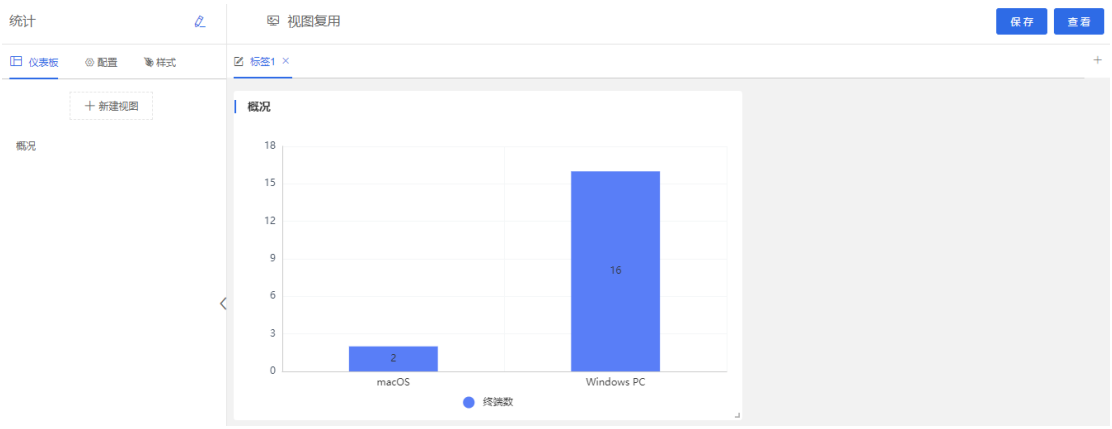
5) 对单个仪表板支持查看、编辑、重命名、公开、复制、移动到、删除操作。

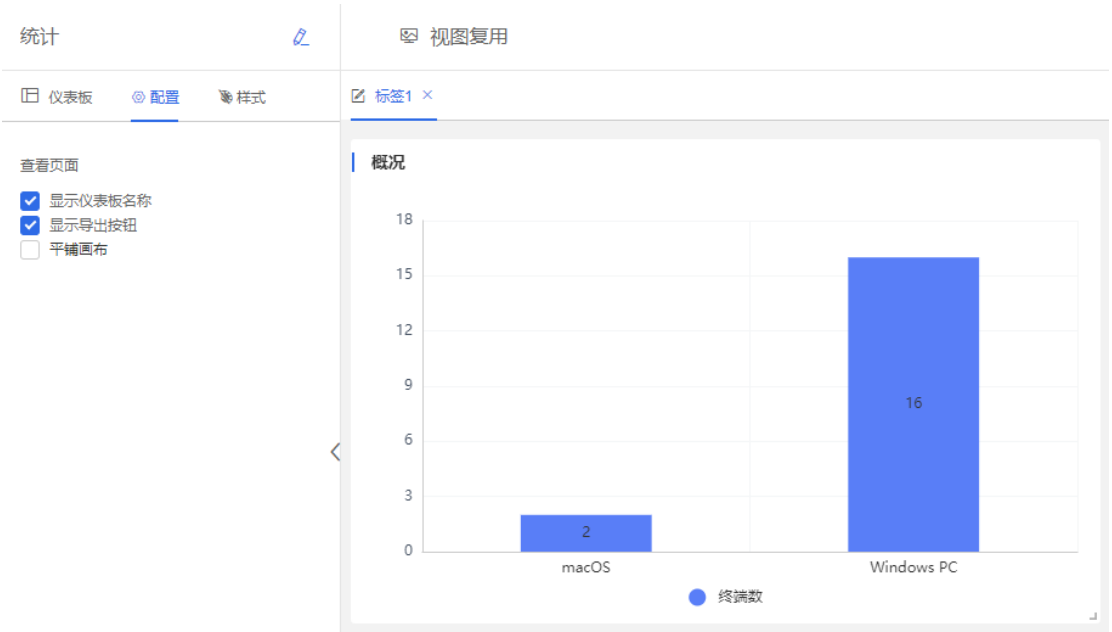
6) 选择某个目录，点击[授权]，可将该目录下的仪表板授权给其他管理员查看、编辑的权限，有授权的管理员可在已授权目录查看到该仪表板。

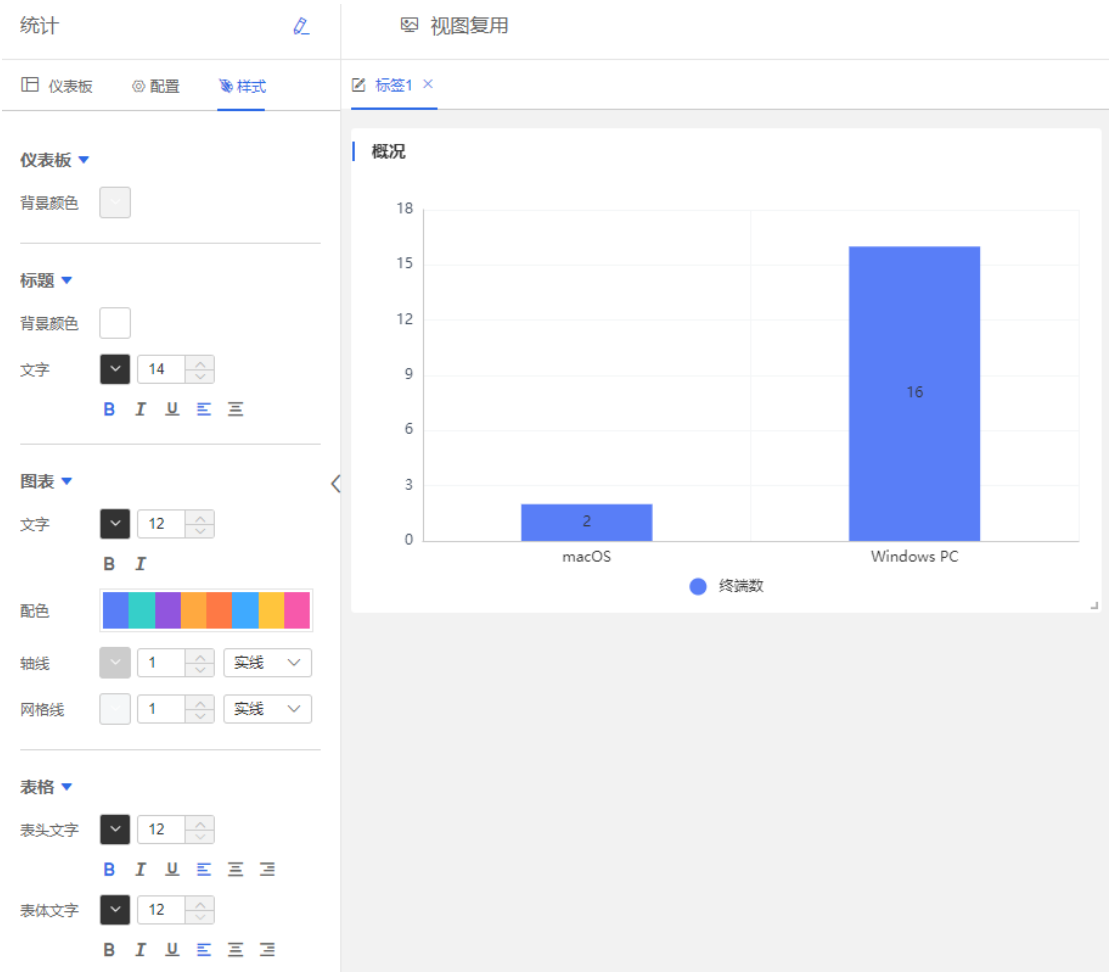
7) 对仪表板进行公开操作，则所有管理员均可在公开目录下查看该仪表板。

8） 点击[编辑]按钮，进入到编辑界面：

- 可复用在视图菜单中已创建的视图、也可在仪表板中现创建视图并使用
- 添加的视图支持操作：编辑视图、隐藏标题、编辑标题、查看数据、复制、删除、视图隐藏
- 仪表板支持配置：是否显示仪表板名称、是否显示导出按钮、是否平铺画布
- 仪表板支持样式设置：背景颜色、标题设置（背景颜色、文字样式）、图表设置（文字样式、配色样式、轴线、网络线）、表格设置（表头、表体文字样式）
- 仪表板支持标签名添加、编辑







9) 点击[查看]按钮，在查看界面展示所添加的视图，查看界面的[导出]功能通过编辑界面的配置项控制是否显示。

27.3. 周期报告

入口：系统管理>报表中心>周期报告

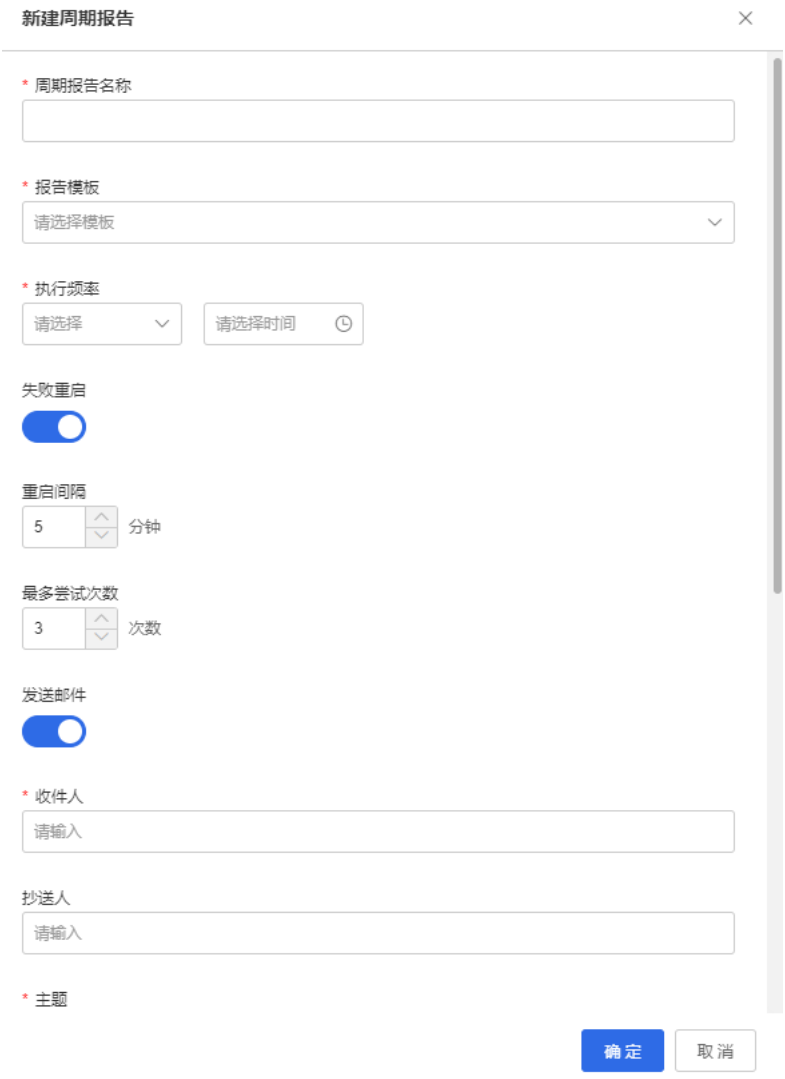
1) 支持基于仪表板创建周期报告

2) 周期报告支持启用、停用、立即运行、编辑、删除功能

3) 周期报告列表支持根据名称模糊搜索

4) 周期报告支持查看/删除历史生成的周期报告

5) 点击[新建周期报告-基于仪表板新建]，在新建周期报告弹窗内，需要配置周期报告名称、选择报告模板（即仪表板）、执行频率（支持按照每年、每月、每周、每天的频率定期生成周期报告）、发送邮件。



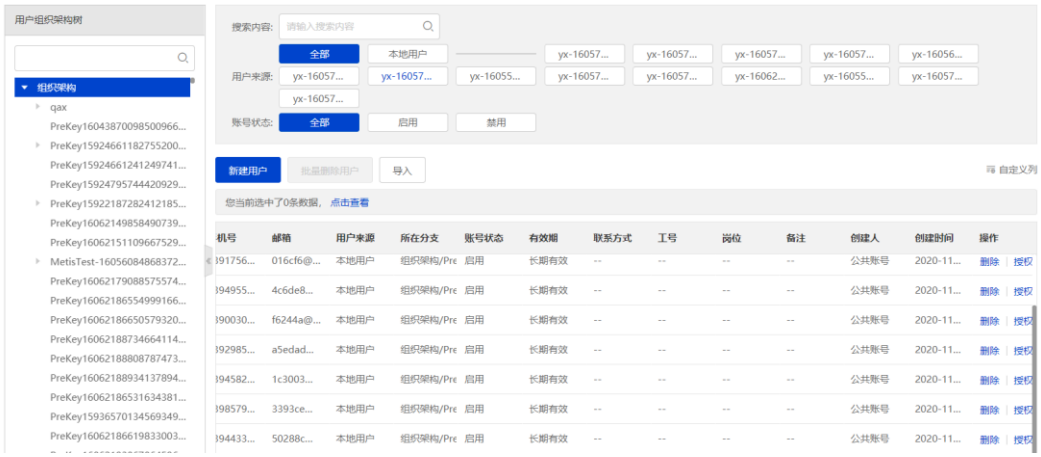
28. 用户中心

在用户与权限模块中，可以对系统的组织架构、用户、管理员权限以及与用户相关设置进行配置。

28.1. 用户

管理员可以通过组织架构、用户来源、账号状态等筛选条件查看用户，包含手动添加的和从第三方系统同步的用户，同时有权限的管理员可对用户进行新建、删除、导入、编辑、重置密码、授权等相应操作。

如果需要按“用户”（人员）来管理终端，需通过用户分组配置策略来实现管理。具体参阅策略章节。



28.2. 用户分组

在 用户中心>用户分组 页面，可以查看当前的用户分组信息，也称用户树。

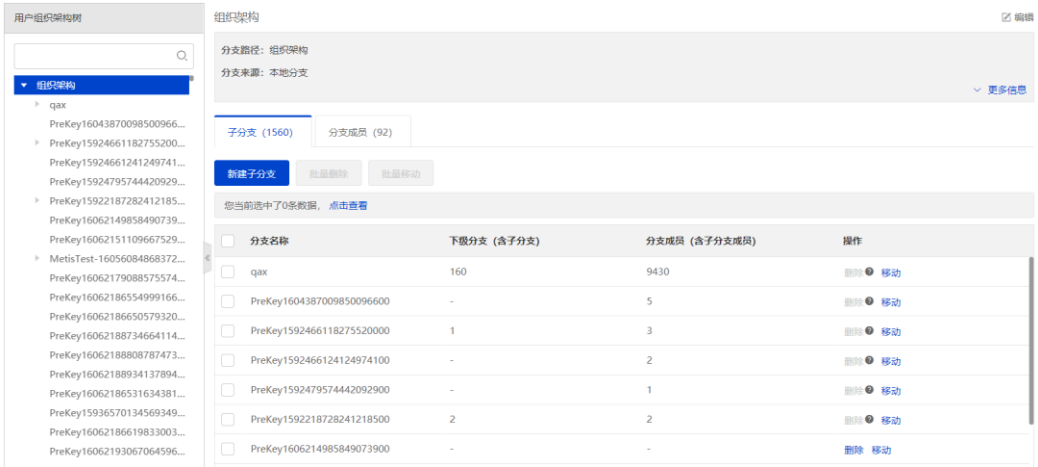
用户分组来源组织架构树（入口：系统管理>用户中心>组织架构），也可以添加自定义分组并设置分组条件。

28.3. 组织架构

组织架构体现企业或者单位的人员组织架构，用于管理人员信息，管理员也是企业或者单位的一员，只是与普通用户的权限不一样。

导航到“用户中心>组织架构”，管理员可对分支机构进行新建、删除、移动、编辑等操作，也可以管理用户的信息，比如新建用户、重置密码。

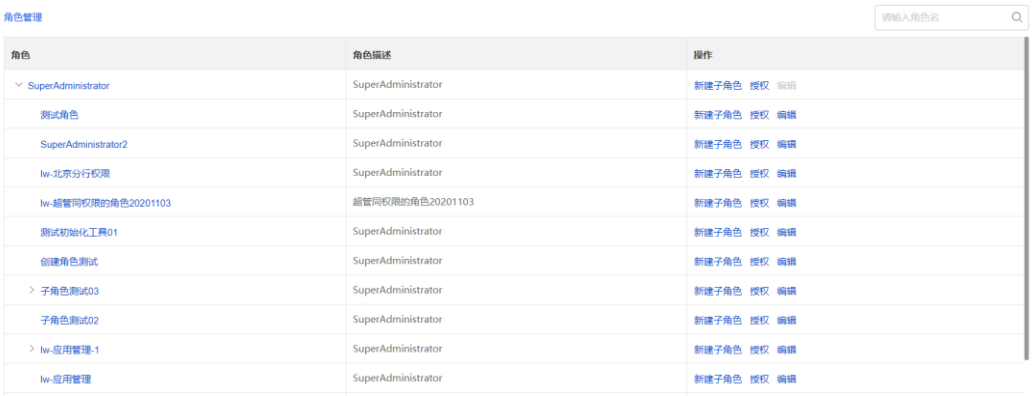
根据实际的管理需要，管理员可以手动创建分支机构，也可以从第三方系统同步组织架构，如 LDAP 等。



28.4. 权限

权限管理即管理员的权限管理，普通用户被授予管理员权限后则变为既是管理员也是普通用户。

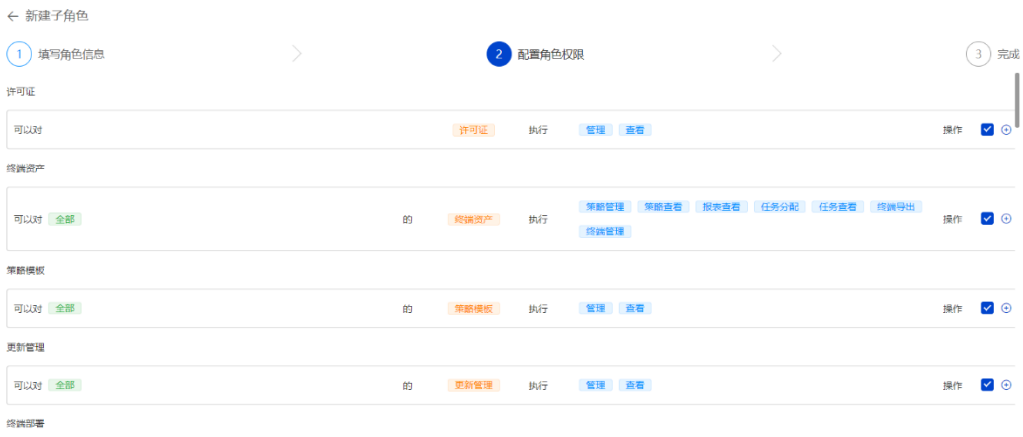
在系统初始化时，企业的管理人员添加企业的用户，并为添加的用户授予超级管理员权限，授予后，所添加的用户登录至管理中心时，可以根据对应的角色和权限来新建子角色、编辑角色、授权等操作。



在某个角色上，点击操作项中的新建子角色，进入新建子角色页面，在新建子角色页面，按照步骤输入相关信息

填写角色名称和描述

配置角色权限，可以对资源、资源的数据、操作权限进行编辑

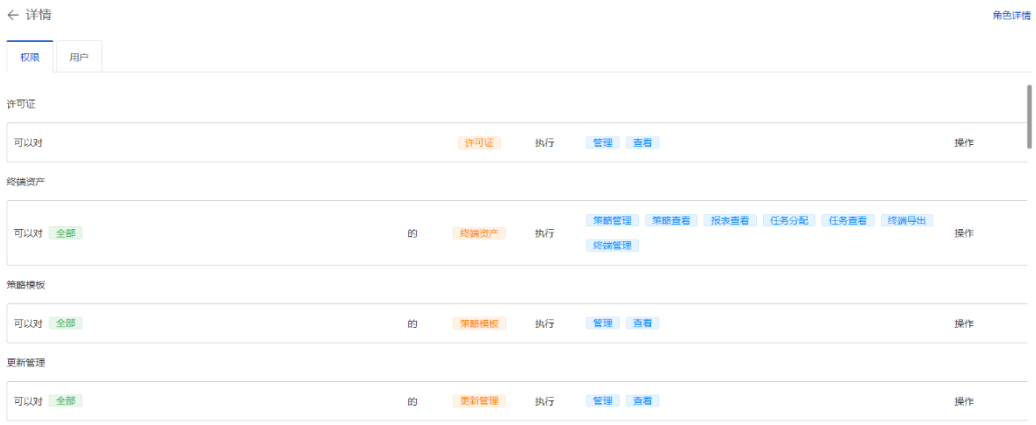


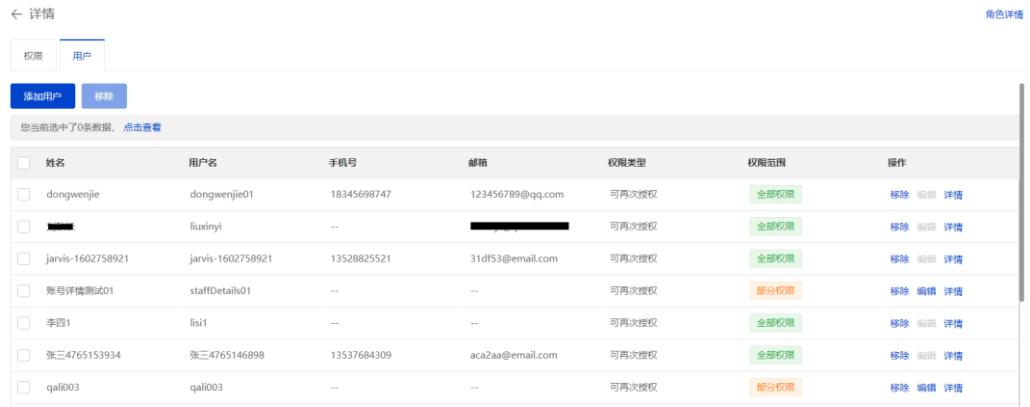
完成后，创建该角色，并可将该角色授权给其他用户。

若权限范围为：该角色全部权限，则是将该角色直接授予该用户，若将勾选去掉，则授予的是该角色的部分权限。两者的区别是对应权限范围和使用方式不同。

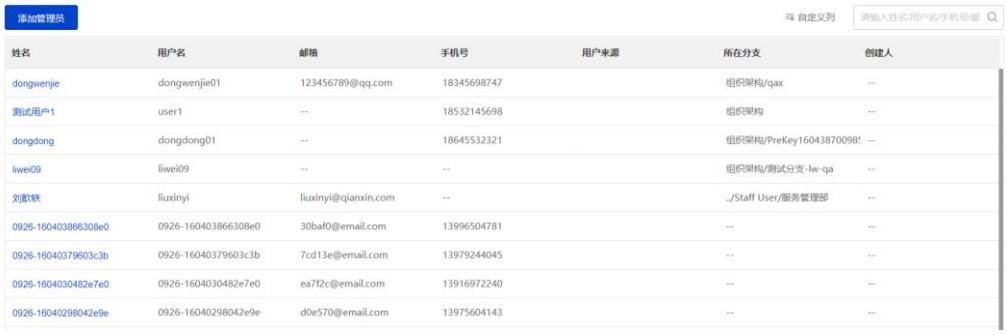
若权限类型为：可再次授权时，对应的用户除了可以使用权限所描述的能力外，还可以将权限再次授权给其他用户，若取消勾选，则代表该用户只能使用权限所描述的功能。

在权限详情中，可以查看该角色对应的权限、以及该角色所授予的用户（包含部分权限和全部权限）。





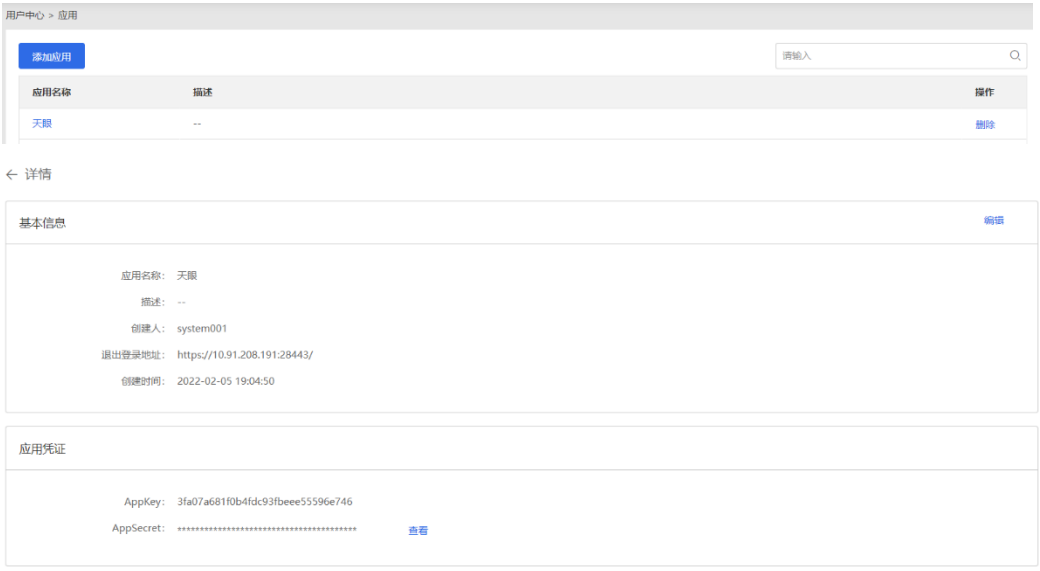
管理员指，对应管控平台有权限且有再次授权权限的用户，在管理员页面，管理员可以查看、添加管理员，且在用户详情页面可以对其权限进行解除等操作。



28.5. 应用

“应用”指本管理系统之外的第三方系统。第三方系统需要与奇安信天擎联动时，必须要在用户中心配置为一个“应用”，否则不能访问奇安信天擎的数据和联动操作。

比如天眼、NGSOC 或者其他 SOC 平台需要对接天擎数据或处置终端，则在天擎中添加应用获得凭证（AppKey 和 AppSecret）后并且在联动前通过认证才可联动。



应用名称：在本系统的显示名称，方便管理。

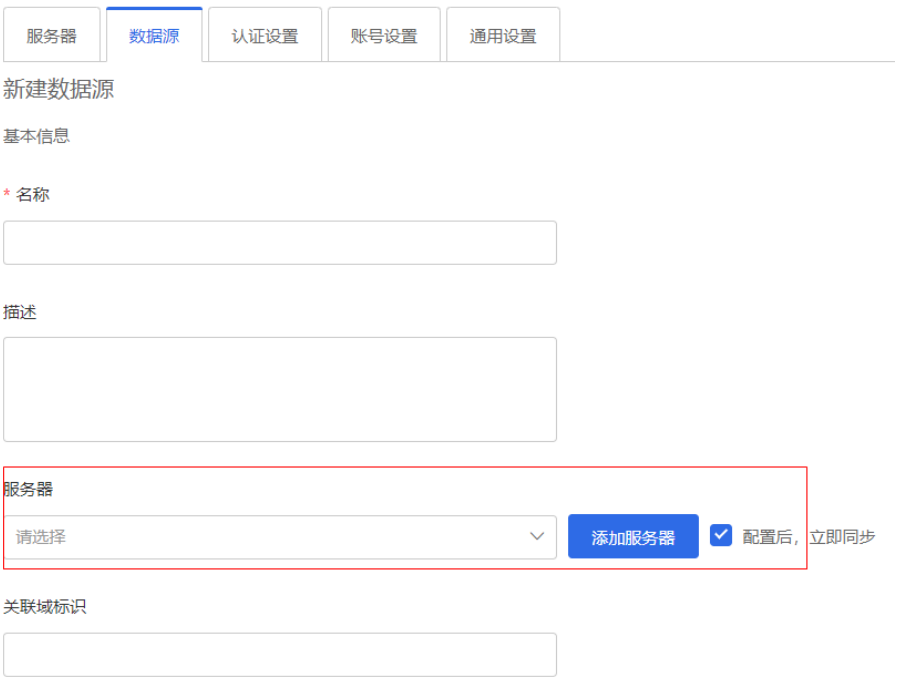
退出登录地址：用于本系统主动触发退出第三方系统退出登录状态。

28.6. 用户设置

与用户相关的配置信息都在用户设置中，包含：服务器、数据源、账号设置、通用设置。

服务器：指同步第三方的用户管理系统的服务器，如 LDAP，需要配置 LDAP 服务器相关配置信息。

配置完成后，在添加数据源和认证因子时，关联所配置的服务器信息。如：

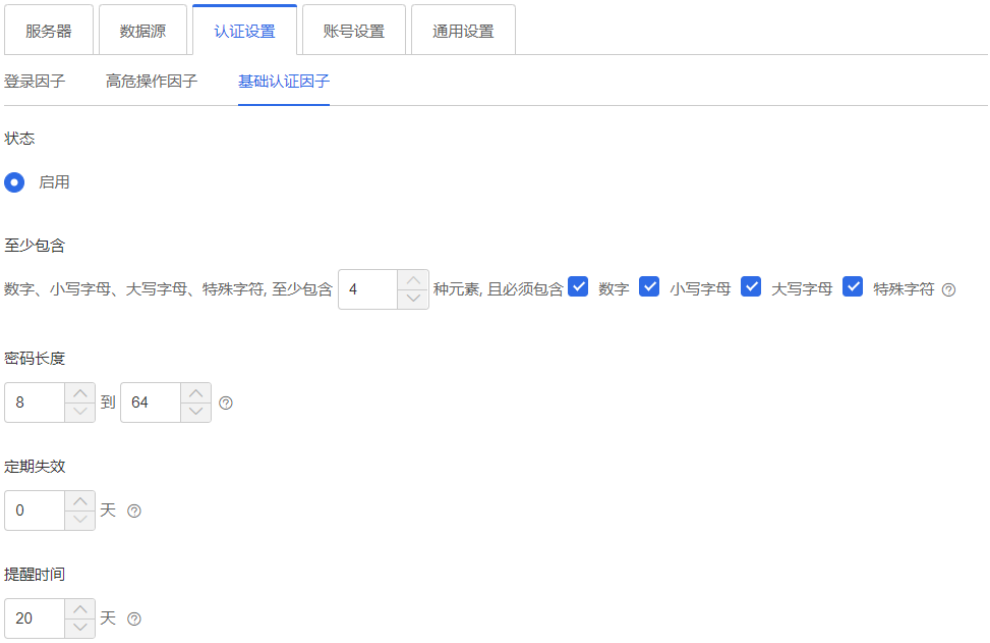


在认证设置页面，可以配置登录因子、高危操作因子和基础认证因子等。登录因子：默认是单因子认证，管理员可以启用双因子认证，启用后管理员在登录时，需要验证两个因子才能登录。

高危操作因子：默认未开启，管理员可以开启，开启后管理员在执行某些操作时需要根据因子再次做验证，若管理员某个因子未初始化（绑定）时，需要先初始化才能操作。高危操作因子具体信息请参考 KB119483

基础认证因子：登录因子和高危操作因子中配置时所需的基础认证因子。

在基础认证因子中，对于内置密码（本地新建用户对应的密码）相关配置信息如下：管理员可以配置密码的长度、复杂程度以及密码有效期等相关设置。



账号设置：账号锁定设置和账号登录设置。

账号锁定设置：当账号在登录时，验证错误次数超过指定次数时的账号锁定策略，在锁定期间内，该账号不能登录。

账号登录设置：设置用户分别在管理中心和终端上可并行登录的个数，以及超出数量的处理办法。

28.7. 审批工作流

审批工作流服务于安全业务，业务流程中的某些权限资格，需要上级批准时才能继续执行的情况，审批工作流提供统一的审批流程定义和过程管理。

28.7.1. 工作流管理

- 支持自定义审批工作流，包括自定义审批节点数量和审批适用的安全业务类型。
- 审批节点支持并行和串行关系进行组合。串行审批节点为必过，并行审批可配置部分通过即完成审批。
- 每一个审批节点的审批人既可以直接定义一个用户，也可以定义为审批角色。
- 工作流按使用者角度可应用给用户、用户组和用户审批角色。
- 工作流创建后，管理员可进一步进行挂起、编辑和删除操作。

28.7.1.1. 审批角色

审批角色为用户标签，不具备平台管理属性。

定义：为了使审批工作流能够批量操作，将一批具有相同审批等级的用户定义为相同的审批角色，简化审批工作流本身的维护量。

新建审批角色：

授权：将审批角色赋予用户的过程。

28.7.1.2. 新建工作流

工作流创建分为业务定义和执行范围定义两个步骤，前者定义详细的审批节点和模式，后者定义工作流本身的生效用户范围。

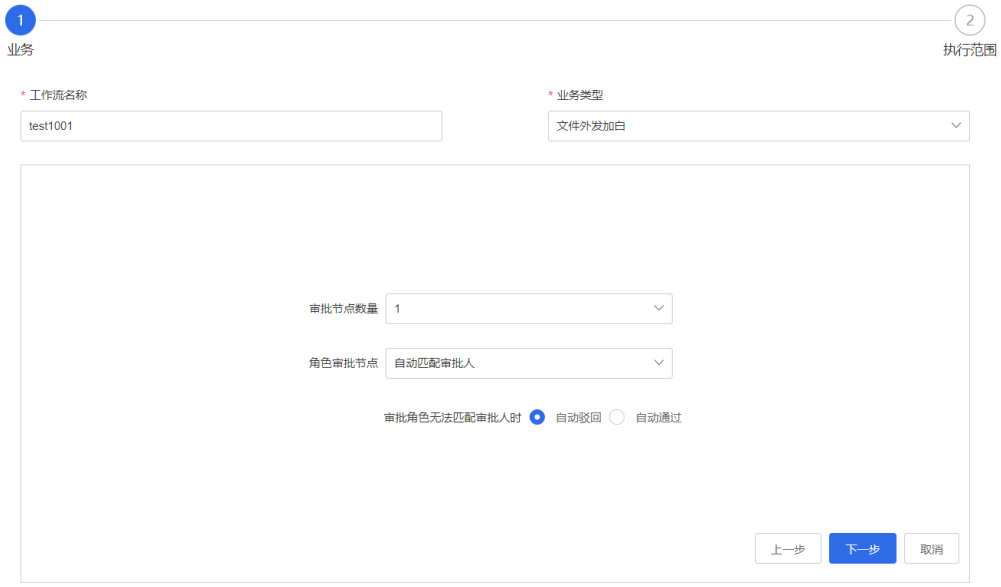
第一步：定义审批流模式

业务类型：适用的安全业务。

自动匹配审批人模式：如果将一个审批节点定义为审批角色，“自动匹配审批人”模式下，审批时会自动在申请人所在的部门匹配符合审批角色的用户并把审批任务发给他们，任意审批人通过审批即视为当前节点通过。如果找不到审批角色，会到父级部门继续匹配符合角色的用户，直到找到符合审批角色的用户才停止部门上溯。

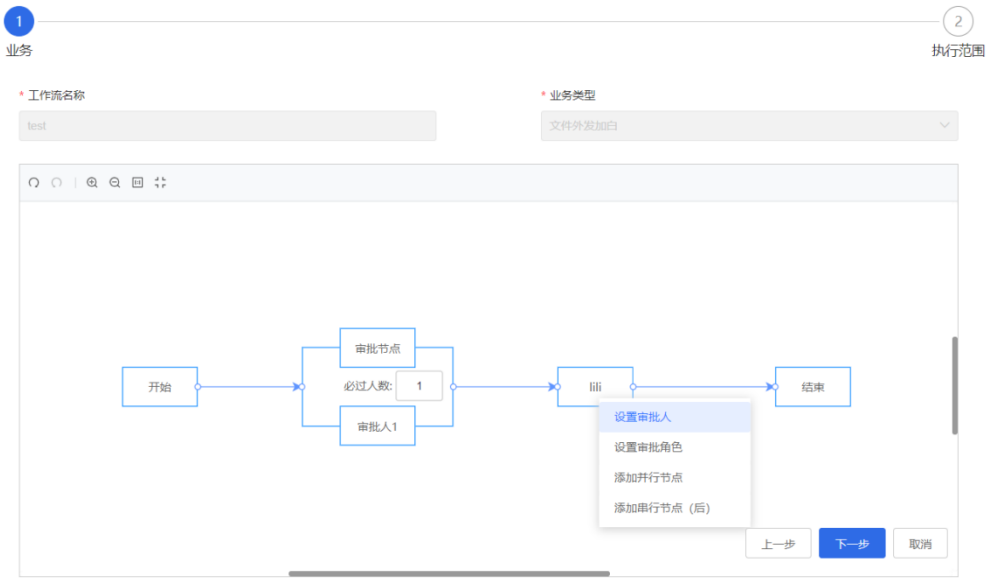
指定审批人模式：如果将一个审批节点定义为审批角色，“指定审批人”模式下，系统会将下个节点符合审批角色的审批人展示给当前节点，由当前节点用户指定下一个节点的审批用户。

审批角色无法匹配审批用户时，系统默认自动驳回工作流，可设置为自动通过。



第二步：定义审批节点

审批人：每一个审批节点可定义为具体的审批用户，也可以定义为审批角色。



第三步：定义执行范围

工作流可赋予用户组、用户和审批角色使用，同一个业务的多个工作流不能赋予同一维度的使用对象。优先级：用户>角色>用户组>上级用户组。

28.7.2. 个人中心

28.7.2.1. 当前用户的申请信息

展示当前用户的申请信息，对于没有进入实际审批（没有任何审批人进行审批操作）的审批流程，可以主动撤回。

28.7.2.2. 当前用户的审批信息

展示需要当前用户审批的工作流信息，并进行具体审批操作。

28.7.2.3. 自动审批

当前用户进行系统托管审批设置，可按业务进行自动通过和自动拒绝设置。

28.8. 个人中心

普通用户查看用户个人信息和修改密码。

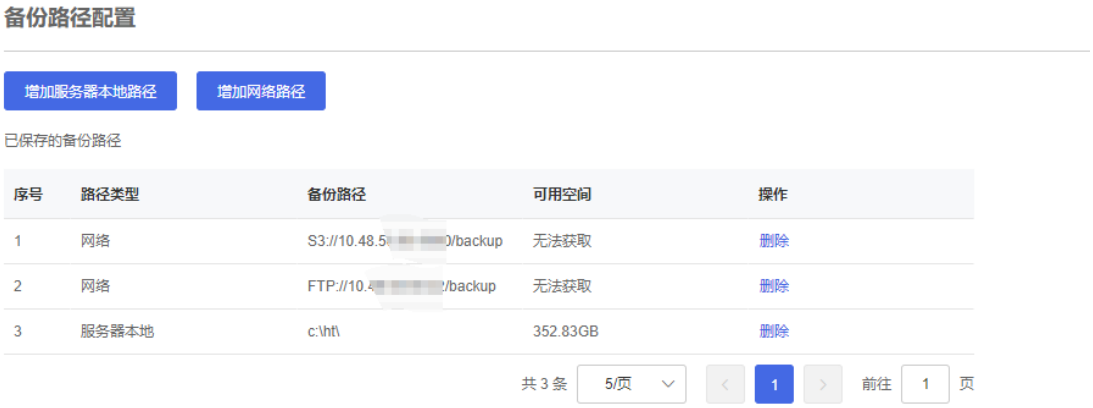
29. 运维管理

支持手动和自动定期备份管理系统所有的数据，包括基础数据、日志。（暂只支持 Windows 服务器单机部署、Linux 服务器单机部署、信创服务器单机部署的管理中心）

导航到“系统管理>运维管理”。

1） 打开“备份计划与配置”，配置备份路径。

i：点击“增加服务器本地路径”按钮



ii：弹窗“服务器本地备份路径”页面，在服务器本地路径输入框中，输入备份路径：

Windows 示例：D:\backup\

Linux 示例：/qaxbackup/backup/

iii:点击确定按钮（点击确认时校验输入的路径所在盘符是否存在，若不存在报错“本地路径未找到”，若盘符存在，之后的路径不存在，则新建路径）

备份路径可设置本地路径(本地路径的末尾也需要配置分隔符)，或网络路径。网络路径支持 FTP 和 S3。网络路径需要测试后连通性后，才可保存成功。

2） 手动备份。进入“系统管理>运维管理”主页面，点击立即备份。

可填写备份名称。选择需要备份的数据，基础数据为必选。此时预计的备份数据大小仅为压缩前的预估，实际备份文件大小会经过压缩后存储。

选择备份路径，可选择多个。说明：

a. 若路径在天擎安装磁盘上，需保证该磁盘剩余空间，在减去预估备份文件大小后，剩余空间占比>50%，防止管理中心因磁盘不足运行卡慢。

b. 若未选择服务器本地类型，由于需要暂存备份文件在天擎安装磁盘，仍需保证磁盘的剩余空间安全。

c. 服务器本地类型的路径最多只可设置 1 个。请确保所有路径的可用空间充足，否则，该备份路径将会备份失败。

d. 选择“网络”类型备份路径时，请考虑网络传输带宽和备份文件大小，避免传输时间较长，天擎停服时间过长。

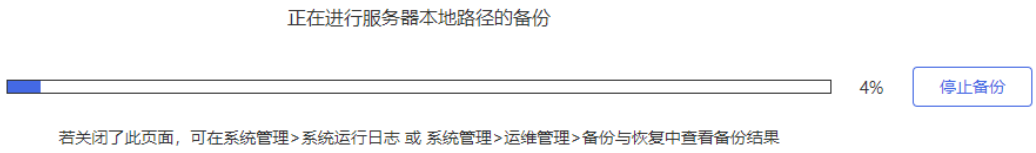
备份原理说明：

a. 首先，天擎停服，备份出一份文件在服务器本地路径中；若未设置本地路径，则会在天擎安装磁盘备份一份文件（暂存，用完即删）。

b. 然后，天擎服务启动，将此备份文件异步复制到网络类型的备份路径中。此时管理中心可用。

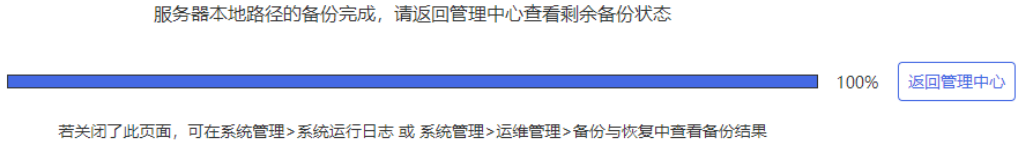
设置完成后，点击立即备份，确认后，将进行停服，执行备份，并跳转到备份进度页面。

停服阶段，备份进度页面将展示本地路径备份/暂存进度。若备份的文件较多，此环节耗时较长，请耐心等待。



点击停止备份，且确认后，将立即停止此次备份。

当本地备份/暂存完成后，将执行传输到网络备份路径上。此时管理中心将启动，备份的进度可去往管理中心查看。

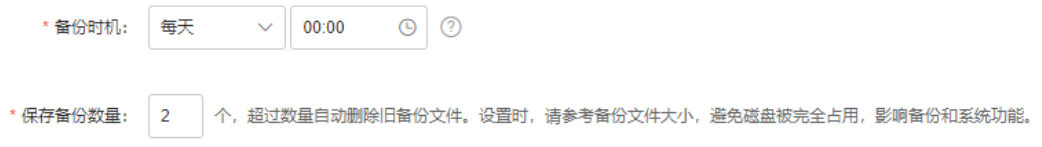


点击返回管理中心，可在管理中心>系统管理>运维管理中查看网络路径备份情况。

3） 备份计划，周期备份

在系统管理>运维管理>备份与恢复中，点击备份计划与配置。点击新建计划

配置方式同手动备份。有差异处：备份时机、保存备份数量。



配置完成后点击保存计划。跳转回列表后，勾选上“开启数据自动备份”，列表中的计划将按时执行。

4） 恢复

10.7.0.1000 及以上版本如果需要恢复，请联系厂商工作人员进行恢复。

请参考：https://kb.qianxin.com/detail/16f95940752

【注意】备份过程中将会暂停对外服务，即不能访问管理中心、不能管理终端。如果采用虚拟机部署，并且支持虚拟机镜像，推荐对虚拟机进行整体镜像快照备份。

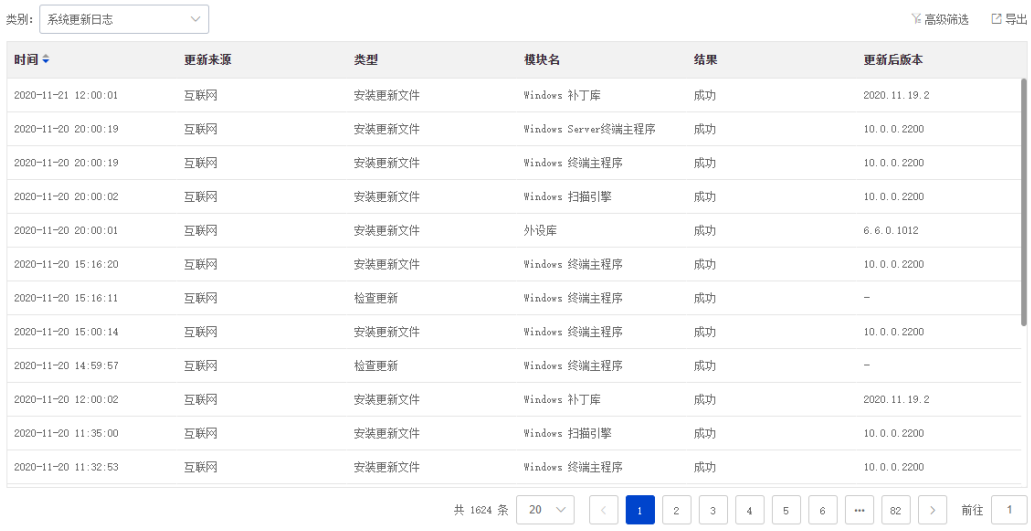
30. 系统日志

30.1. 系统运行日志

30.1.1. 系统更新日志

对管理中心后台进行的更新管理中支持的各主程序和各种库文件的自动更新检测行为

的记录，包括时间、更新来源、类型、模块名、更新结果以及更新后版本，同时支持筛选和导出。



30.2. 系统运行日志

记录管理中心后台进行的非更新动作的行为比如与第三方的联动处置等，包括开始时间、结束时间、类型/事件、描述和操作，同时支持筛选和导出。

30.3. 管理员日志

记录管理员在管理中心的登录操作行为，包括操作时间、管理员、来源 IP、操作级别、类型/事件以及详细信息，同时支持筛选和导出。

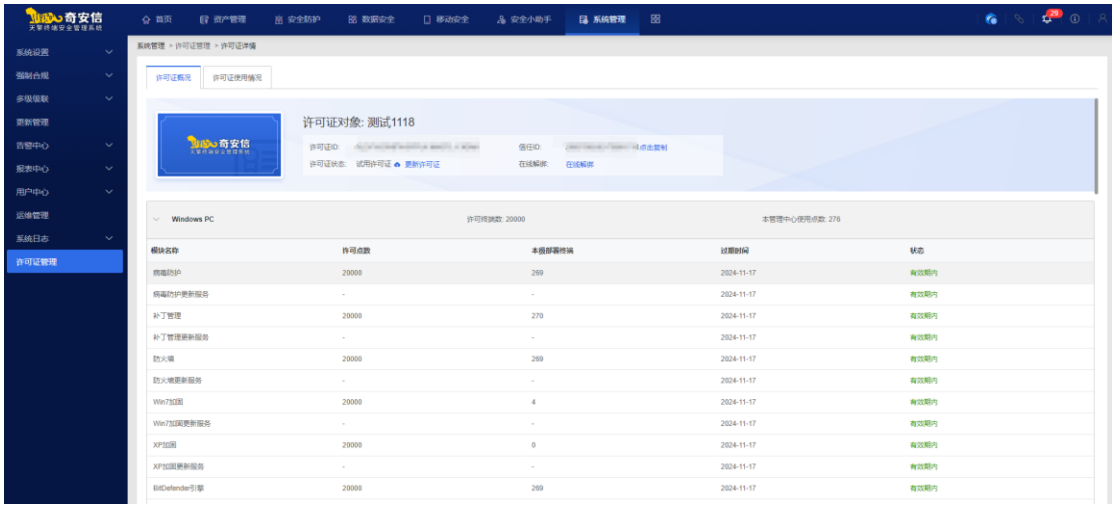
31. 许可证管理

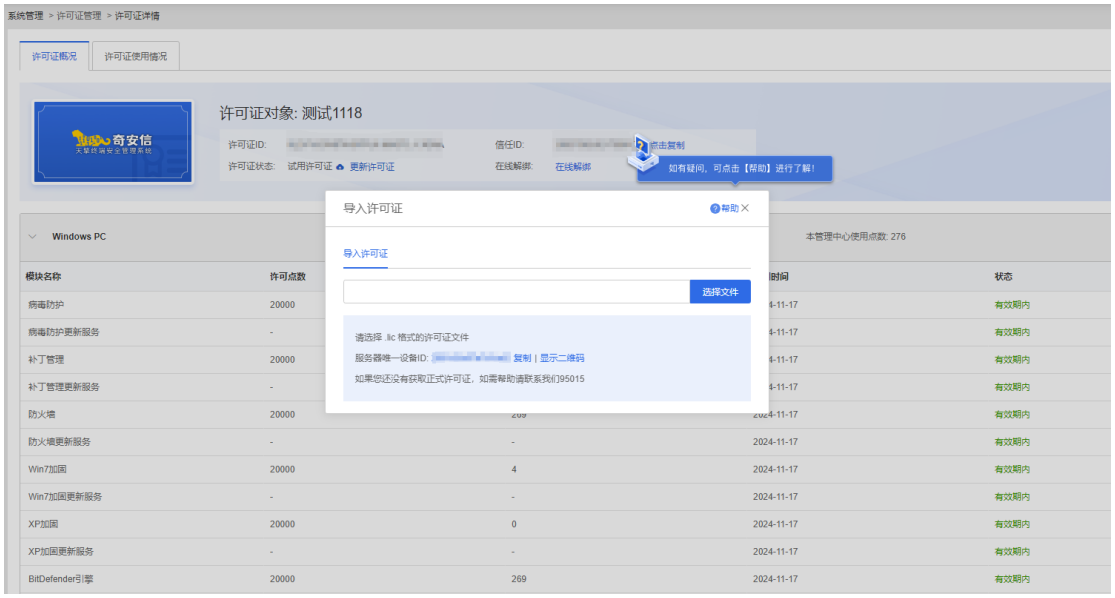
31.1. 许可证概况

许可证概况主要提供许可证使用情况的展现，包括操作系统平台、过期时间、许可点

数及部署情况等信息，并支持更换许可证。

入口：系统管理>许可证管理>许可证概况。





31.2. 许可证使用情况

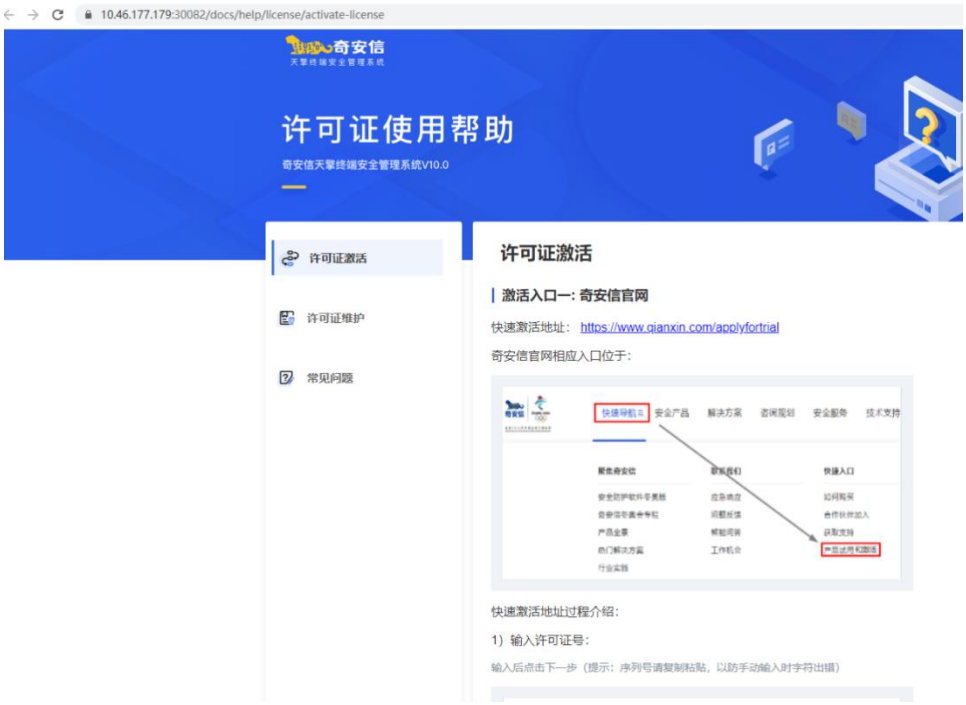
许可证使用情况主要提供购买模块在终端侧的使用情况的查看，支持分组搜索和查看、自定义展示列及导出。

入口：系统管理>许可证管理>许可证使用情况。

31.3. 许可证帮助文档

许可证帮助文档主要提供了许可证的使用方法和常见问题的处理方法

入口：系统管理>许可证管理>更新许可证>帮助。



31.4. 更新许可证注意事项

新增或者更新 EDR 授权后,需要手动重启 EDR 相关服务，请参考 KB119952 。

【注意】许可证更新时，如果模块有变化，则会提示模块变化情况。如果模块有减少，则会提示模块的变化以及导入后可能的变化。确定导入后则可能自动触发终端策略更新并卸载减少的模块。如果有重要模块减少，建议对相关模块的配置做好提前处理，防止模块卸载带来的副作用。