奇安信天擎终端安全管理系统 EDR 先锋版

V10.0R6(10.6.2.1000)

管理员手册

● 版权声明

目录

1. 天擎 EDR 先锋版简介

1.1. 产品简介

奇安信天擎终端安全管理系统 EDR 先锋版（简称“天擎 EDR 先锋版”）是实效与轻量化结合的一体化终端安全解决方案；轻松部署，免维护；集成全球领先的自研+三方多引擎病毒查杀、漏洞防护、高级威胁防御引擎；拥有实用的终端管控、软件管理、主机防火墙、弹窗防护、文件分发等安全工具；私有化部署方式保障政企客户终端安全数据自主掌控。轻量化天擎 EDR 先锋版，将帮助中小规模的政企客户轻松构建终端安全能力。

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。

- **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。

- **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。

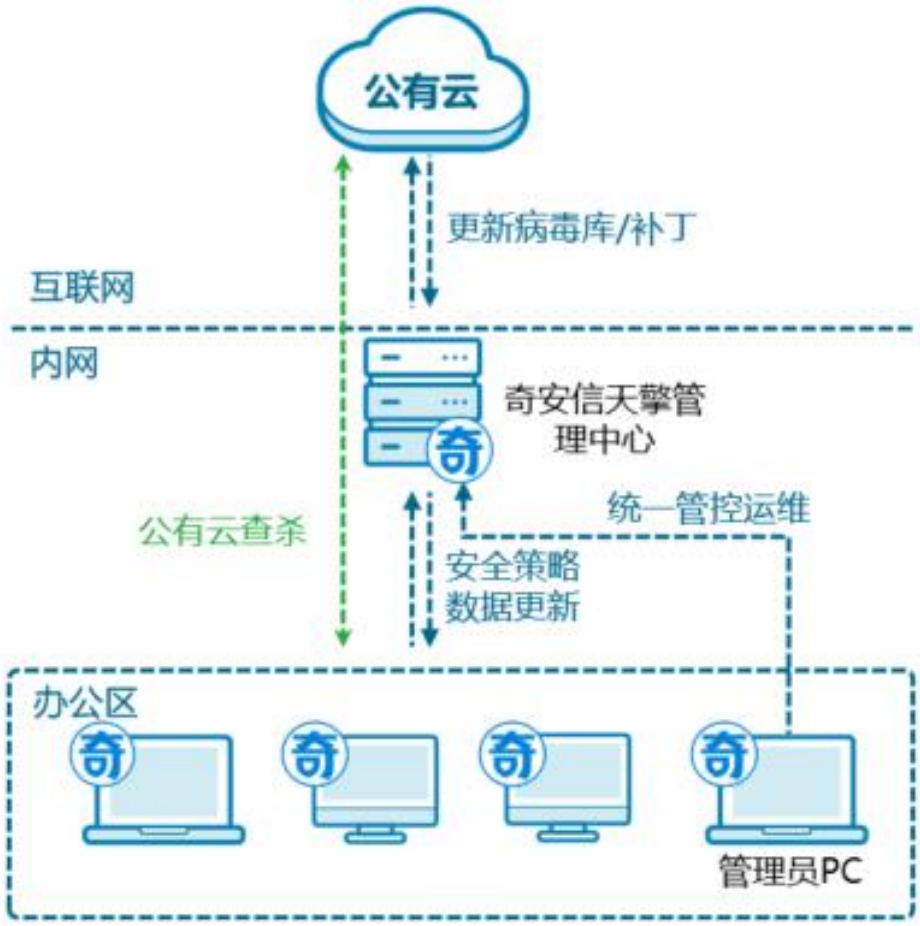
1.3. 典型部署场景

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。

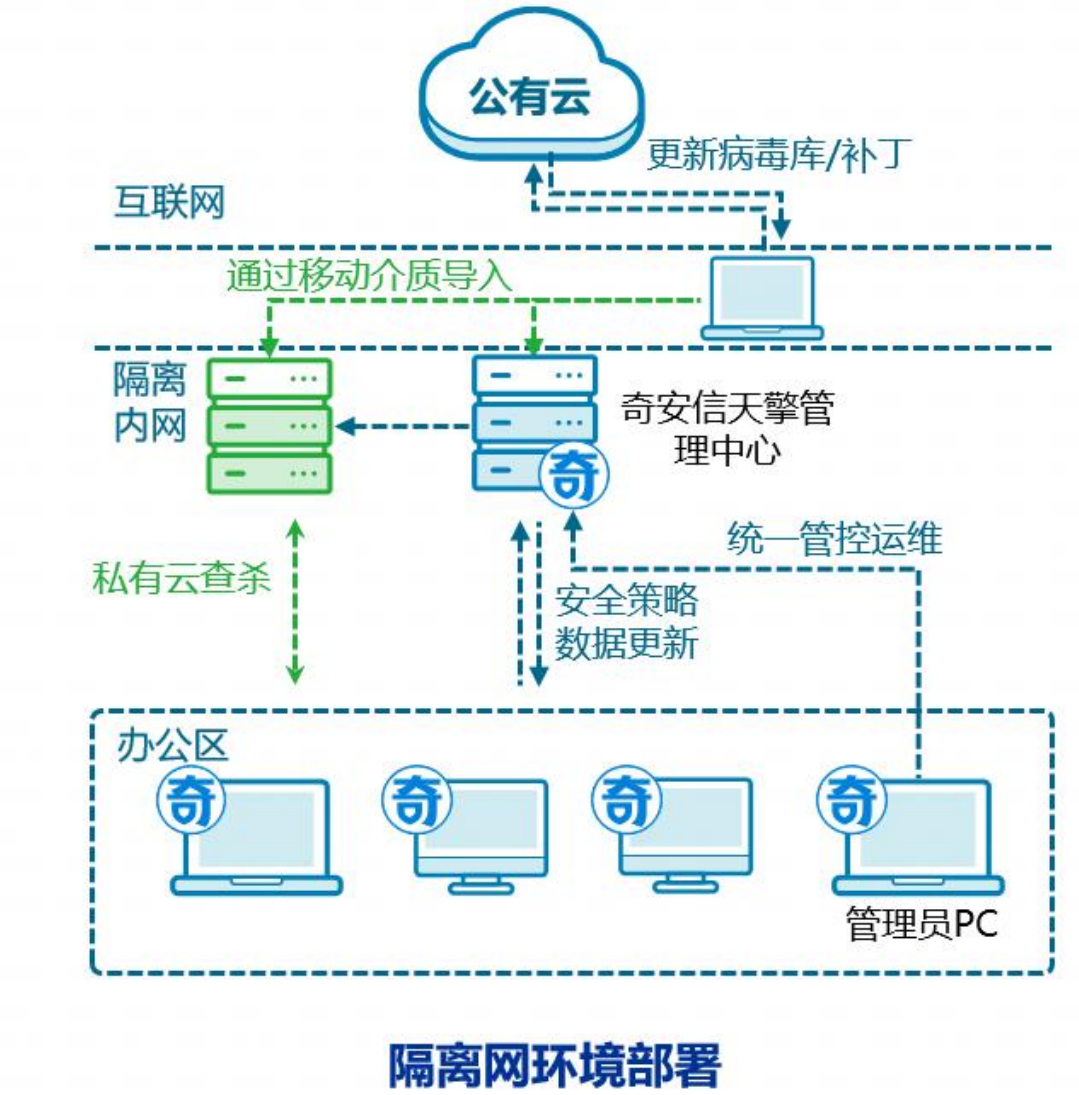
终端可连接云端进行云查杀，极大地提高终端病毒的查杀能力。

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。

1.4. 典型部署形态

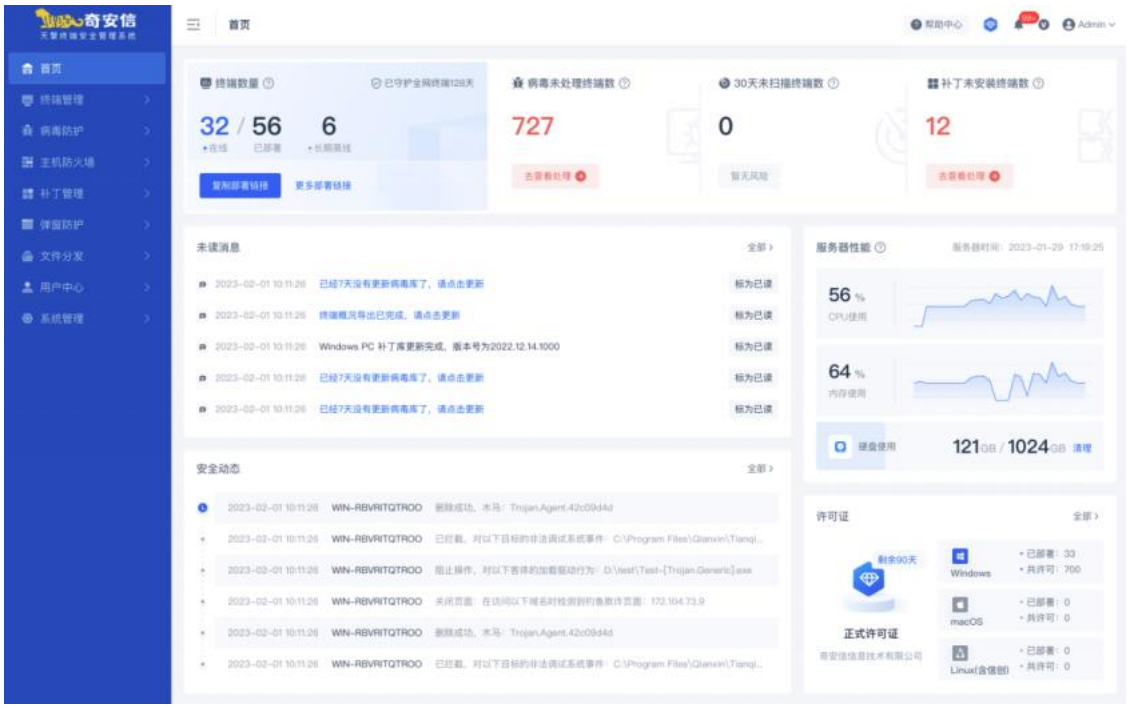
1.4.1. 单机部署

单机部署是指在单台服务器上完成天擎 EDR 先锋版的部署，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。

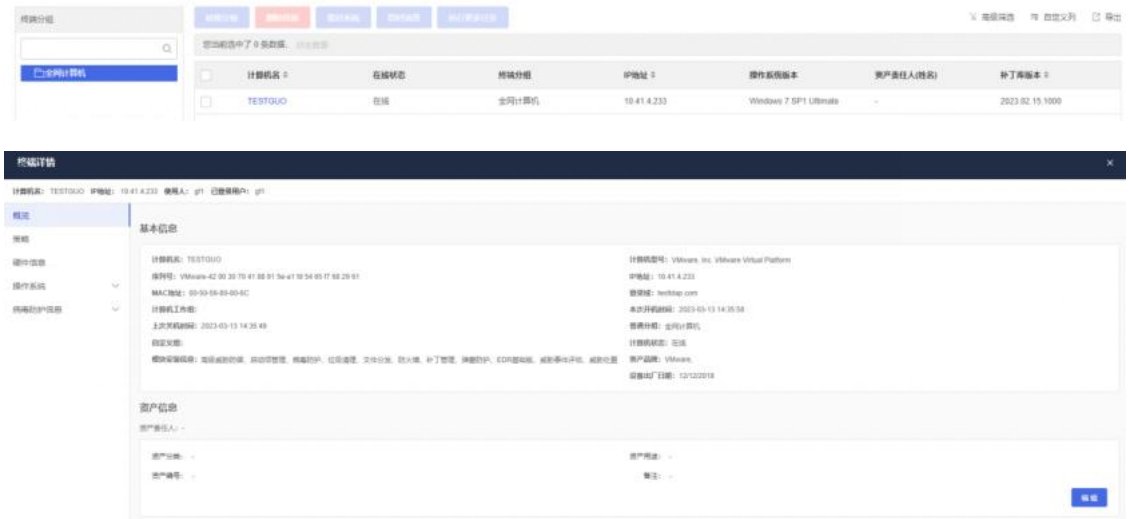
2. 终端管理

2.1. 终端概况

在首页可概览终端数量，点击数字，可跳转到“终端概况”详细页面可查看终端详情和对终端进行安全管理。



管理和查看终端的概况，并支持高级筛选和单终端查看详情。



A.概览。查看终端的基本信息（计算机名、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。

B.策略。查看终端当前的策略配置信息。

C.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、硬盘序列号等）。

D.操作系统。包括查看系统信息、账号信息。

E.查看病毒防护设置。

F.点击终端图标可直接对终端绑定资产责任人、查询退出和卸载客户端的验证码、配置单终端任务、收集客户端排障日志操作。

部分字段说明：

通信 IP 地址：指服务器视角看见的终端 IP 地址。

IP 地址：与服务器通信的网卡的 IP 地址。

2.2. 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。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、计算机名、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”。

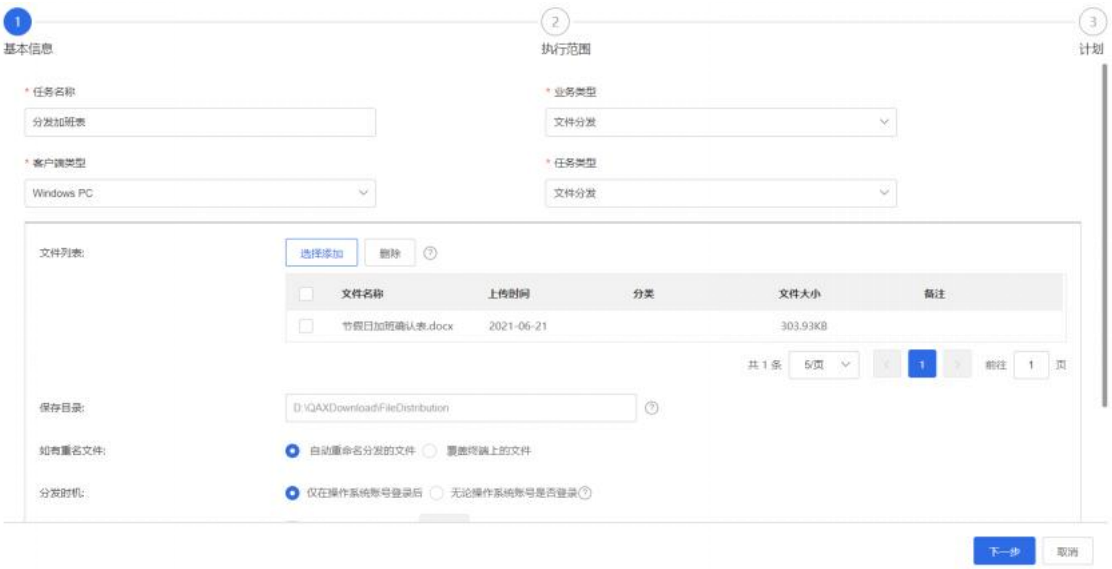
点击更多操作，可以为选择的分组同步组织架构、复制组织架构以及自动分组、调整分组顺序、导入导出分组。

2.3. 终端任务

2.3.1. 分发任务

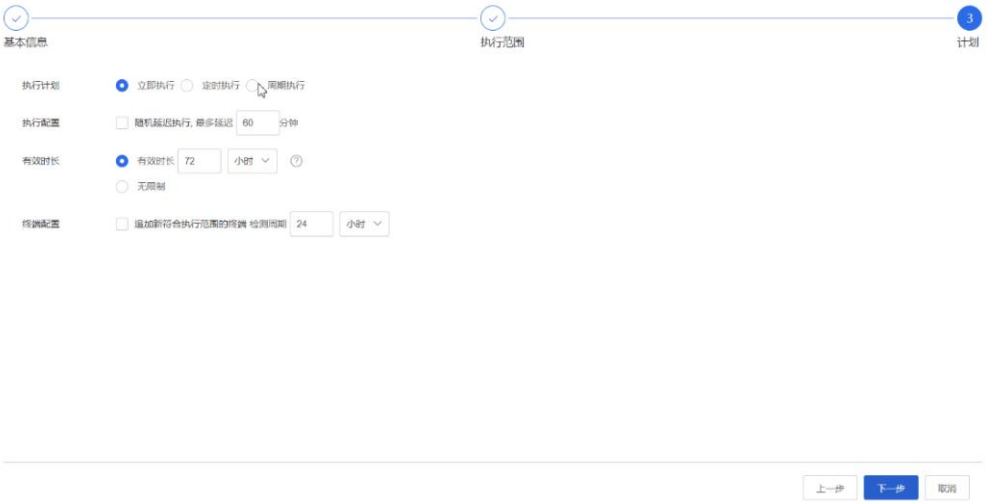
导航到"终端管理>终端任务"，新建和编辑终端任务分为 3 步骤，配置基本信息、执行范围、计划。

A. 基本信息，配置任务的名称、具体内容。



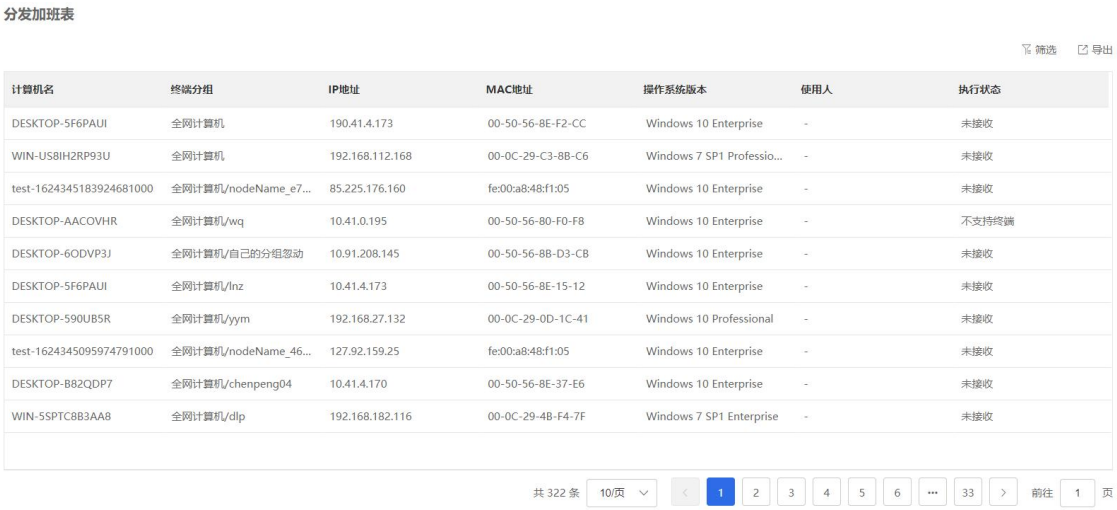
B. 执行范围，配置任务的执行的终端范围。

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。



2.3.2. 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。

2.3.3. 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。

2.3.4. 任务设置

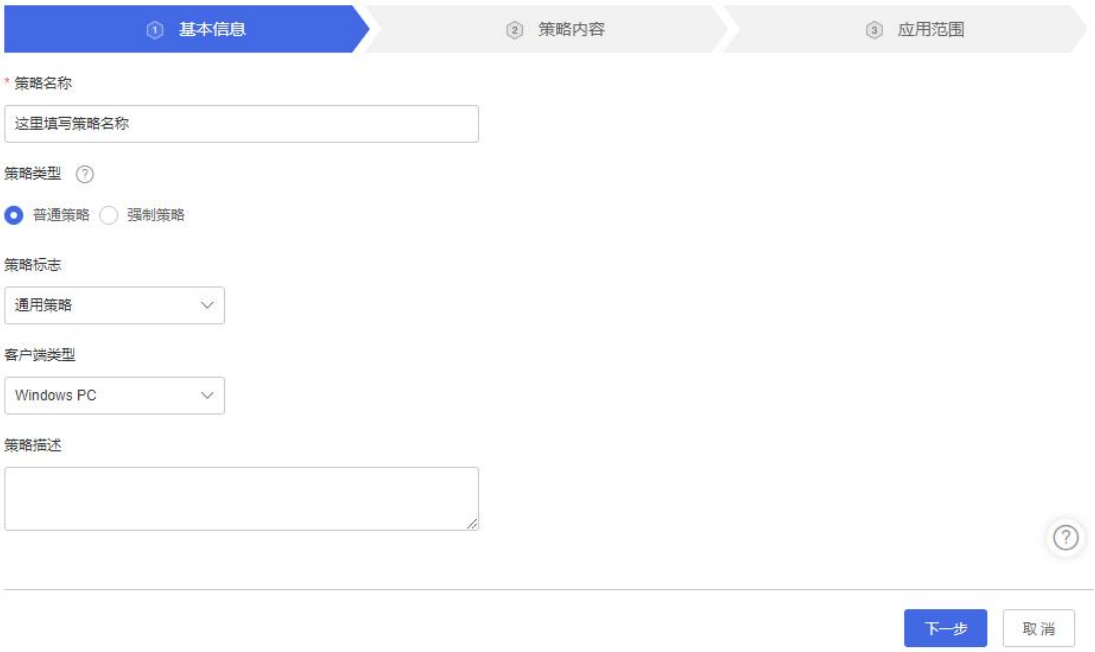
可设置自动清理已完成的历史任务和限制任务数量。将默认限制周期任务的最大运行数量为 20 个，限制追加终端的任务的最大数量为 50 个，以避免无限制的新增任务将会导致服务器的资源耗尽。

2.4. 基础策略

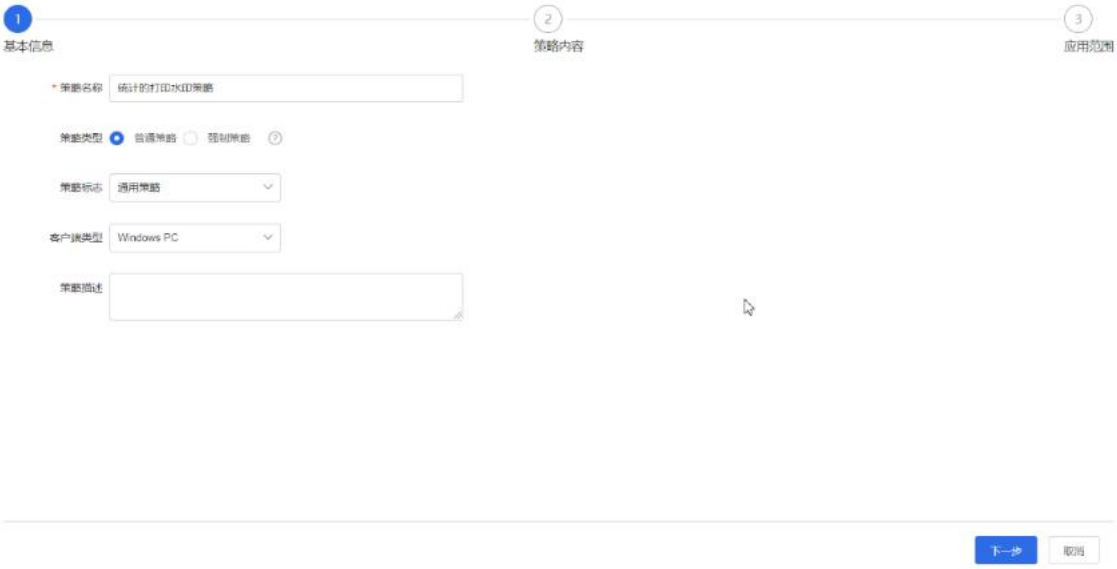
策略是配置项的集合，用于将企业的安全管理制度转换为终端可执行的指令。根据安全业务特性，由 N 个配置项组成。分为终端策略和用户策略，两者的分发方式一致。

导航到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

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。

策略标志

- 策略的标签，用于策略管理中方便筛选。

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”。

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。

策略管理原则

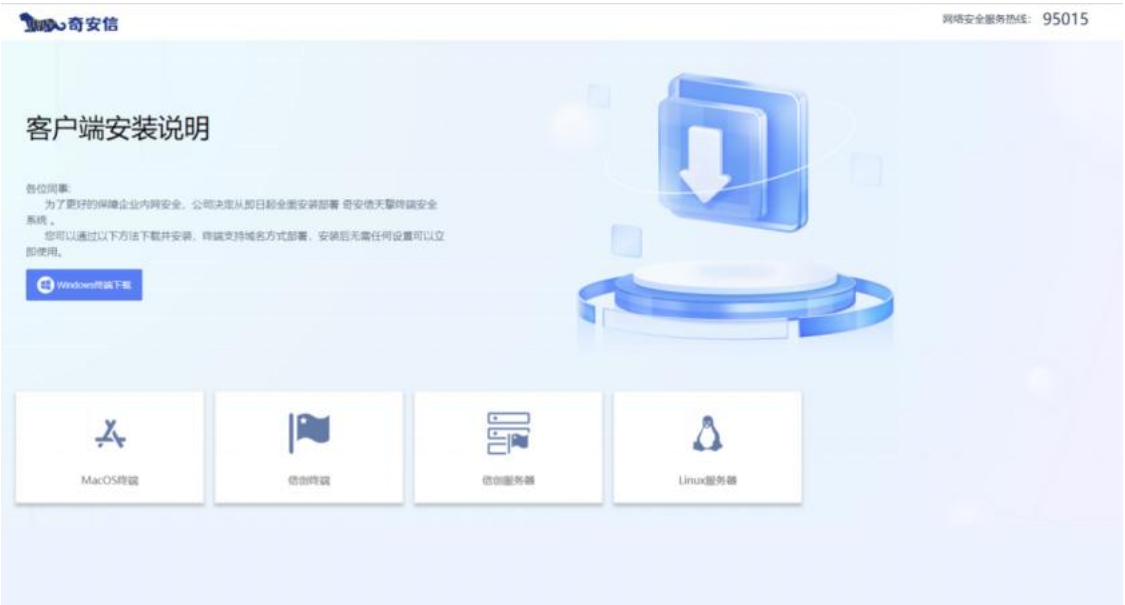
- 如果需要策略不会被下级覆盖则必须将配置项设为”强制策略”或者不分配给下级管理员创建策略的权限。
- 如果需要刷新（覆盖）下级组的策略则必须将新建”强制策略”覆盖已有策略。

2.5. 终端部署

2.5.1. 在线部署

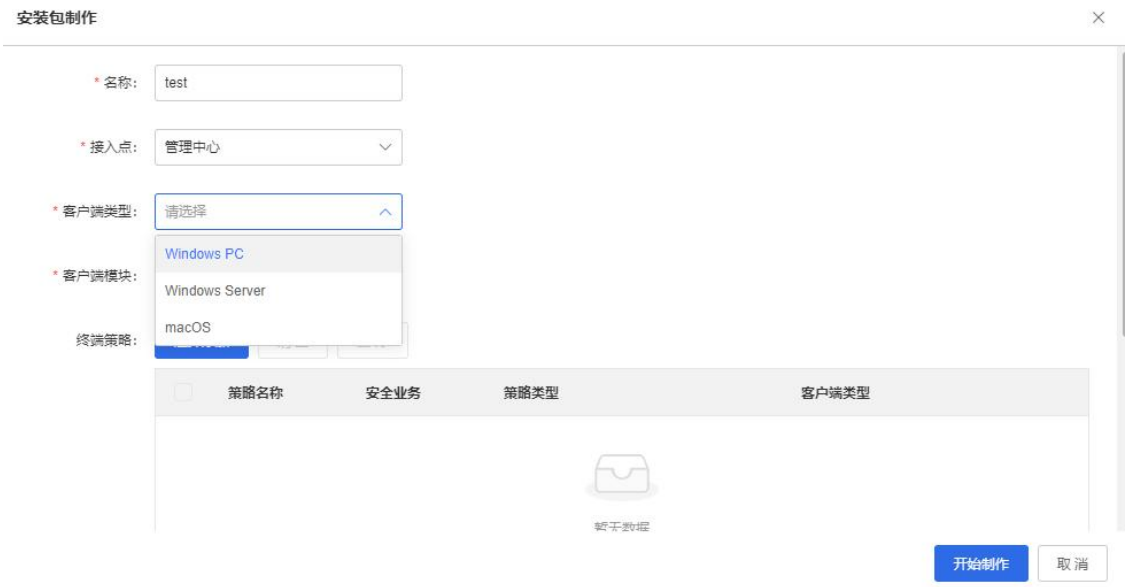
通过复制分享在线部署链接，发送给终端，终端打开链接下载客户端安装进行安装。

客户端下载页面。



2.5.2. 一体化安装包

管理员可通过添加一体化安装包，制作离线安装包，将安装包线下发送给终端，终端进行安装。



2.6. 终端日志

2.6.1. 终端部署日志

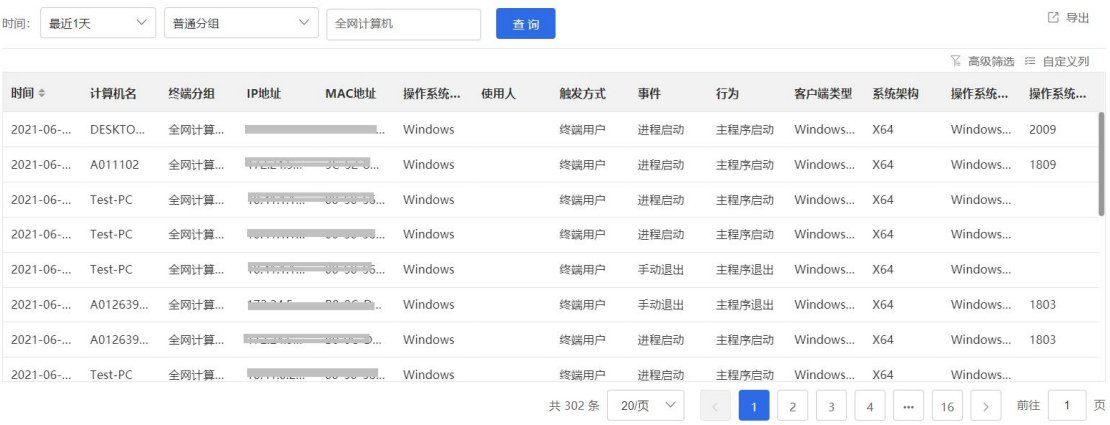
记录该管理中心下的终端的部署信息，包括模块的安装和卸载，支持筛选和导出，支持展示的字段自定义。

2.6.2. 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。

2.6.3. 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。

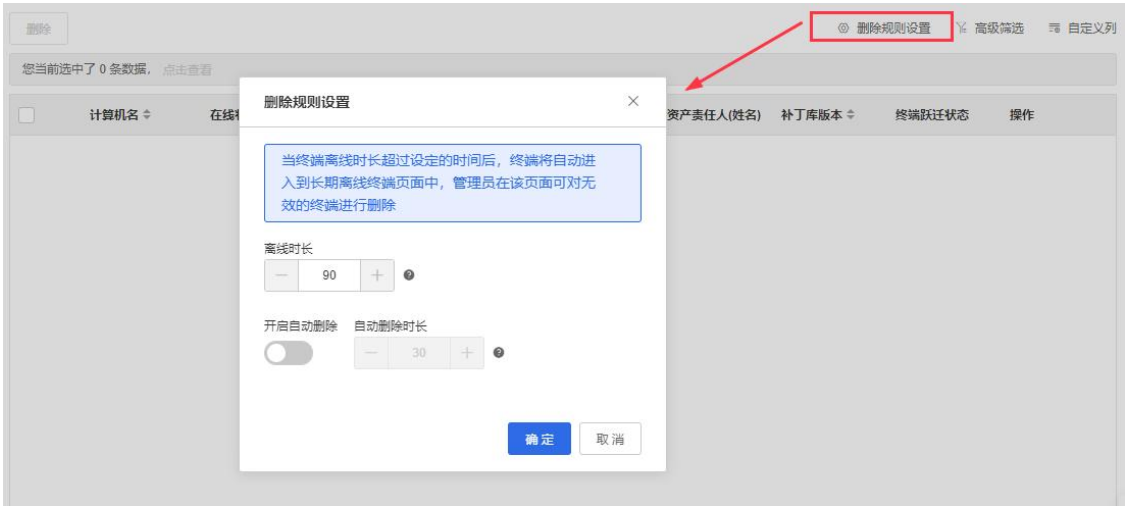


2.6.4. 终端排障日志

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）。

2.7. 长期离线终端

可查看长期离线的终端状况，并可设置判断长期的规则；可设置自动删除规则。



2.8. 资产统计

按终端分组对终端进行数量统计，展示在线率。

2.9. 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。

可操作导入/导出资产登记。

需在系统管理>通用设置中添加资产类别。

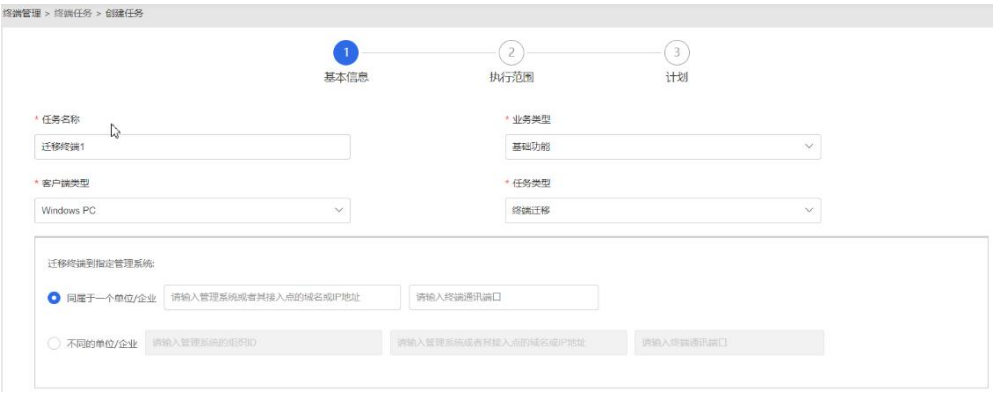
之后，通过基础策略>基本设置 中配置开启资产登记。

2.10. 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：管理中心>终端管理>终端任务。



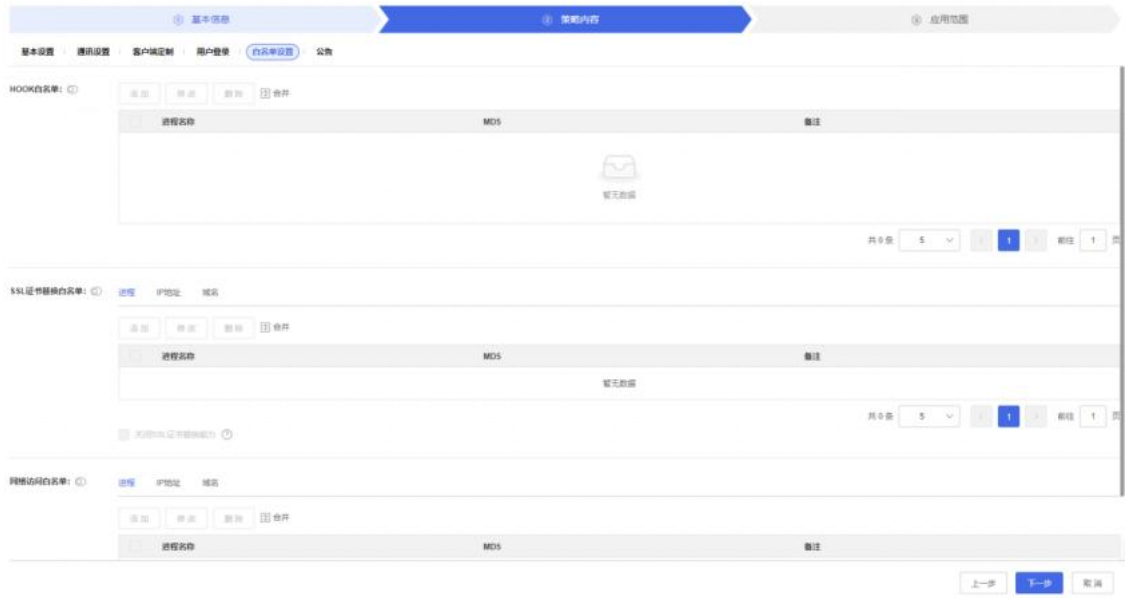
2.11. 自动切换服务器

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天擎 EDR 管理中心中。

入口：管理中心>终端管理>基础策略>通讯设置。

2.12. 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。



2.12.1. HOOK 白名单

操作入口：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。

2.12.2. SSL 证书替换白名单

操作入口：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。

2.12.3. 网络访问白名单

操作入口：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。

2.13. 典型场景

2.13.1. 如何手动删除已卸载的终端

天擎 EDR 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天擎 EDR，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。

2.13.2. 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（参考中资产登记部分系统管理>通用设置>资产登记），然后导航到"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。

3. 病毒防护

3.1. 基本概念

3.1.1. 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。

3.1.2. 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。

3.1.3. 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。

3.1.4. 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。

3.1.5. 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。

3.1.6. 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、键盘记录防护、系统账号防护）、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（勒索软件防护）、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）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。

- 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漏洞攻击。

- 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。

3.2. 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病毒任务）。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。

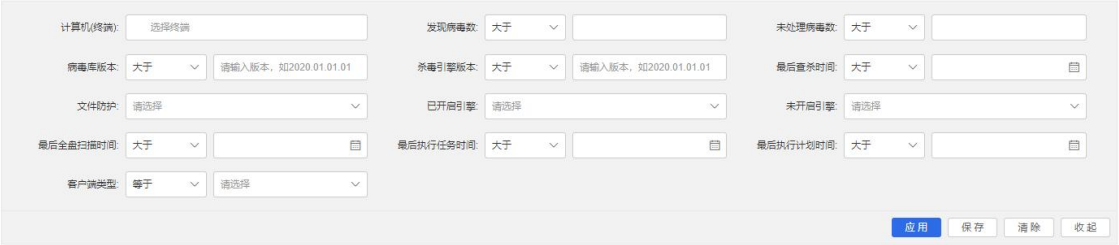
共发现病毒数：所选终端分组中的终端上检出的病毒次数总和。

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。

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、客户端类型来筛选目标终端。



3.3. 病毒防护策略

功能入口：管理中心>病毒防护>策略管理。管理中心提供了默认设置。管理员可根据企业自身的网络环境、业务特点和管理制度进行微调。

3.3.1. 通用设置

3.3.1.1. 检出类型增强设置

PUA（Potentially Unwanted Application）类型，是指潜在不需要的程序。破解、静默安装、弹广告等行为本身不破坏电脑系统，仅包含此类行为的程序不属于病毒。勾选该项可以阻止包含上述行为的流氓软件。

3.3.1.2. 云查杀设置

随着病毒制作机的发展，一方面，受限于客户端资源，本地病毒特征库无法无限扩大；另一方面，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挨打的痛点，杀毒行业发展出云查杀技术。

云查杀首先是一种世界观，把电脑程序文件分为白、黑、未知（灰），任何新病毒样本会落在“未知”这个逻辑区域。杀毒软件把电脑资源重点投放在防范“未知”上，可以做到打击未知病毒的同时保持低误报率。由于电脑上大部分软件是白程序，所以云查杀技术扫描更快。

用户可以根据网络环境选择云查杀模式，产品默认是直连公有云。

- 通过服务器代理云查

  客户端向管理中心发送云查请求；管理中心的云查服务组件做缓存处理：未命中缓存则转发到公有云，并返回客户端查询结果；命中缓存直接返回缓存数据。

  适合网络环境：不允许客户端连接公网，仅允许管理中心访问公网。云查请求需要开通的域名、端口请查阅部署手册。

  使用该模式前，建议点击【连接测试】确认管理中心云查请求网路畅通。否则，客户端发起的云查请求会因为积压而消耗服务器内存资源，造成服务器卡慢。

  当客户端与管理中心失去联系、处于漫游状态，会自动尝试连接公有云进行云查杀。在低配置服务器上（内核低于 8 核或者内存低于 16G），该模式被禁用。

- 直连公有云

  客户端直接向奇安信公有云发送云查请求。

  适合网络环境：允许客户端连接公网，不允许管理中心访问公网。

使用该模式前，建议评估出口带宽是否匹配终端规模，每千点终端 20M(Bit)。客户端在本地有云查数据缓存，以节省带宽。

- 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。

适合网络环境：不允许客户端连接公网、不允许管理中心访问公网。

奇安信私有云杀毒管理系统需要单独够买，部署后在隔离网中可以享受到云查杀的技术优势：白的快、黑的全、灰的防得严。

使用该模式，需要填写私有云 IP、端口、APP key、AppSecret。后两项来自私有云的系统设置-连接设置-应用凭证,如下图所示

- 隔离网不连云

客户端不会发起云查请求。

适合网络环境：不允许客户端连接公网、不允许管理中心访问公网、未采购私有云。

在该模式下，客户端关闭云查请求，但不会影响管理中心的黑白名单功能。

3.3.1.3. 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。

为了避免客户端上的隔离区数据一直占据磁盘空间，默认设置隔离区文件最大保留的天数为 180 天。客户端每天定时检查隔离区文件，删除超期数据。

3.3.1.4. 信任区设置

信任区是全局黑白名单的补充，支持添加文件全路径、文件路径、扩展名三种信任数据。

文件全路径：该文件被跳过；适用用于路径固定且经常变化的程序文件加白。

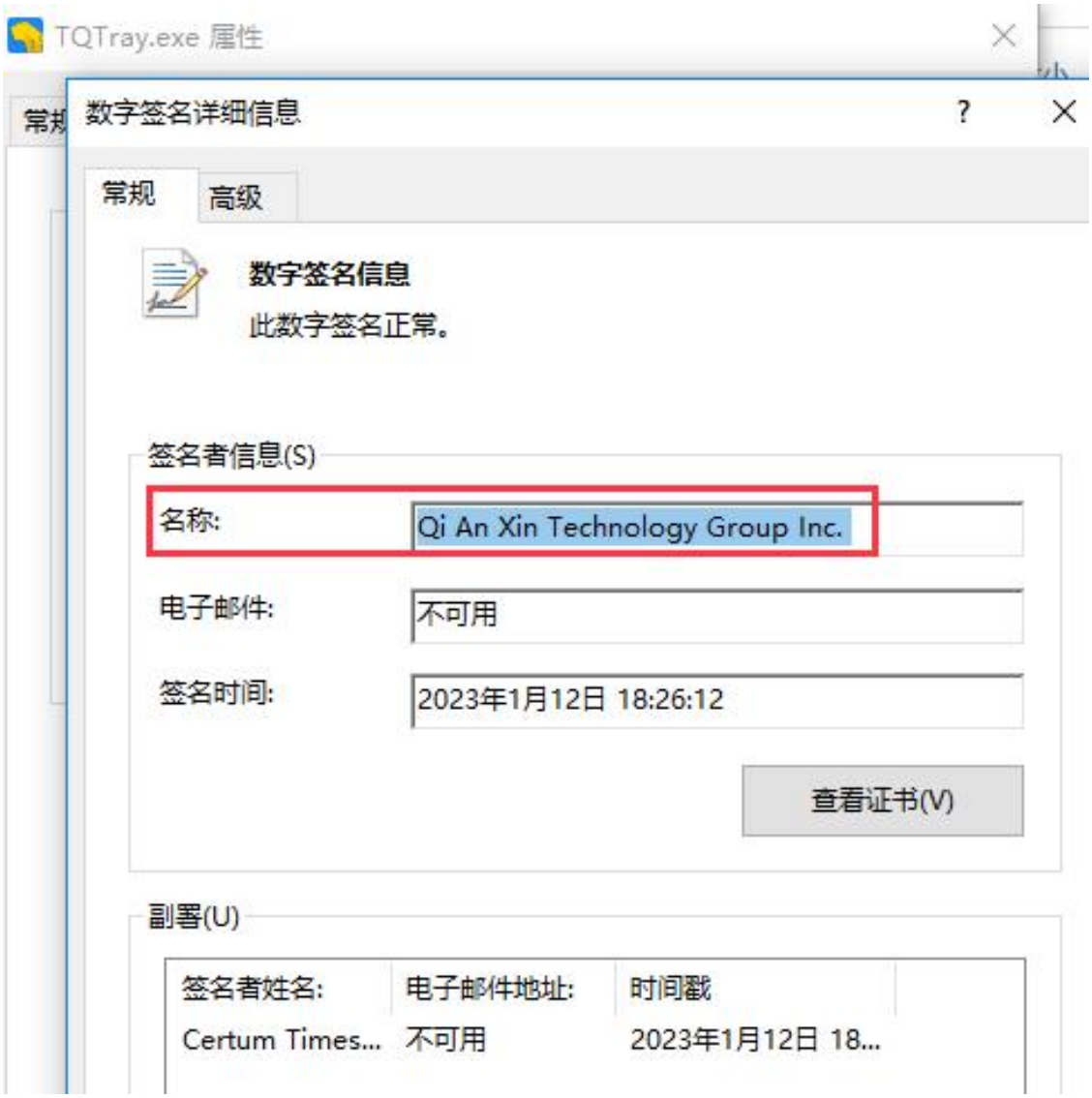
文件路径：位于该路径下面的文件及其子路径全部被跳过；适用于安装路径固定，文件特别多的软件加白。

扩展名：该扩展名的全部文件被跳过；适用于加白自研软件的数据库系统。

3.3.1.5. 文件数字签名设置

将文件的数字签名名称拉黑或者加白。推荐使用该功能加白无安全隐患的自研软件。

获取文件数字签名名称方法如图：



有效的数字签名是：有受信任 CA 证书机构颁发的签名证书。

3.3.1.6. 终端用户安全操作控制

为了满足企业对终端用户的严格管理需求，提供一键勾选按钮，避免产生安全管理盲区。勾选后从四个维度来限制终端用户操作：

- 禁止终端用户从隔离区恢复文件
- 禁止终端用户管理路径/文件白名单
- 禁止终端用户管理扩展白名单
- 扫描时不允许终端用户暂停、停止扫描任务

由于该功能会增加网络运维管理工作，所以，对于 Windows PC 客户端，默认不开启；对于 Windows Server 客户端，默认开启。

3.3.1.7. 弹窗模式

- 智能模式：

  病毒扫描，按照病毒处理方式设置。

  实时防护，按照病毒处理方式设置；在自动处置后，会弹出拦截结果通知窗口。

  主防防御,按照病毒处理方式设置；在自动处置后，会弹出拦截结果通知窗口。

- 免打扰模式：在发现风险时候，按照默认操作进行程序自动操作，并记录日志，不弹出提示框。

  该模式与病毒处理方式的关系如下：

  病毒扫描，病毒处理方式的询问用户模式被修正。

  实时防护，病毒处理方式的询问用户模式被修正；在自动处置后，不会弹出拦截结果通知窗口。

  病毒扫描，病毒处理方式的询问用户模式被修正；在自动处置后，不会弹出拦截结果通知窗口。

3.3.2. 病毒扫描设置

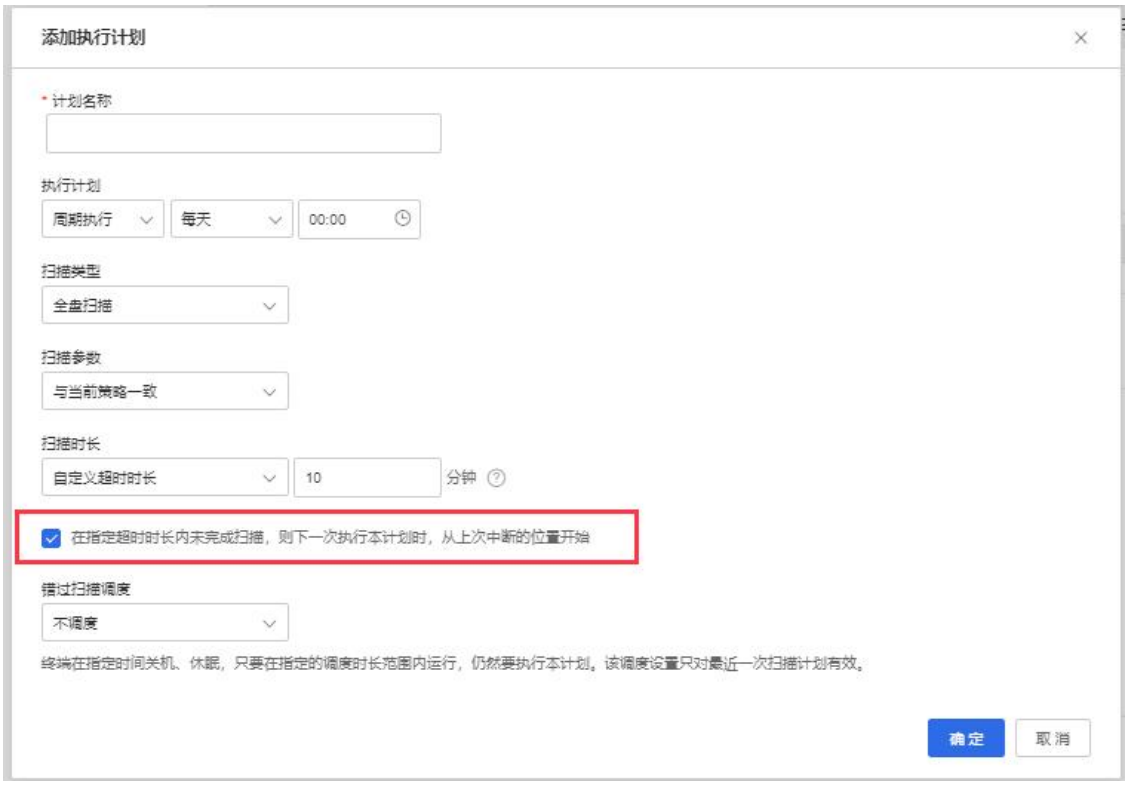
3.3.2.1. 定时查杀

定时查杀用来配置终端定时启动病毒查杀。按照每天、每周、每月指定时间来执行扫描动作。支持设置开机执行扫描。支持三种扫描类型：全盘、快速、自定义。

因为策略中的定时查杀下发到客户端，所以，漫游、脱缰状态的客户端只要处于开机状态，也会定时执行扫描任务。这种场景，周期扫描任务做不到。

针对企业客户，提供两种管理功能：

（一）断点续扫：把全盘扫描任务分为几个时间段来完成。



适用场景：将扫描任务定在员工休息时段，但无法用一个时段完成一次完整的全盘扫描。

配置方法：扫描时长选择 自定义超时时间，比如设置为 60 分钟（中午休息 1 小时）；勾选“在指定超时时长内未完成扫描，则下一次执行本计划时，从上次中断的位置开始进行扫描”

（二）错过扫描调度：提升定时扫描完成率。

适用场景：总有部分客户端在规定的扫描时间处于关机状态。

配置方法：设置【错误扫描调度】中的自定义时长，在该时间范围内，客户端开机后仍然会执行扫描计划。

3.3.2.2. 病毒处理方式

三种处理方式：由程序自动处理、询问用户和不处理病毒仅上报日志。

程序自动处理：在扫描结束后，终端检出病毒会自动清除；扫描、实时防护、主动防御的误报率，相对而言，前二者都很低；即使误报，还可以从隔离区恢复数据，因为，程序自动处理是病毒扫描的默认处理方式。

询问用户：在扫描结束后，终端检出病毒会弹框，由用户决定是否处理；

不处理病毒仅上报日志：终端检出病毒后，不进行处理，但会记录日志，处理结果为不处理病毒仅上报日志。适用场景：首次部署，用这种方式全盘扫描，先收集检出数据进行收白处理，确保没有误报业务系统软件。常见问题：在部署阶段完成后，要记得修改回来。

3.3.2.3. 扫描文件范围

支持设置扫描所有文件、仅扫描程序及文档文件。默认是后者。

- 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。

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：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。

扫描网络映射驱动器：将在全盘扫描时候进入网络映射驱动器进行扫描。

扫描压缩包设置：可以选择是否扫描压缩包。可以设置扫描压缩包的层数和大小；层数，是指压缩包中的压缩包文件，不是压缩包中的文件目录。

3.3.2.4. 扫描限制

设置终端病毒扫描时候的资源占用。

- 不限制：终端进行病毒扫描时候，不限制 CPU 占用。
- 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 25%（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。

3.3.2.5. 深度查杀

功能特点:该模式会锁定系统全部文件、路径的修改。

适用场景：终端扫描病毒发现感染型和顽固型病毒时触发。抑制全盘感染型病毒在查过程中扩散。这种模式会造成文件无法保存，所以在使用前关闭打开的文档。

3.3.3. 实时防护

3.3.3.1. 病毒处理方式

三种处理方式：由程序自动处理、询问用户和不处理病毒仅上报日志。

程序自动处理：在扫描结束后，终端检出病毒会自动清除；扫描、实时防护、主动防御的误报率，相对而言，前二者都很低；即使误报，还可以从隔离区恢复数据，因为，程序自动处理是病毒扫描的默认处理方式。如果勾选了弹框的智能模式，会把拦截结果通知用户。

询问用户：在扫描结束后，终端检出病毒会弹框，由用户决定是否处理；如果勾选了弹框的免打扰模式，不会弹框，由程序自动处理。

不处理病毒仅上报日志：终端检出病毒后，不进行处理，但会记录日志，处理结果为不处理病毒仅上报日志。适用场景：首次部署，用这种方式，先收集检出数据进行收白处理，确保没有误报业务系统软件。常见问题：在部署阶段完成后，要记得修改回来。

3.3.3.2. 实时防护

实时防护功能开关。对于老旧终端，可以增加开机延迟加载。

实时防护拦截处理是异步机制。该功能不会阻塞电脑软件运行。

防护的操作类型是文件的创建/修改。例如：右键查看一个病毒文件的属性，不会触发检出；把一个病毒文件复制到其他目录，则会触发拦截；把病毒文件写入其他电脑的共享目录，如果未开启局域网文件防护，不会触发拦截；

3.3.3.3. 防护文件范围

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。

3.3.3.4. 防护资源占用

不限制：不限制使用 CPU 和磁盘 IO 资源；

均衡型：限制使用 CPU 和磁盘 IO 资源平均低于 50%

低资源：限制使用 CPU 和磁盘 IO 资源平均低于 25%

3.3.4. 主动防御

3.3.4.1. 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。

3.3.4.2. 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。

3.3.4.3. 入口防护

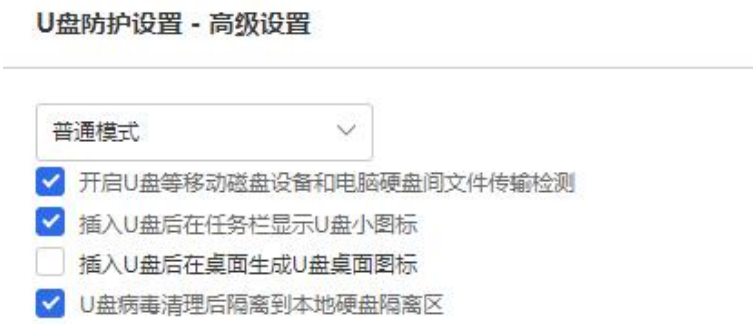
入口防护是针对终端可能从外界进入文件的环节进行防护。包括：U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护。

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。

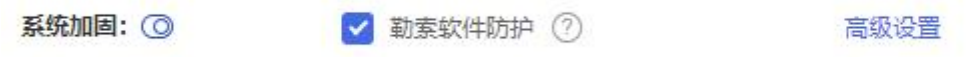


3.3.4.4. 系统加固

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。

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。



高级设置。

3.3.4.5. 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。
- 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。

3.3.5. 高级威胁防御

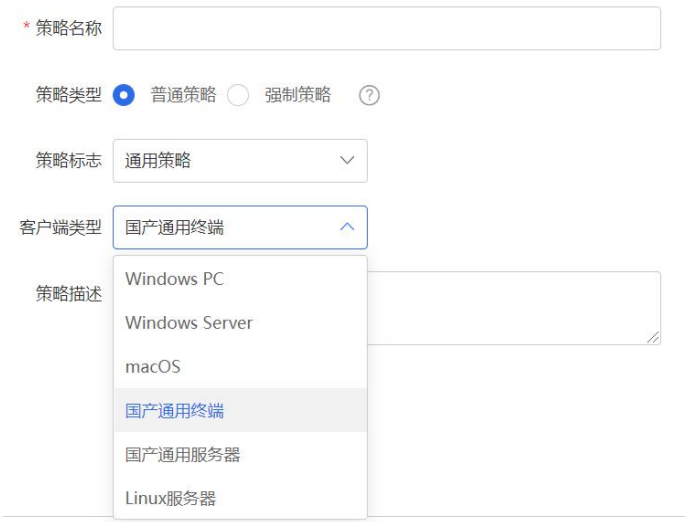
高级威胁防御 Tab 页面，包含无文件攻击防护、文档攻击防护、横移渗透攻击防护、和内存攻击防护。支持 Windows PC 和 Windows Server 两种终端类型。

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。

3.3.6. 国产终端病毒防护策略

功能说明：设置 Linux 服务器终端、国产通用终端、国产通用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。

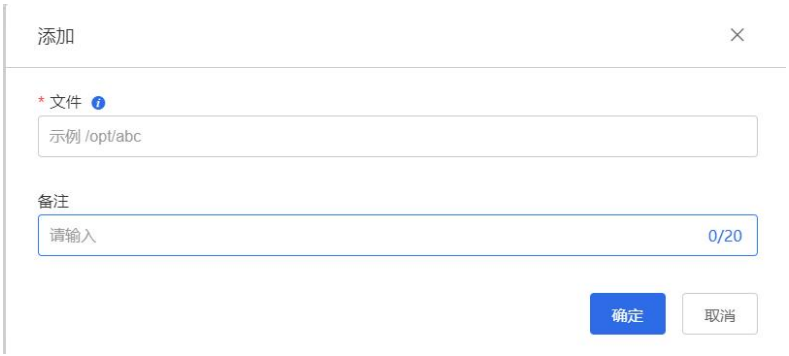
功能入口：病毒防护>策略管理>客户端类型（选择 Linux 服务器终端、国产通用终端、国产通用服务器终端）。



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：

添加信任区请参考提示信息：



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。

实时防护包含实时防护、防护文件类型。

主动防御包含系统防护、入口防护。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。

定时查杀包含，定时查杀，支持周期执行，不支持开机执行。

3.4. 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、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。

导出有三种方式图片、CSV、EXCEL。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。

3.4.1. 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。

3.4.2. 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。

3.4.3. 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。

3.4.4. 网页安全防护日志

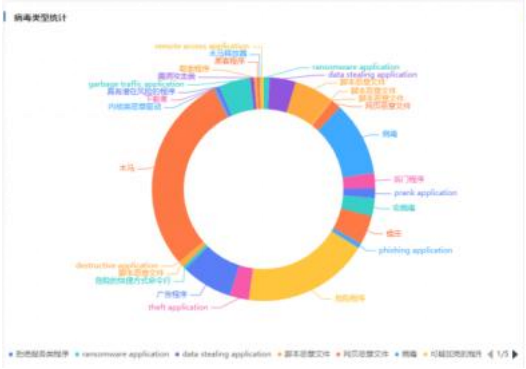
网页安全防护日志是网页安全防护功能的发现威胁结果展示。展示扫描终端的信息，网页安全防护相关信息：访问的 IP、访问的域名、防护动作、防护详情等信息。

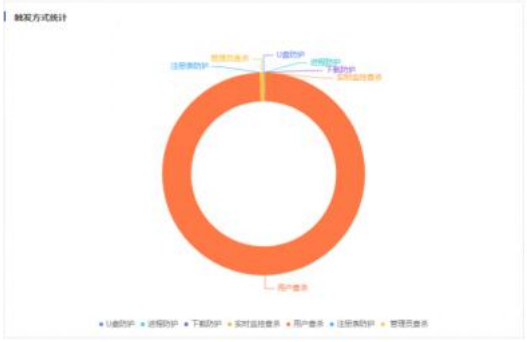
3.5. 病毒报表

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、按分组统计。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。

3.5.1. 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，传播最多病毒数 TOP10，受感染最多分组 TOP10 等报表。





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

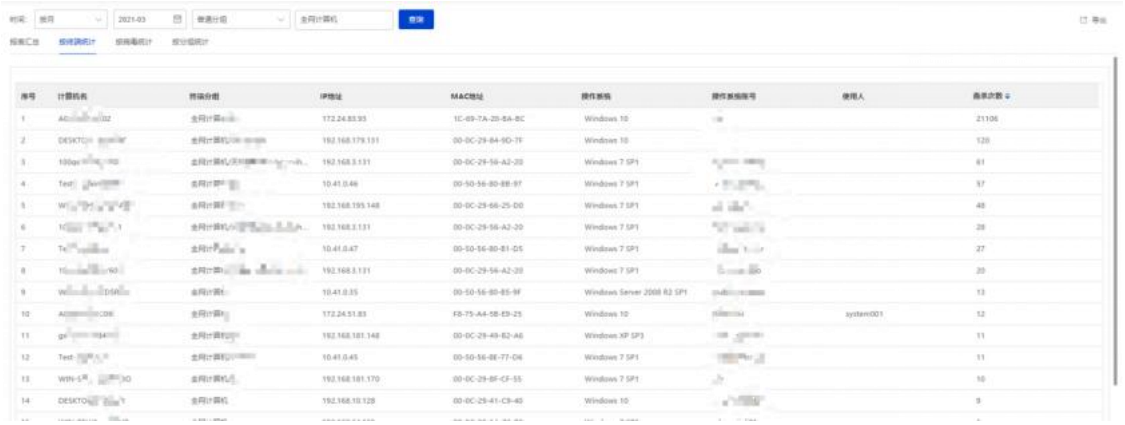
序号	病毒名	病毒类型	感染终端数
1	PUA.Signature.Risk	危险程序	20
2	Trojan.Win.Agent.d7c0fd1d	木马	20
3	Risk/CRS.Autorun.Generic	危险程序	19
4	Trojan.Generic	木马	16
5	QDE.v1.0.1LAA2CKP13.1IBYBZ	木马	14
6	Backdoor.Win32.Wabot.8	后门程序	14
7	Win32/Trojan.4cb	木马	14
8	Virus.Win32.Viking.Q	病毒	14
9	QDE.v1.0.SN594DZHQ.2HWMN	木马	13
10	QDE.v1.0.1LA9SKNMNK.8F	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(未知)	24	292
3	gx	9	21212
4		5	161
5	hhhhstest	3	92
6		3	40

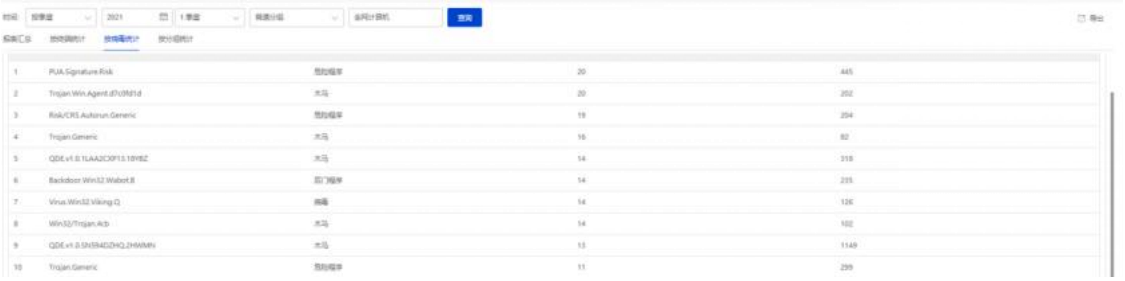
3.5.2. 按终端统计

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。



3.5.3. 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。



3.5.4. 按分组统计

该功能提供根据终端分组，统计感染终端数、查杀次数，可以通过筛选、排序对数据进行查看。

3.6. 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。

3.6.1. 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。

3.6.2. 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，从十一个病毒的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。

3.7. 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。

3.8. 日常运维管理

3.8.1. 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。

3.8.2. 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。

3.8.3. 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。

3.8.4. 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。

3.8.5. 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。

3.8.6. 处理紧急问题

3.8.6.1. 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。

3.8.6.1.1. 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。

3.8.6.1.2. 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。

3.8.6.1.3. 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。

3.8.6.2. 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。

3.8.6.2.1. 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。

3.8.6.2.2. 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。

3.8.6.2.3. 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。

3.8.6.2.4. 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。

3.8.6.2.5. 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。

3.9. 终端病毒任务

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、查杀未处理等任务。并对扫描结果进行分析和处理，是保障内网安全的基础。

3.9.1. 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。

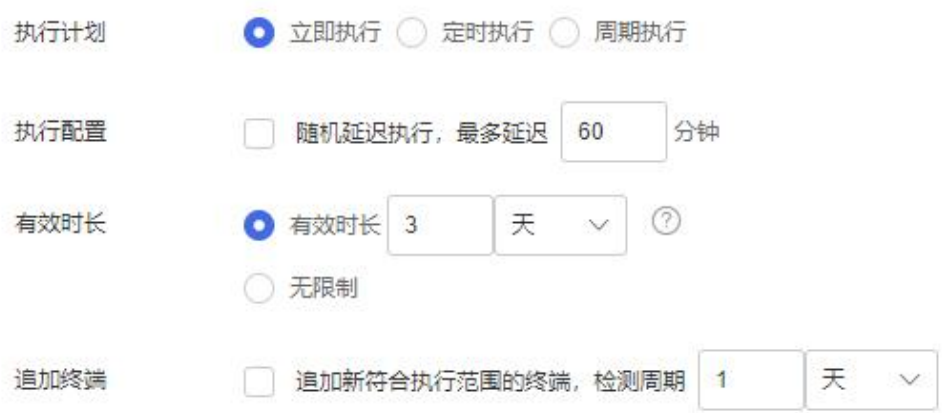
点击下一步，即完成任务的分发。终端执行时间内接收到任务后，将在任务有效期内开始任务。

3.9.2. 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。

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任务。

3.9.3. 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。

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。完成策略配置后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任务。

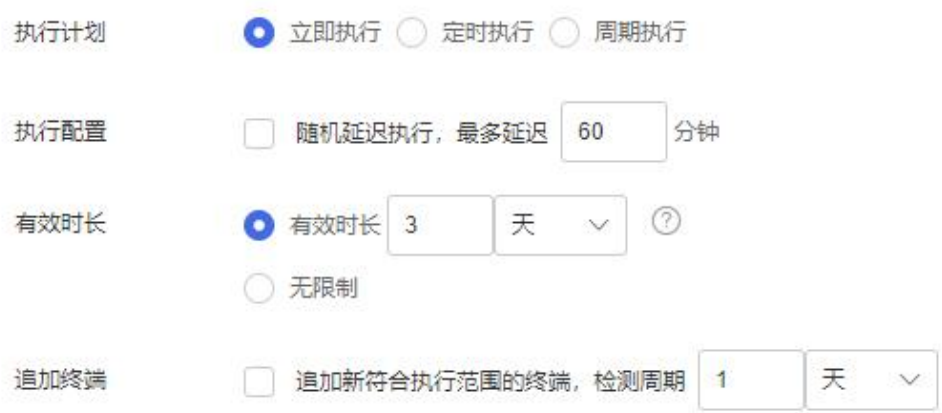
3.9.4. 文件专杀

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。

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任务。

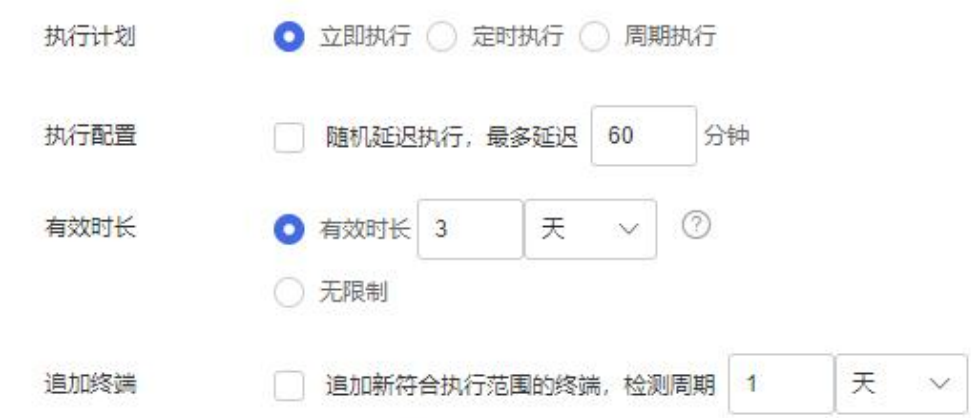
3.9.5. 隔离区恢复

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。

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任务。

3.9.6. 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。

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任务。

3.10. 典型场景

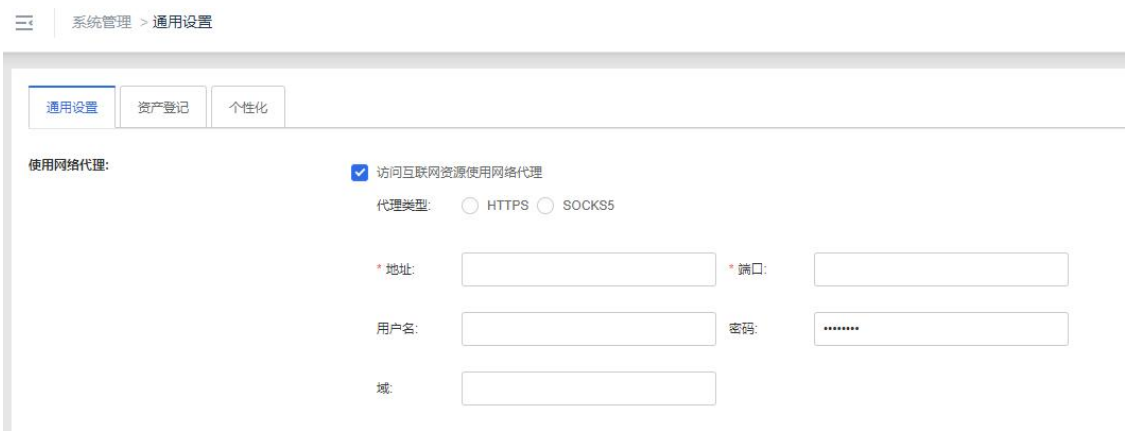
3.10.1. 适配网络环境

3.10.1.1. 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，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。



3.10.1.2. 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”。

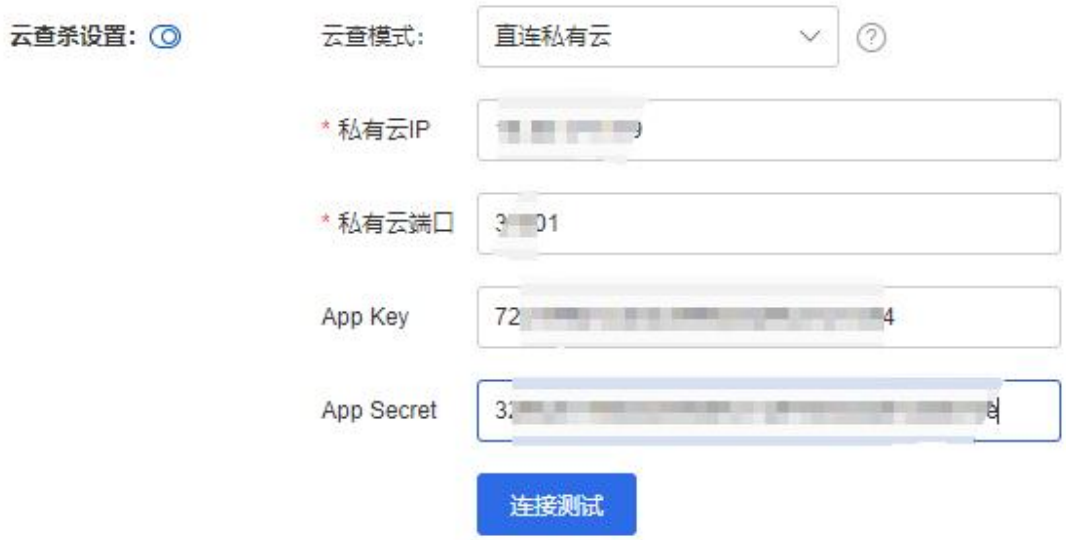
3.10.1.3. 隔离网

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特征库升级到最新。

3.10.1.4. 有私有云时

购置了私有云，需要把云查杀模式调整为“直连私有云”，并且设置四项私有云的信息，如下图



4. 主机防火墙

4.1. 基本概念

4.1.1. 主机防火墙

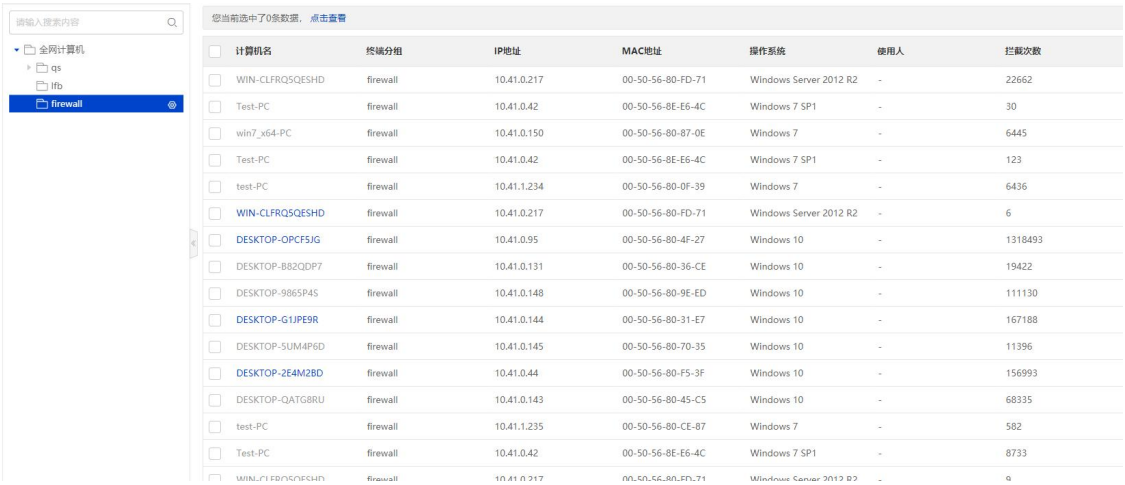
主机防火墙（Host Firewall），是针对终端上的基于网络五元组信息对主机网络流入流出进行防护的模块。通过配置和管理防火墙放行或拦截规则，来增强阻断或放行终端的异常网络请求、保障终端和内网的安全的能力。

4.1.2. 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。

4.2. 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。



4.3. 防火墙策略管理

主机防火墙策略设置，位于管理中心>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。

4.3.1. 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。

4.3.2. 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）、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。

防火墙规则支持 IPv6。

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

4.3.3. 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。在国产终端中，开启接管会停用系统防火墙。

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。

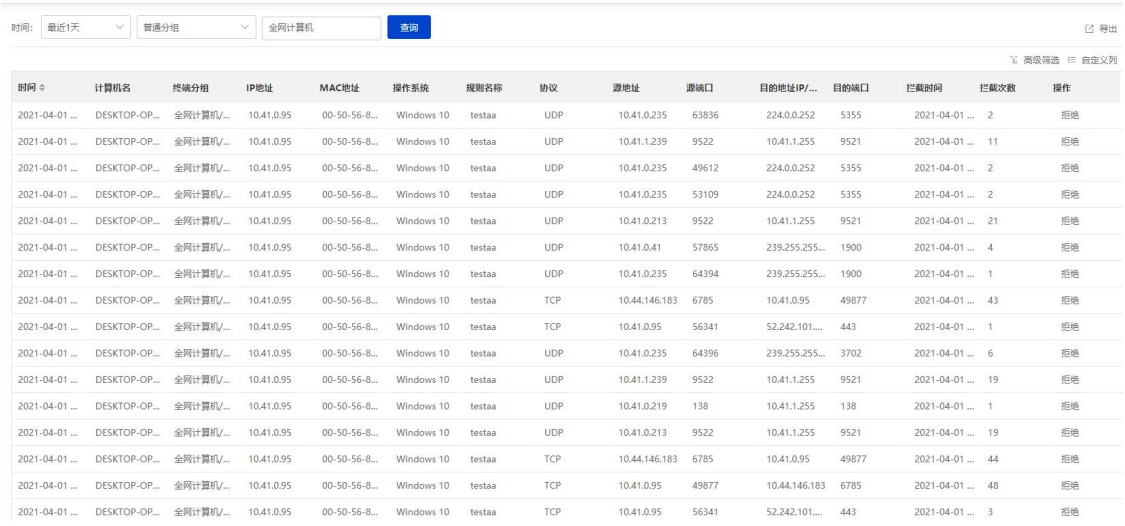
4.3.4. 日志上报配置

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。

4.4. 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。

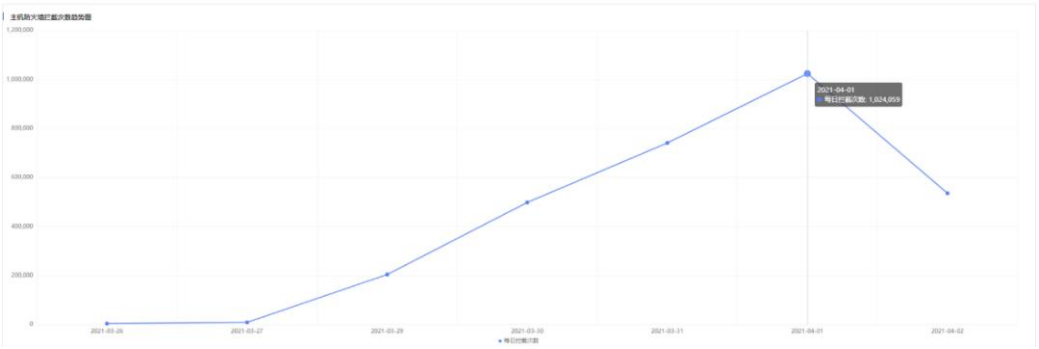


4.5. 防火墙报表

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。

4.5.1. 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。

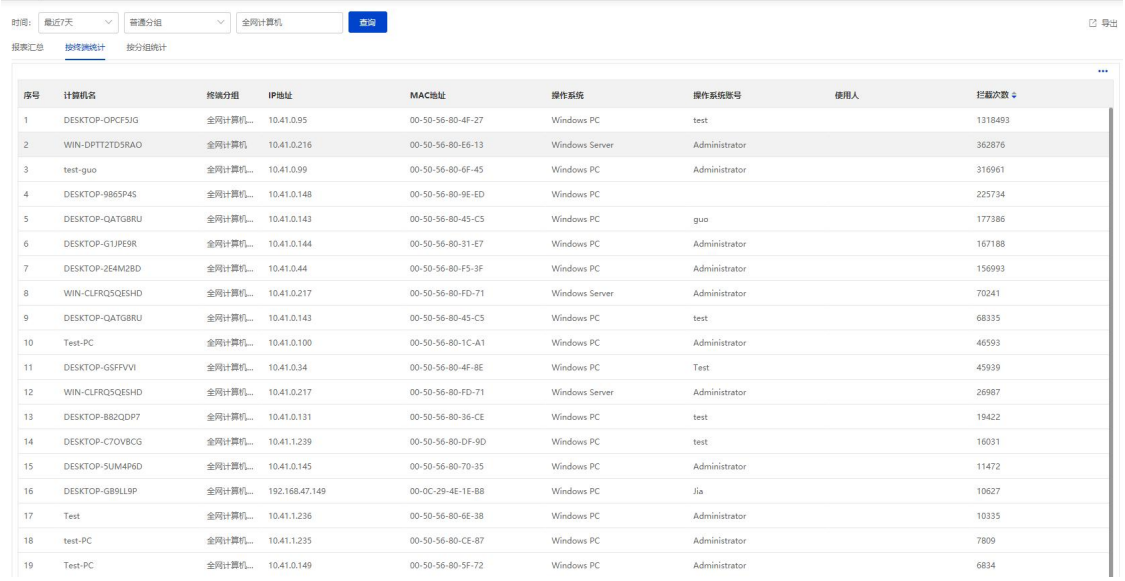


拦截终端排行榜TOP10

序号	计算机名	终端分组	IP地址	MAC地址	使用人	拦截次数
1	DESKTOP-OPCF5JG	全网计算机/g...	10.41.0.95	00-50-56-80-4F-27		1318493
2	WIN-DPTT2TD5RAO	全网计算机	10.41.0.216	00-50-56-80-E6-13		358413
3	test-guo	全网计算机/g...	10.41.0.99	00-50-56-80-6F-45		316961
4	DESKTOP-9865P4S	全网计算机/g...	10.41.0.148	00-50-56-80-9E-ED		225734
5	DESKTOP-QATG8RU	全网计算机/g...	10.41.0.143	00-50-56-80-45-C5		177386
6	DESKTOP-G1JPE9R	全网计算机/g...	10.41.0.144	00-50-56-80-31-E7		167188
7	DESKTOP-2E4M2BD	全网计算机/g...	10.41.0.44	00-50-56-80-F5-3F		156993
8	DESKTOP-QATG8RU	全网计算机/g...	10.41.0.143	00-50-56-80-45-C5		68335
9	WIN-CLFRQ5QESHD	全网计算机/fir...	10.41.0.217	00-50-56-80-FD-71		65594
10	Test-PC	全网计算机/g...	10.41.0.100	00-50-56-80-1C-A1		46593

4.5.2. 按终端统计

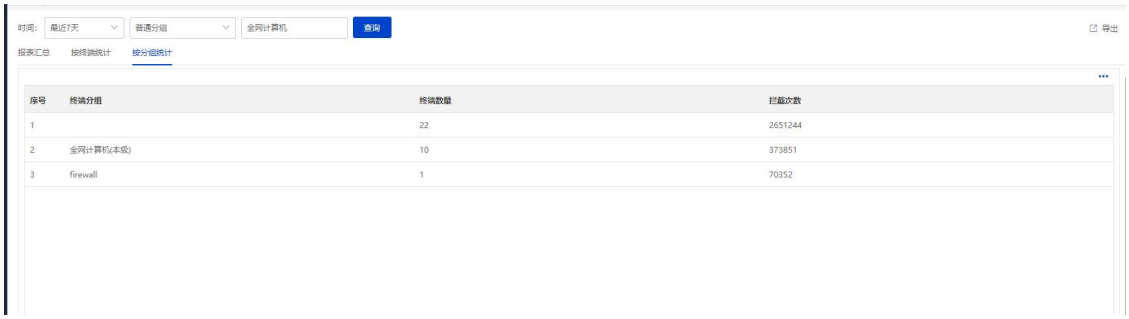
该功能提供根据终端统计防火墙拦截的情况，通过筛选排序功能，可以快速定位出内网安全风险的范围和影响情况，通过分析做出处理决策。



序号	计算机名	终端分组	IP地址	MAC地址	操作系统	操作系统账号	使用人	拦截次数
1	DESKTOP-OPCF5JG	全网计算机...	10.41.0.95	00-50-56-80-4F-27	Windows PC	test		1318493
2	WIN-DPTT2TD5RAO	全网计算机	10.41.0.216	00-50-56-80-E6-13	Windows Server	Administrator		362876
3	test-guo	全网计算机...	10.41.0.99	00-50-56-80-6F-45	Windows PC	Administrator		316961
4	DESKTOP-9865P4S	全网计算机...	10.41.0.148	00-50-56-80-9E-ED	Windows PC			225734
5	DESKTOP-QATGBRU	全网计算机...	10.41.0.143	00-50-56-80-45-C5	Windows PC	guo		177386
6	DESKTOP-G1JPE9R	全网计算机...	10.41.0.144	00-50-56-80-31-E7	Windows PC	Administrator		167188
7	DESKTOP-2E4M2BD	全网计算机...	10.41.0.44	00-50-56-80-F5-3F	Windows PC	Administrator		156993
8	WIN-CLFRQ5QESHD	全网计算机...	10.41.0.217	00-50-56-80-FD-71	Windows Server	Administrator		70241
9	DESKTOP-QATGBRU	全网计算机...	10.41.0.143	00-50-56-80-45-C5	Windows PC	test		68335
10	Test-PC	全网计算机...	10.41.0.100	00-50-56-80-1C-A1	Windows PC	Administrator		46593
11	DESKTOP-GSFFVVI	全网计算机...	10.41.0.34	00-50-56-80-4F-8E	Windows PC	Test		45939
12	WIN-CLFRQ5QESHD	全网计算机...	10.41.0.217	00-50-56-80-FD-71	Windows Server	Administrator		26987
13	DESKTOP-B82QDP7	全网计算机...	10.41.0.131	00-50-56-80-36-CE	Windows PC	test		19422
14	DESKTOP-C7OVBCG	全网计算机...	10.41.1.239	00-50-56-80-DF-9D	Windows PC	test		16031
15	DESKTOP-5UM4P6D	全网计算机...	10.41.0.145	00-50-56-80-70-35	Windows PC	Administrator		11472
16	DESKTOP-GB9LL9P	全网计算机...	192.168.47.149	00-0C-29-4E-1E-B8	Windows PC	Jia		10627
17	Test	全网计算机...	10.41.1.236	00-50-56-80-6E-38	Windows PC	Administrator		10335
18	test-PC	全网计算机...	10.41.1.235	00-50-56-80-CE-87	Windows PC	Administrator		7809
19	Test-PC	全网计算机...	10.41.0.149	00-50-56-80-5F-72	Windows PC	Administrator		6834

4.5.3. 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。



序号	终端分组	终端数量	拦截次数
1		22	2651244
2	全网计算机(本级)	10	373851
3	firewall	1	70352

5. 威胁检测与响应

5.1. 基本概念

5.1.1. EDR

EDR（Endpoint Detection and Respons）即“终端检测与响应系统”，在天擎 EDR 先锋版管理中心中，以“威胁检测与响应”进行管理。

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。

EDR 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与响应，提供安全风险告警、威胁深度调查、威胁分析溯源、多种处置响应能力，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,为政企终端提供更全面有效的保护。

5.1.2. 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。

5.1.3. 终端调查

对于一个终端是否被攻击，往往需要配合终端的多个迹象或证据来辅助判断，因此需要对失陷终端或疑似失陷终端进行远程调查，以获取更多终端信息来配合深度分析。

5.1.4. 威胁响应

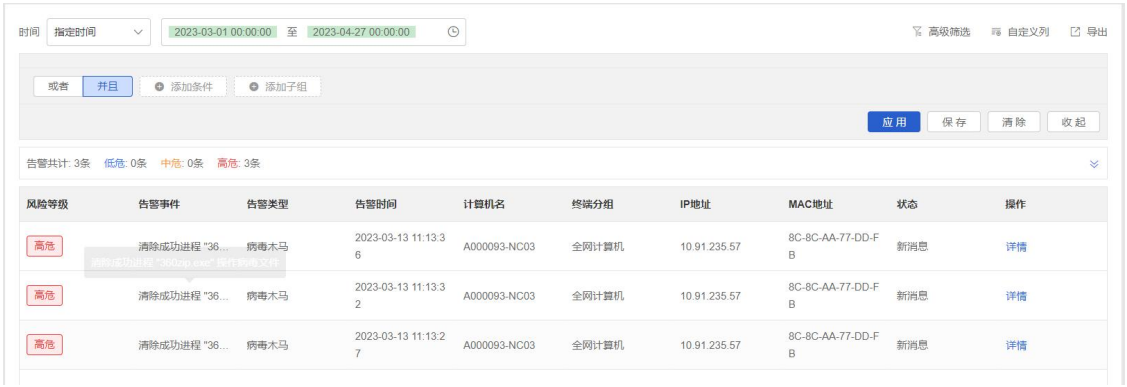
产生威胁告警后，通常需要管理员或者安全分析人员对告警终端进行调查分析，经核实后，确认告警是一个确切的威胁，这时管理员或者安全分析人员可以通过 EDR 对每一个威胁进行处置，包括进程终止、进程隔离等；若分析后发现告警并没有产生实际影响或者不需要处置，可以对告警进行“不处理”。通过对威胁地及时响应，能够保证内网终端的安全。

5.2. 威胁检测与响应策略

威胁检测与响应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。

5.3. 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。



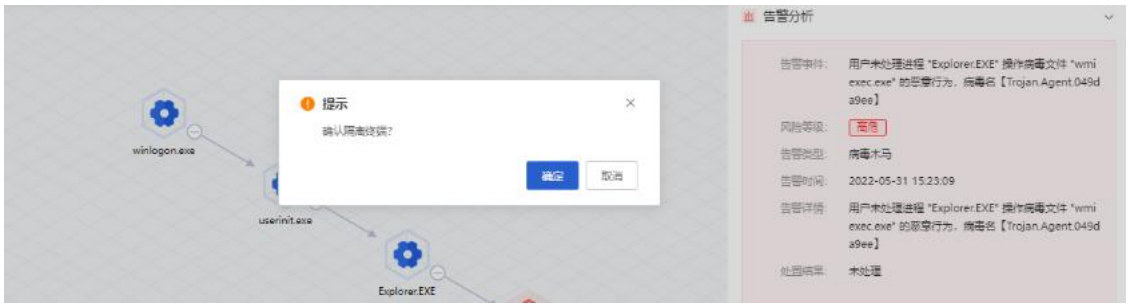
对于威胁告警列表中的告警，产品也提供了丰富的筛选条件，同时关联筛选条件可以更加灵活，帮助安全人员快速找到自己关注的告警内容。

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。

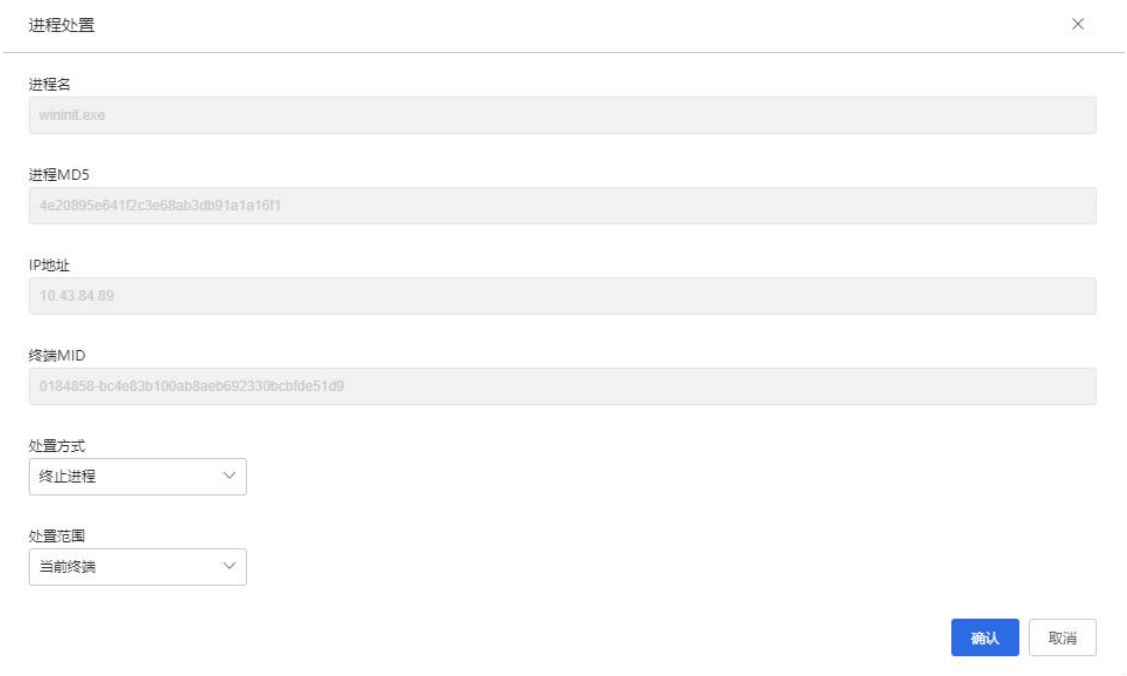
点击“终端调查”按钮可跳转到终端调查页面快速下发调查任务，帮助分析人员远程即可对异常终端进行问题排查及定位，减少远程安全运维成本。

点击“隔离终端”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。

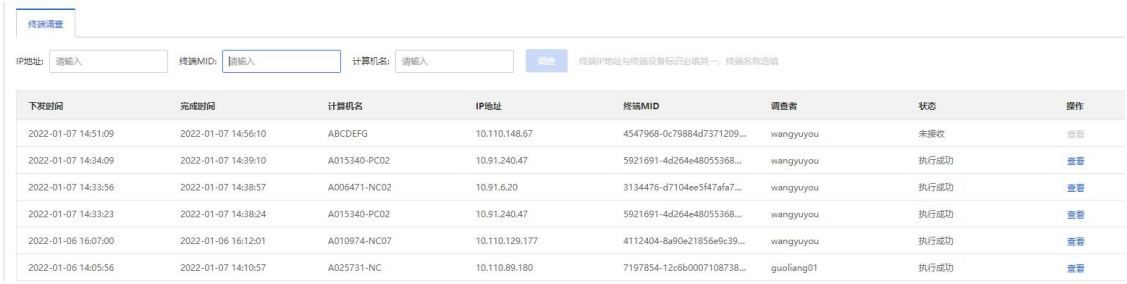
点击“进程处置”按钮可对单台终端或全网终端的进程进行处置，处置动作包含终止进程、终止进程并隔离、终止进程删除、恢复隔离进程文件。



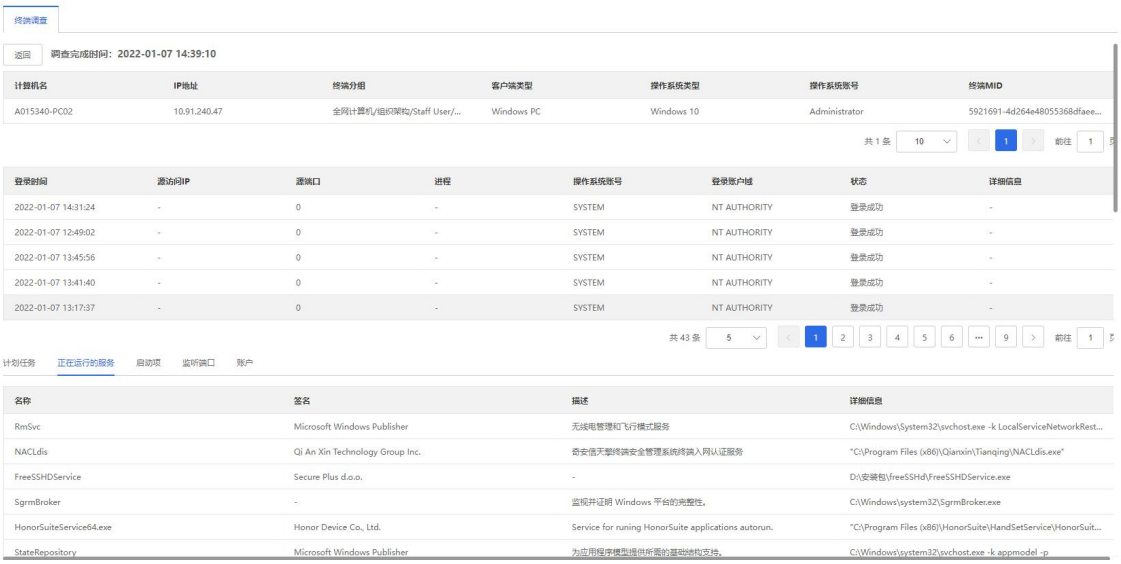
5.4. 终端调查

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。



5.5. 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、隔离终端、网络阻断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。

处置进程：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。

网络阻断：对访问恶意 IP 的网络连接行为进行阻断。

5.6. 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，并通过云端对天擎 EDR 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，待终端处置成功后，刷新页面可查看处置结果。

6. 软件管理

6.1. 基础概念

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。

6.1.1. 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。

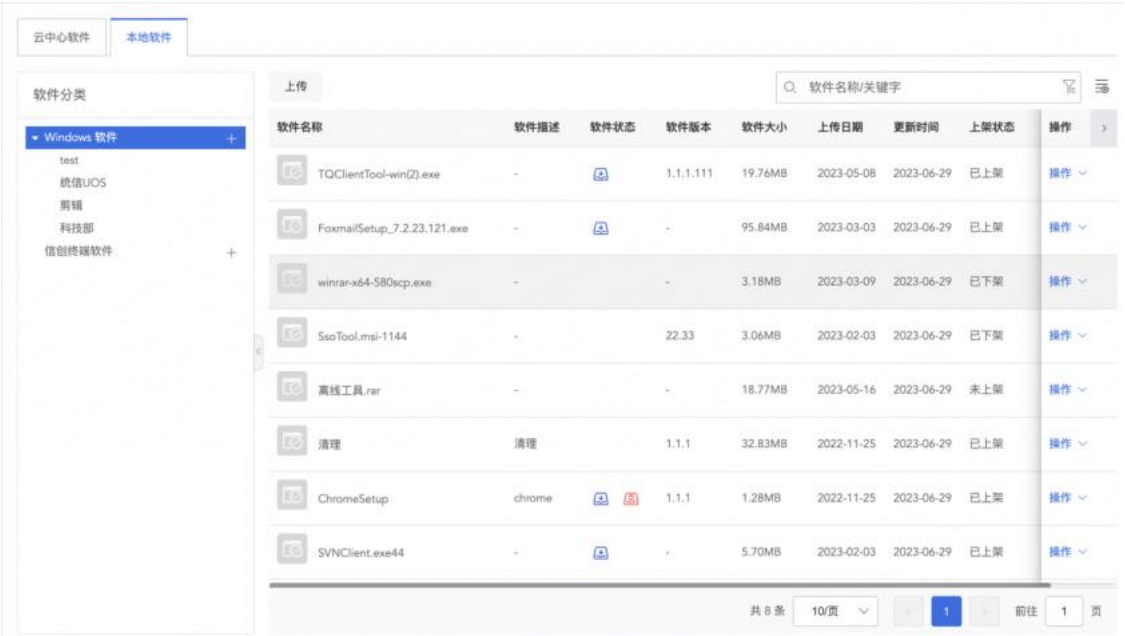
6.1.2. 软件中心

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。

6.2. 软件中心

6.2.1. 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

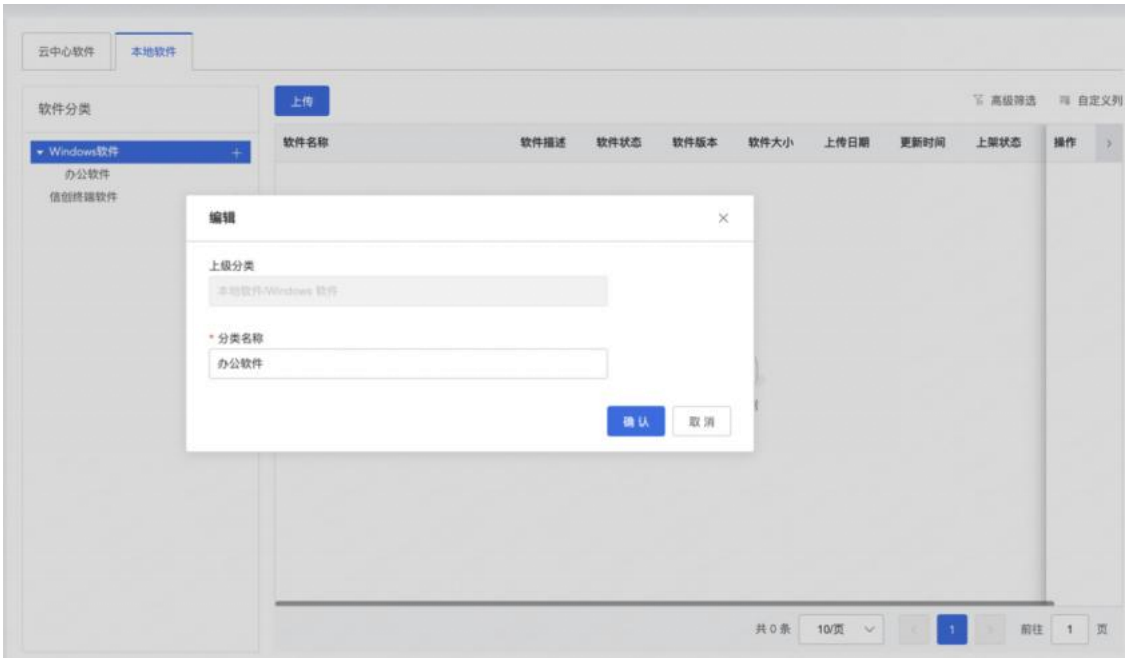


6.2.1.1. 软件分类

按照软件的用途不同将对其进行自定义分类。

- 新建。点击右侧的+，新建软件分类，填写分类名称。
- 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。

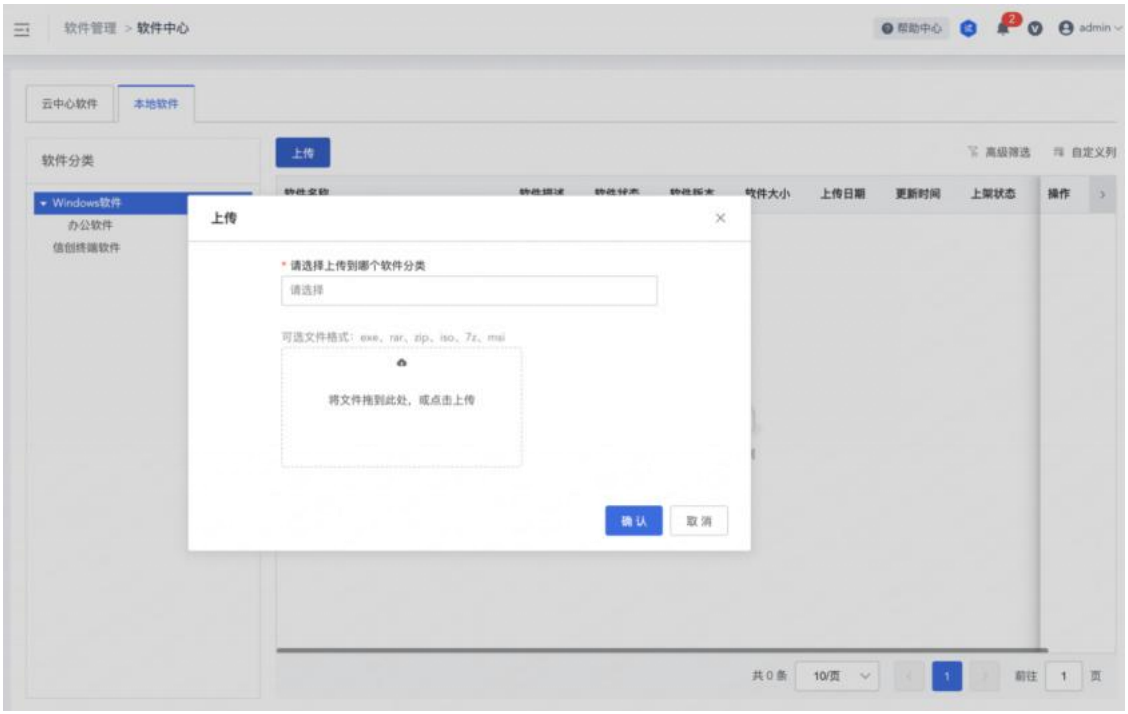
- 删除。点击选中需要删除的分组，右键 选择删除，对该分类进行删除。



6.2.1.2. 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。

- 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：

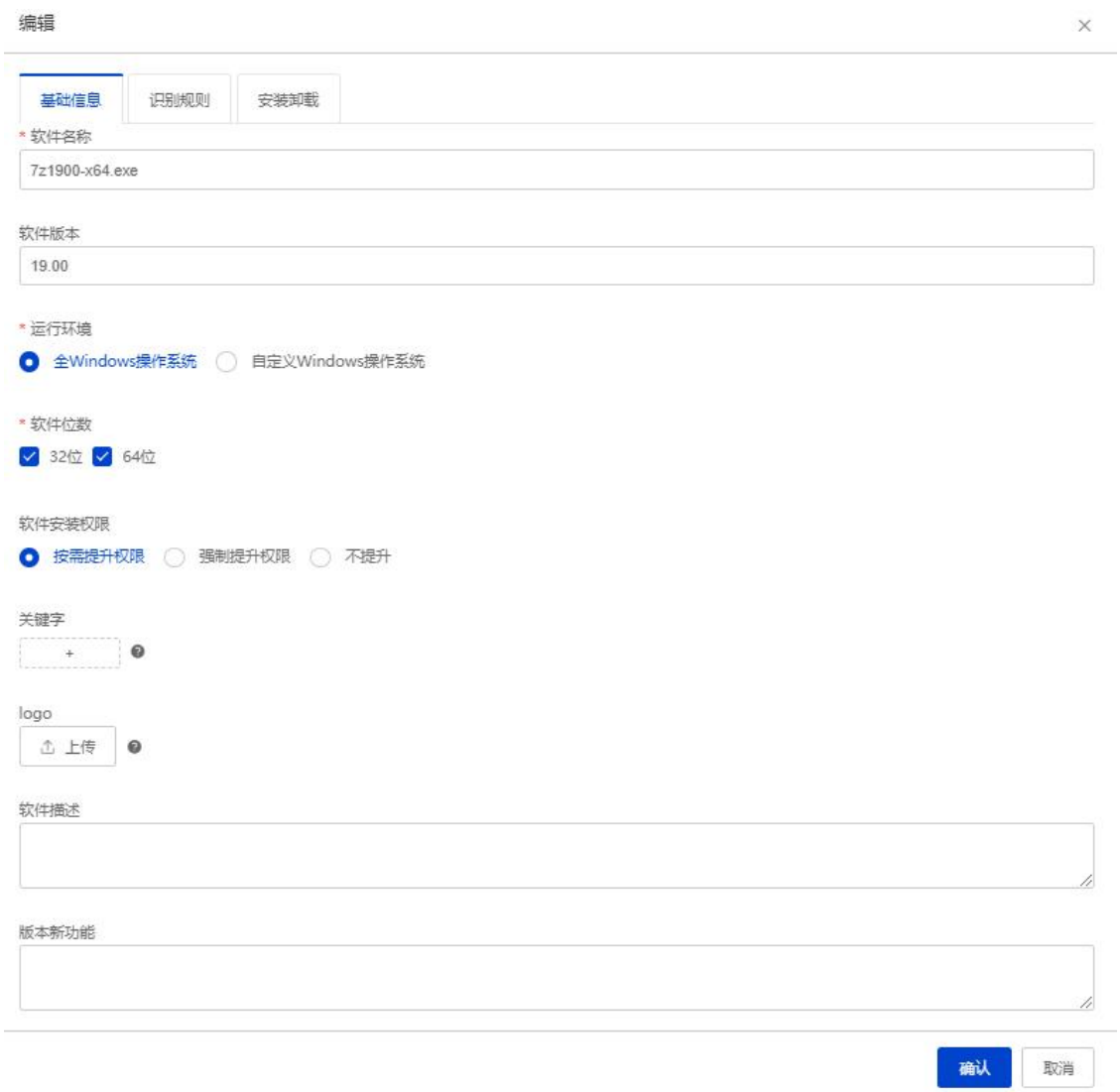


等待上传完成后，会自动生成文件的 MD5 值，管理员可以通过 MD5 值进行软件的校验。

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。

- 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。

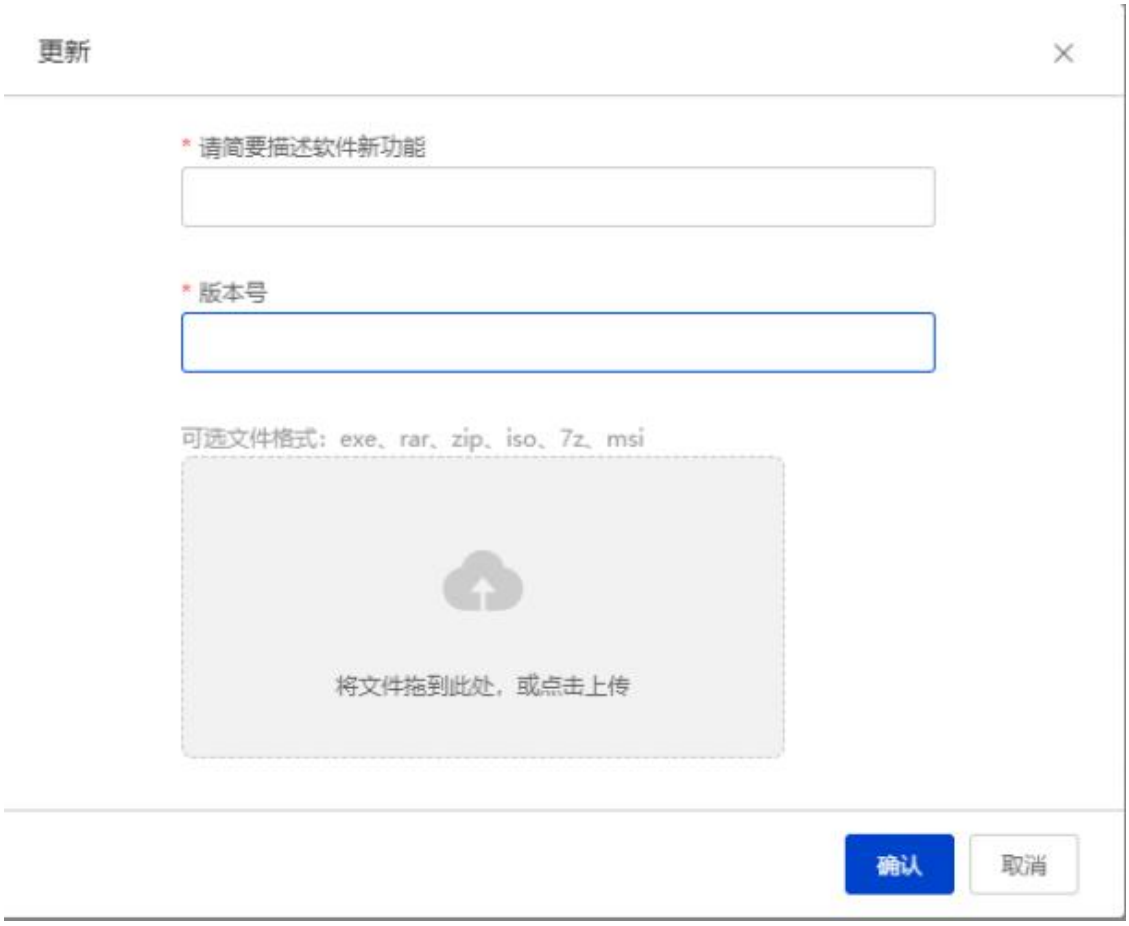


识别规则：配置可以对注册表，自定义组合，配置主程序进行设置。

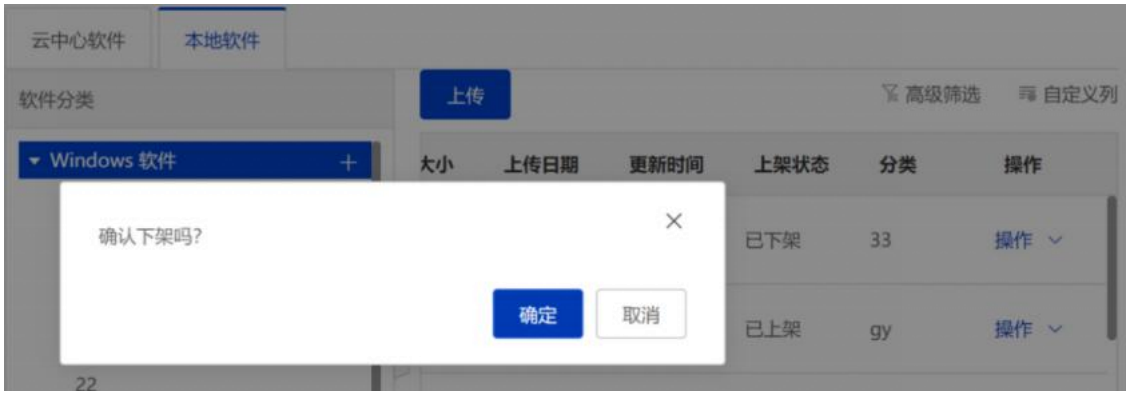
示例：①软件安装在注册表的标志，如蓝信+在注册表的键值为 LanxinSoftCustom ②软件运行时在进程中的主程序名，如蓝信+的主程序名为 LxMainNew.exe

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。

- 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。



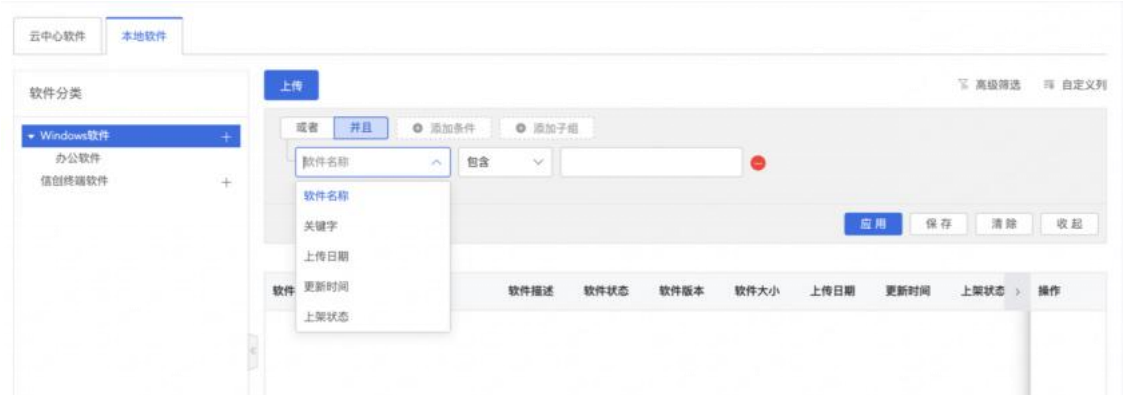
- 上架/下架。选中需要上架或者下架的软件，未上架的软件可将其选择上架，已上架的软件可选择将其下架。



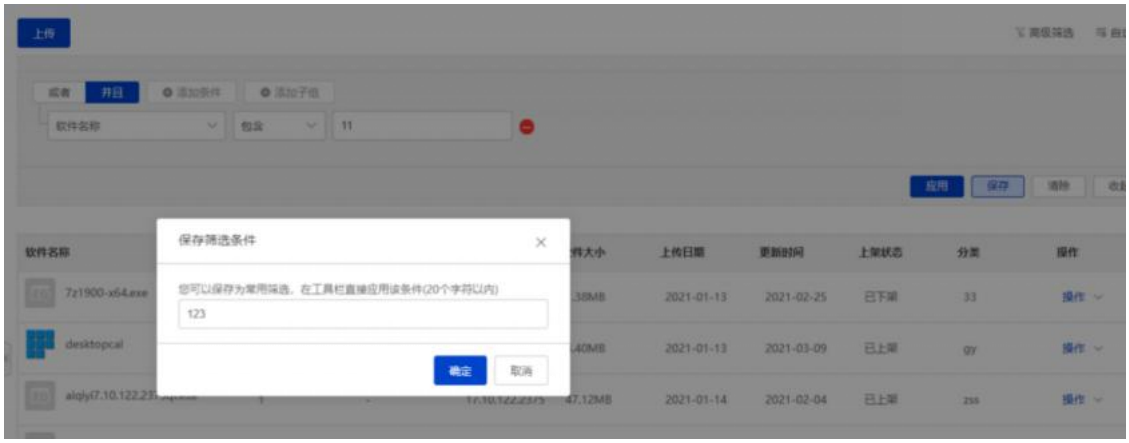
- 转移分组：将软件的当前分组转移到其他分组，完成软件所在分组的变更。

6.2.1.3. 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：

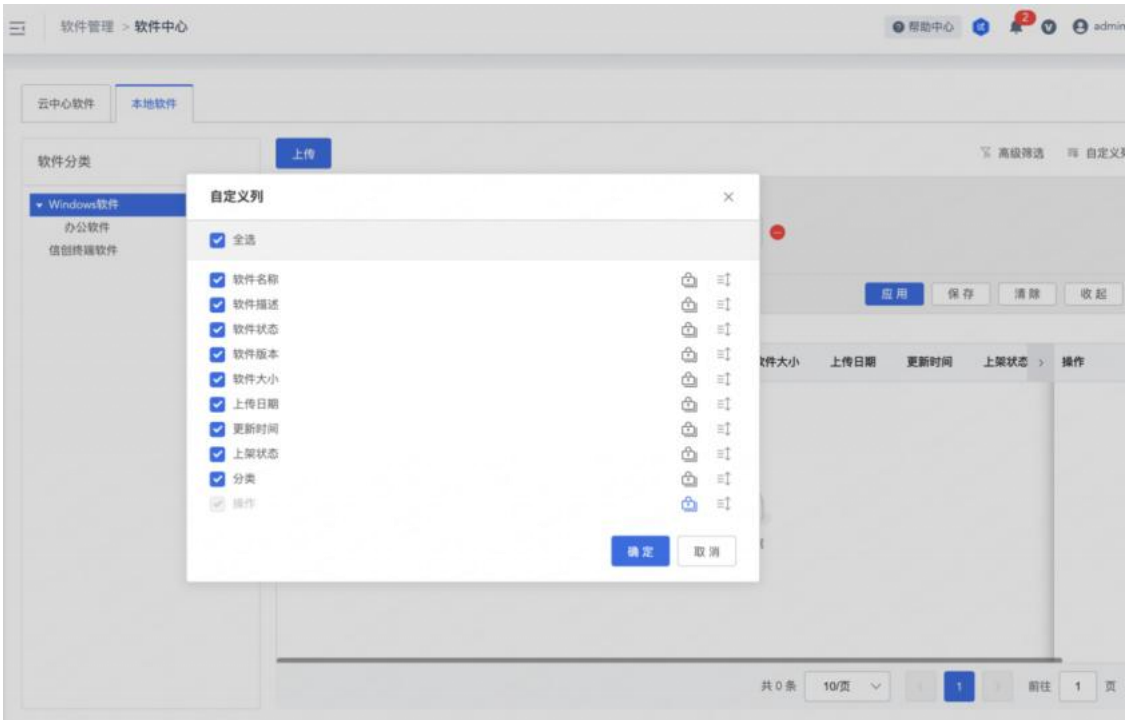


点击应用后即可按照当前条件筛选出查询结果，点击保存可将当前条件保存后方便下次进行筛选。



6.2.1.4. 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。

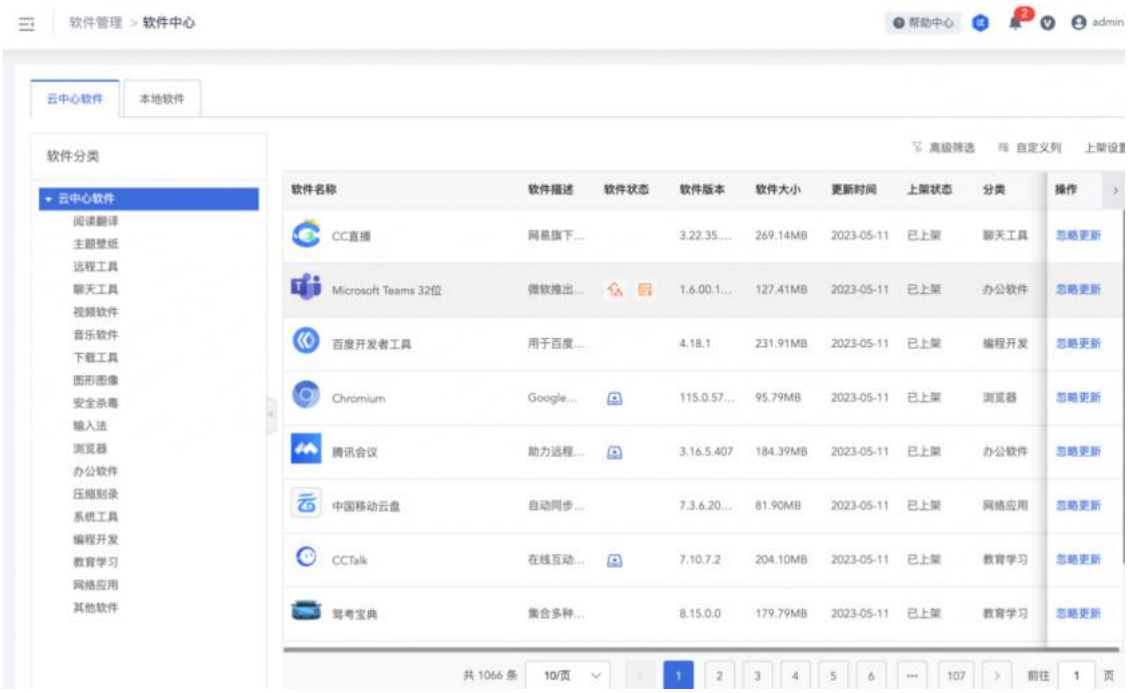


6.2.2. 云中心软件

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。

6.2.2.1. 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。



6.2.2.2. 上架设置

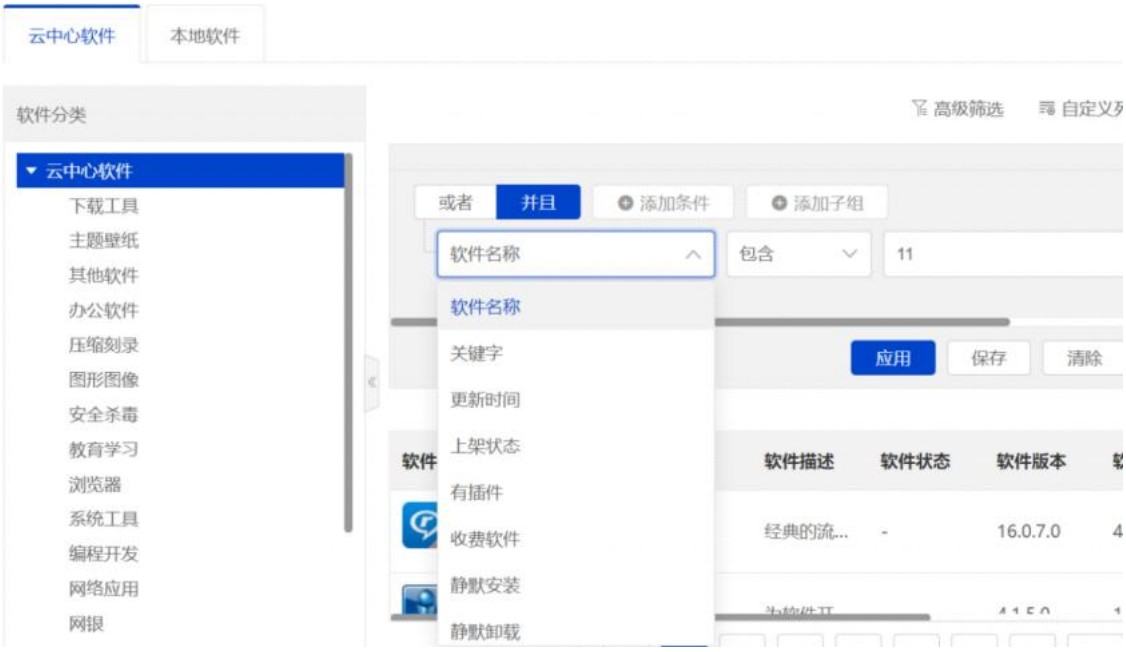
云中心软件上架设置包括黑名单和白名单两种方式。

- 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。

- 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。

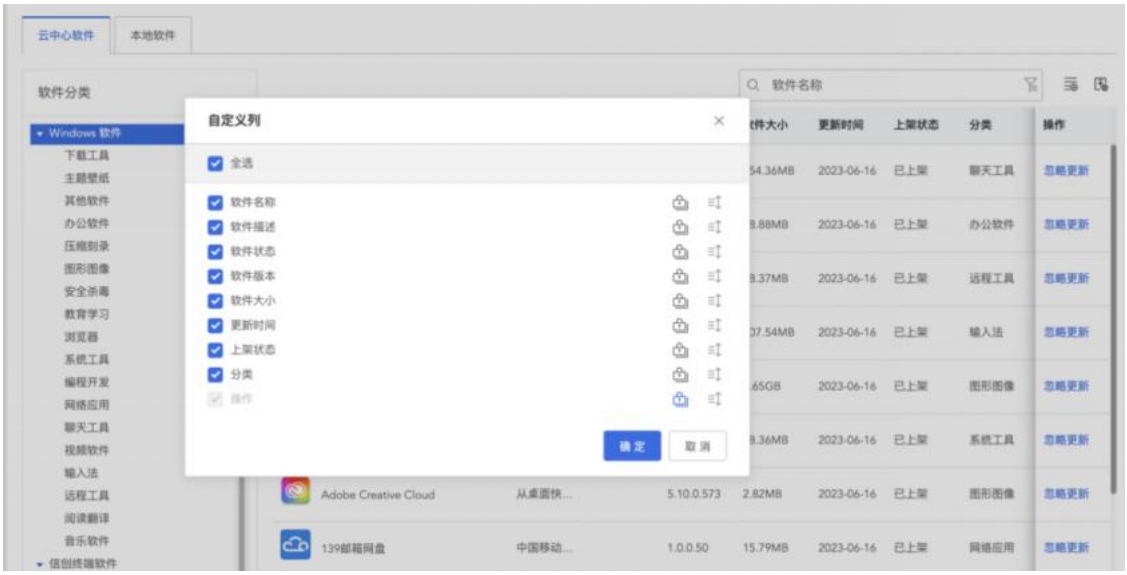
6.2.2.3. 高级筛选

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：



6.2.2.4. 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。



6.3. 软件管理策略

本章节主要介绍企业软件管理系统的使用。

6.3.1. 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。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。

6.3.2. 上报已安装软件

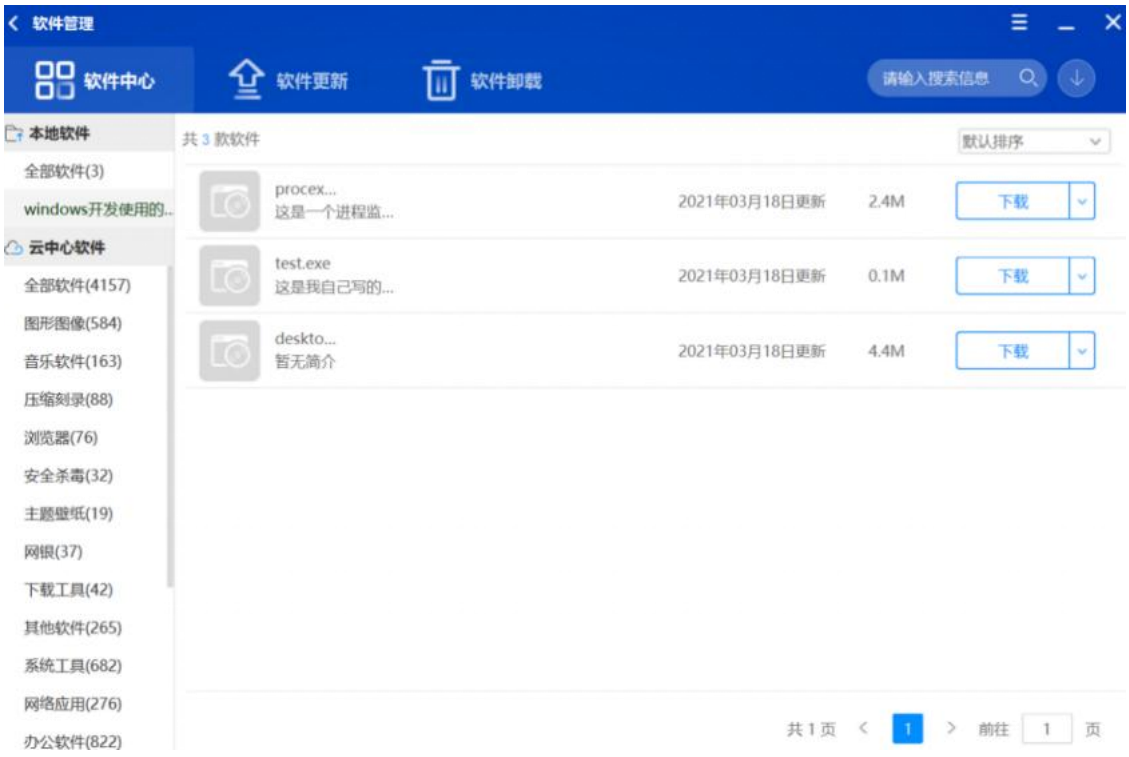
在“软件管理>策略管理>基础设置”功能内“开启上报已安装软件”配置，对客户端会自动采集终端上已经安装的软件，若开启了此选项，终端会强制采集终端安装的软件。

6.3.3. 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。

6.3.4. 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。

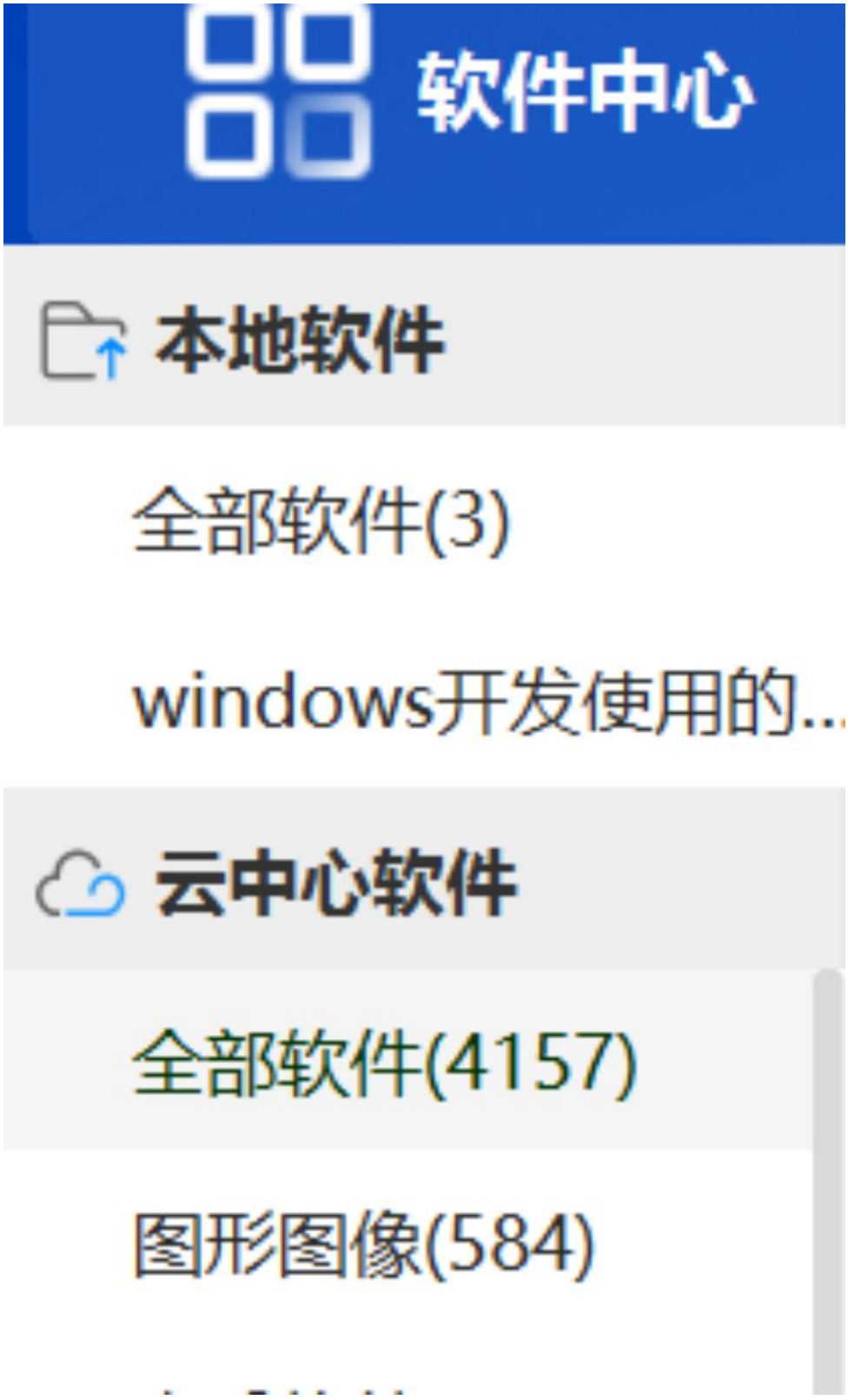


6.3.5. 定制本地软件

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。

6.3.6. 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。



6.3.7. 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。

6.3.8. 定制名称

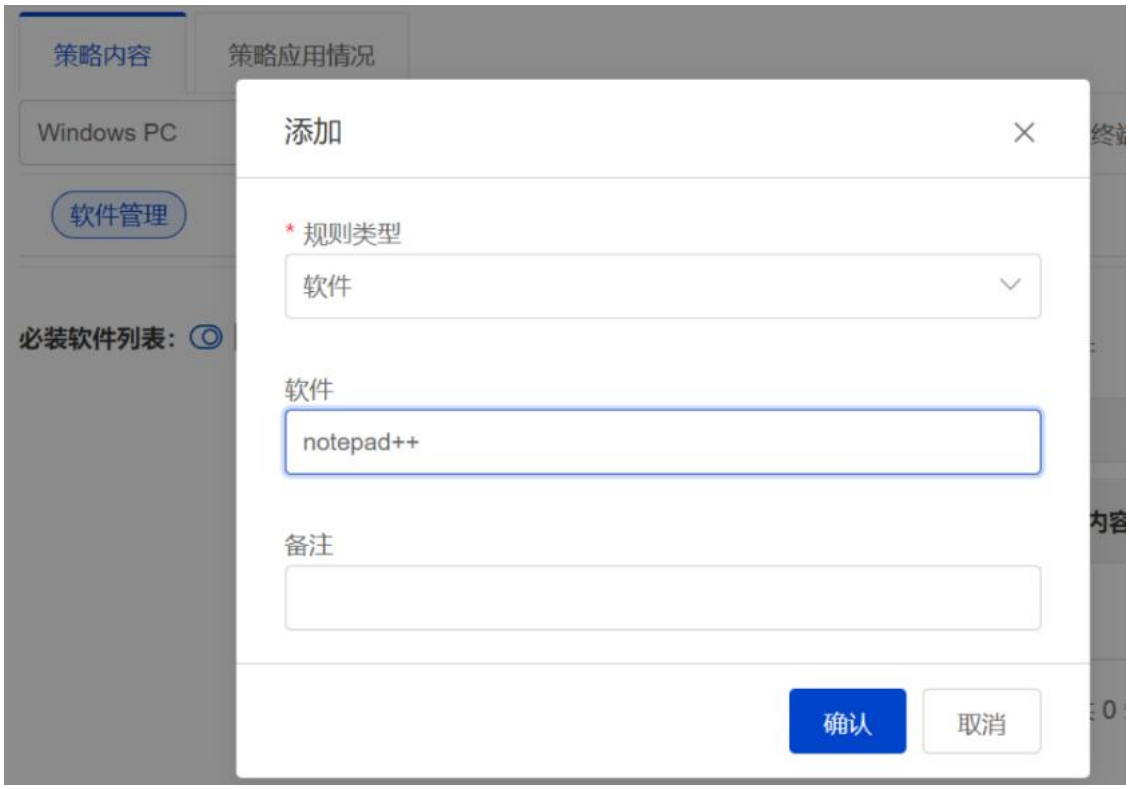
对终端软件管理中显示的名称进行定制，包括本地软件名称和云软件名称。

6.3.9. 自动安装

开启自动安装后，终端会自动安装在必装软件列表中的软件，安装前会有文字提示，可自定义提示文字。

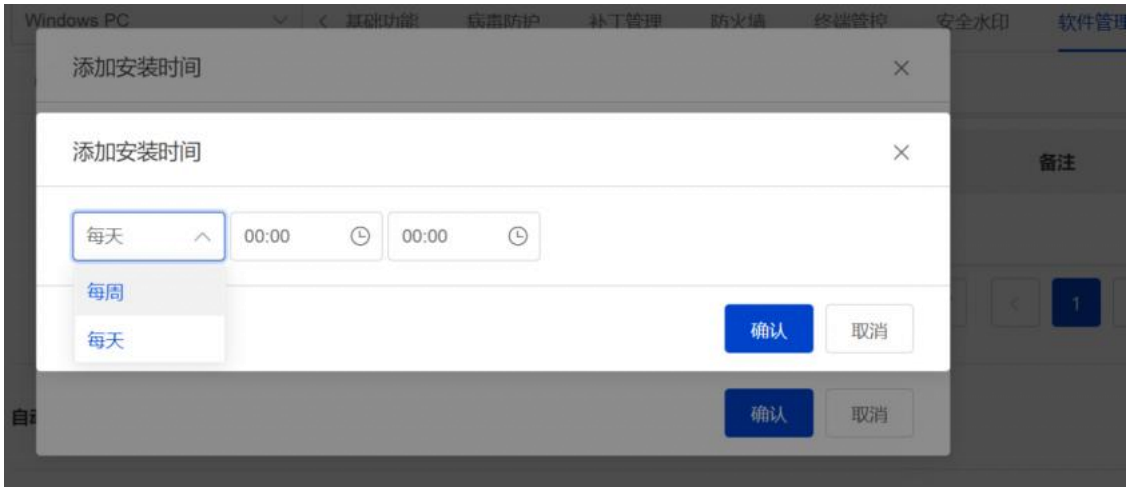
6.4. 必装软件列表

选择需要终端必装的软件，添加到软件列表中，终端会自动安装该列表中的软件。



6.4.1. 自动安装和更新时间段

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



6.4.2. 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。

6.4.3. 下载设置

软件下载目录默认是在（D:），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。

6.4.4. 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。

6.4.5. 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。

6.4.6. 关闭云中心软件

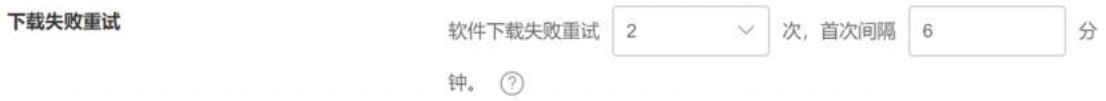
在系统管理>业务设置>软件管理中选择关闭云中心软件，开启此选项后即可关闭云中心软件，终端中不在显示云中心软件。

6.4.7. 任务并发

设置软件安装和更新的任务并发数。

6.4.8. 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。



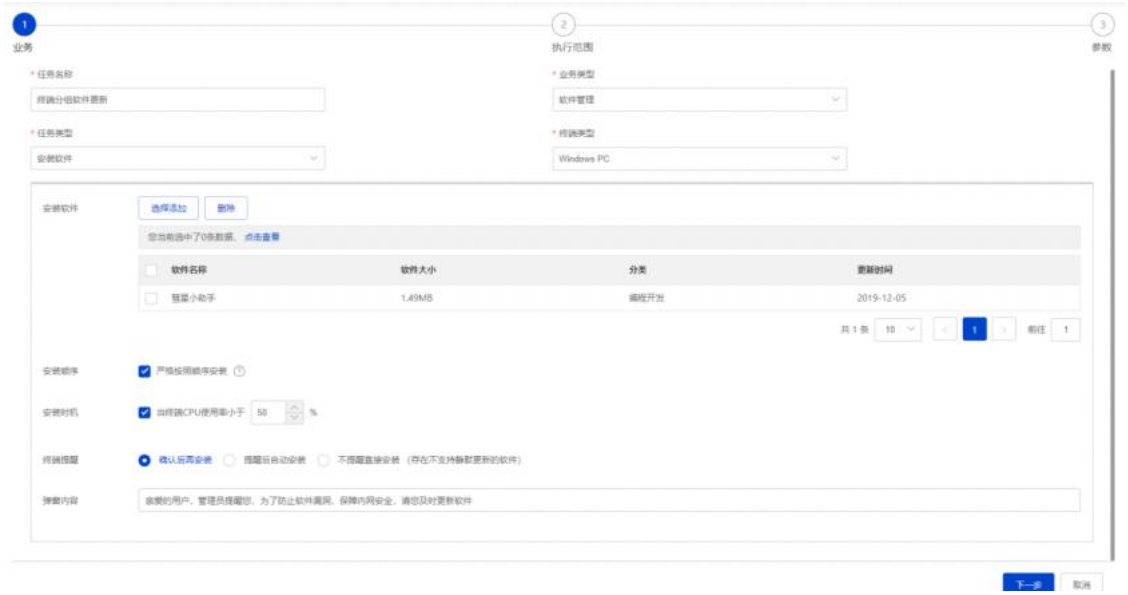
6.4.9. 客户端软件管家全局配置

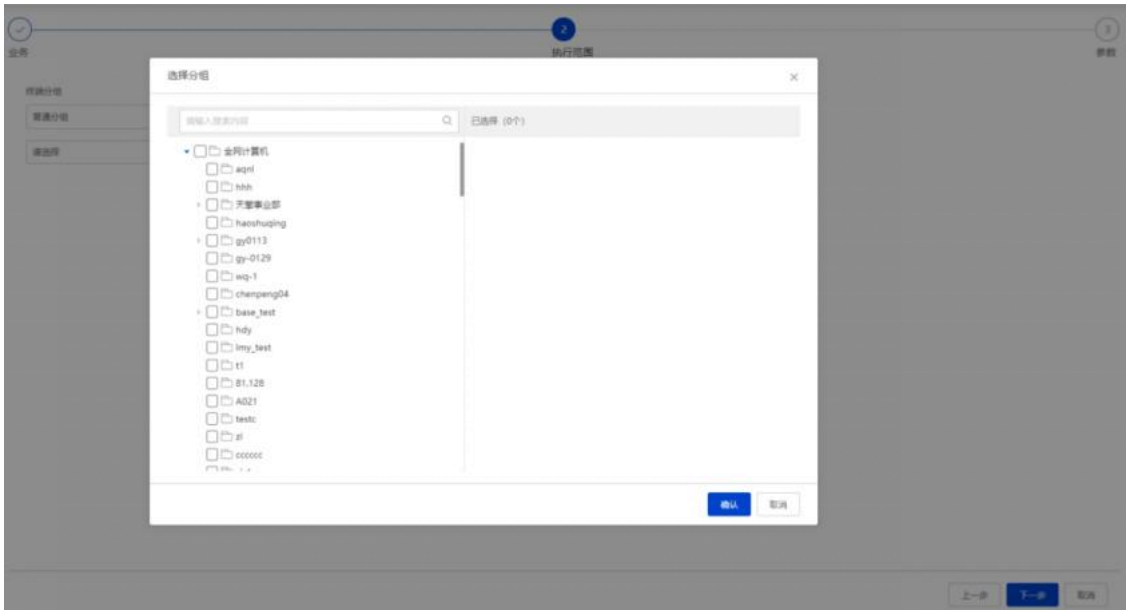
在系统管理>业务设置>软件管理中可开启受限账号使用客户端软件管理、开启软件管理中文输入。 注：受限账号指非操作系统管理员账号。

6.5. 软件终端任务

6.5.1. 分组软件任务

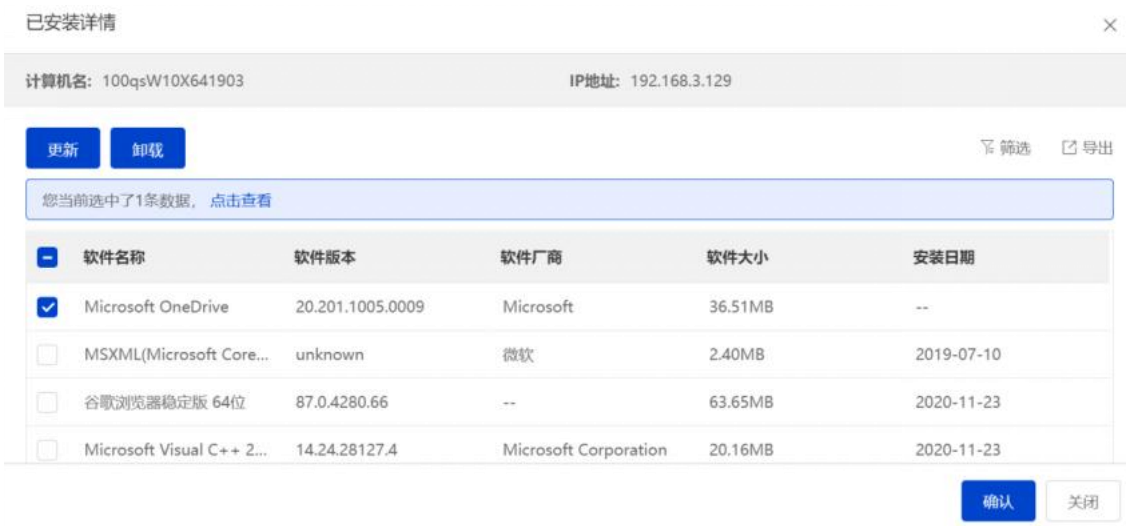
在终端任务业务类型中选取“软件管理”，任务类型包括安装软件，更新软件，卸载软件。终端类型包括 WindowsPC 和 Windows server。在软件列表中选择需要管理的软件进行配置，能够按照软件列表中的顺序进行安装。安装时机是当终端的 CPU 使用率小于阀值时软件不会安装，终端提醒包括确认后再安装，提醒后自动安装，不提醒直接安装三种提醒方式。配置截图如下：



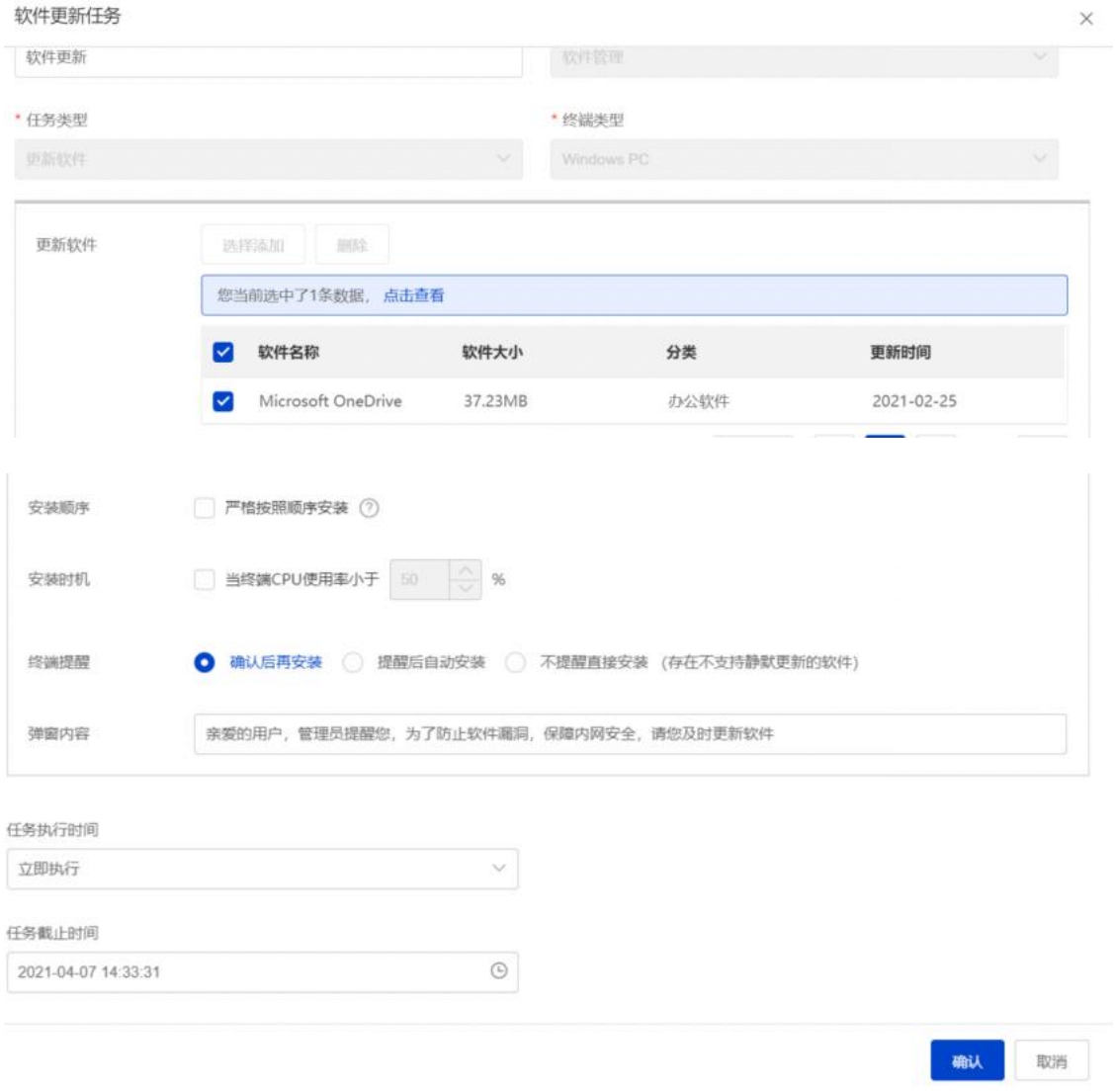


6.5.2. 终端软件任务

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。

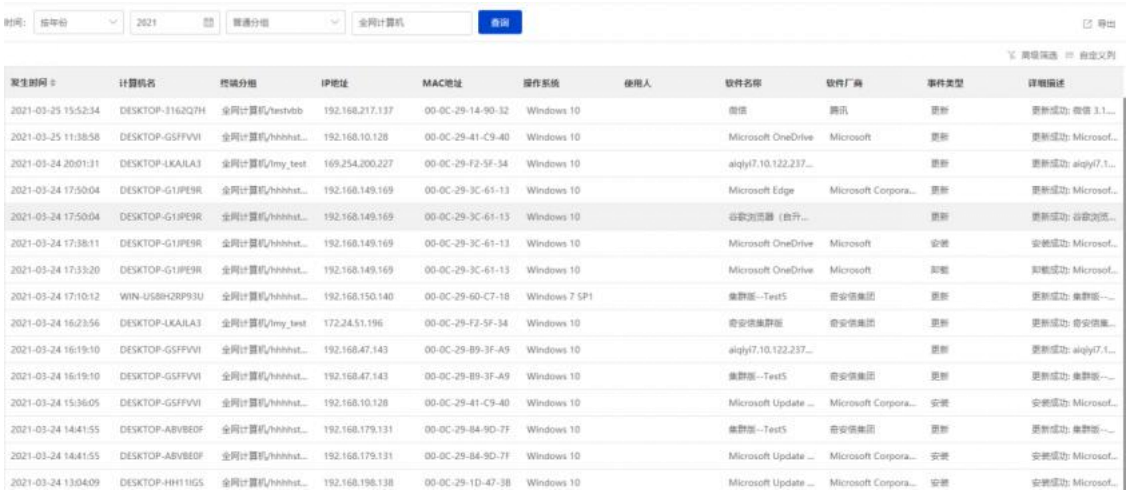


填写任务名称，选取更新软件，配置好安装顺序、安装时机、终端提醒和任务执行开始时间，完成对当前终端的软件升级。



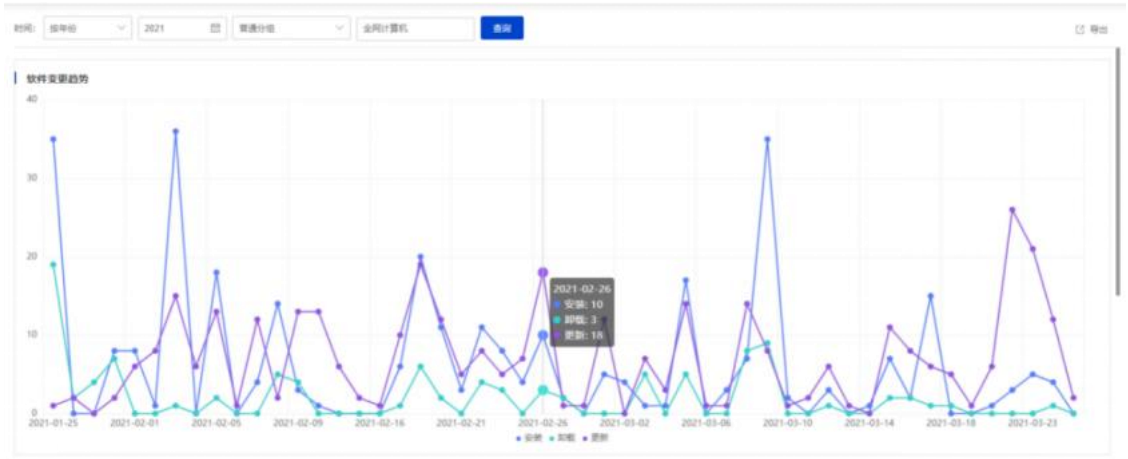
6.6. 软件日志

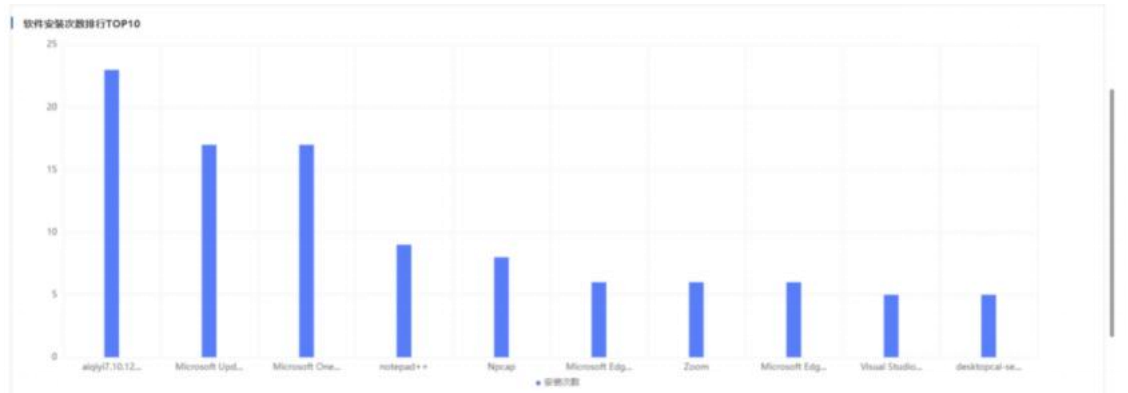
软件日志可按照时间和分组两个不同的维度对终端软件的操作信息进行记录，事件类型包括，软件更新，安装，卸载。日志可以通过报表的形式导出。

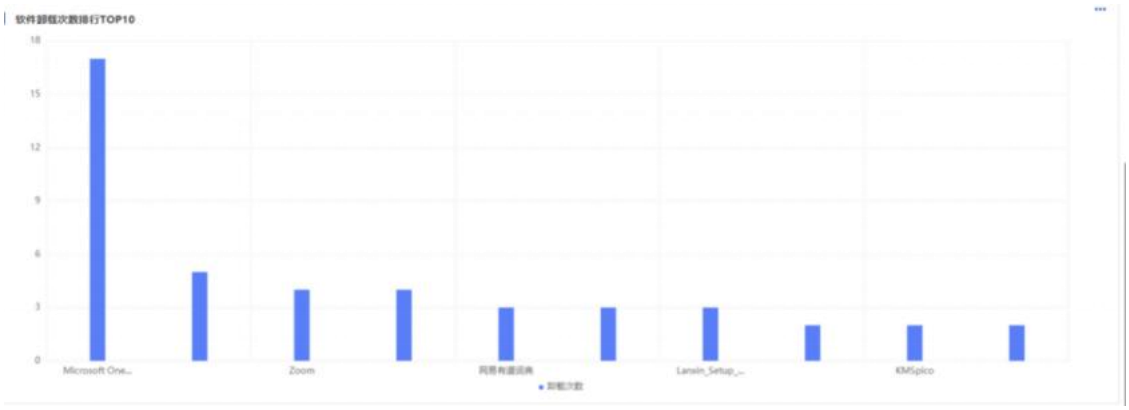


6.7. 软件报表

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。







6.8. 正版化管理

6.8.1. 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。

6.8.2. 正版化信息统计

系统基于统计规则定期生成统计结果，并可真对统计结果进行筛选、数据下钻查看详情、导出。

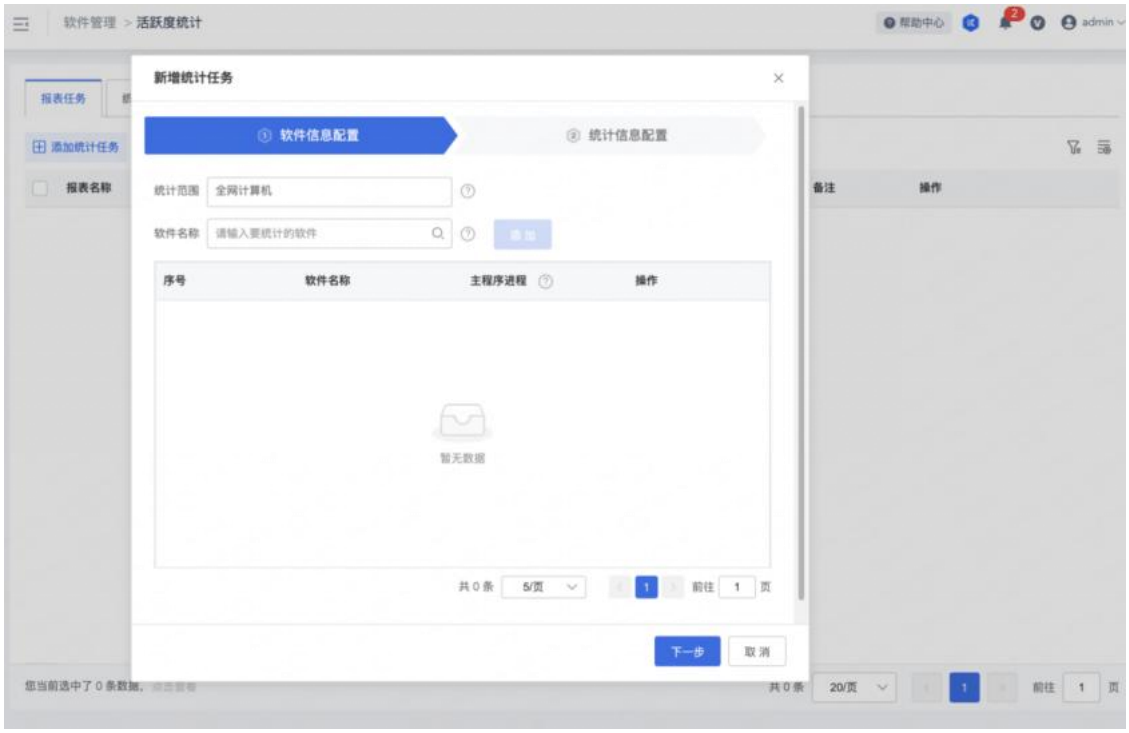
6.8.3. 软件活跃度统计

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。

6.9. 活跃度统计

6.9.1. 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。

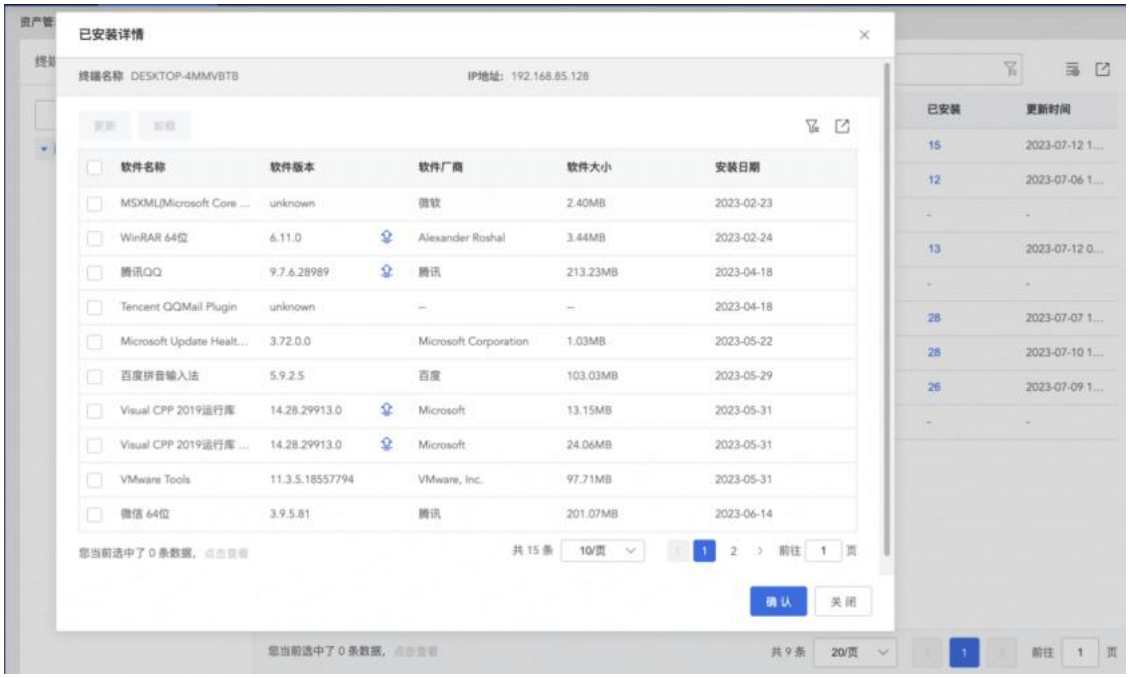


6.9.2. 统计报表

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。

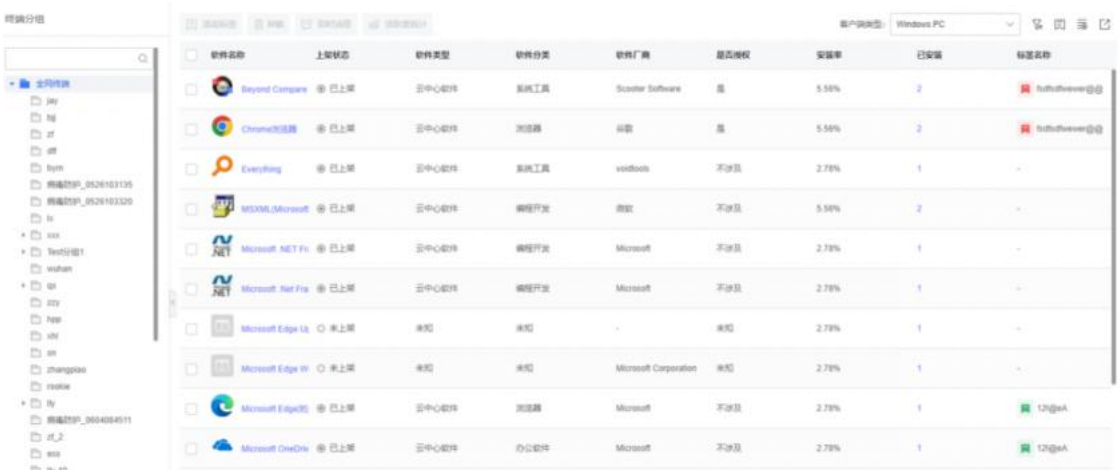
6.10. 终端软件概况

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。



6.11. 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。

7. 补丁管理

7.1. 基本概念

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、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。

7.1.1. 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。

7.1.2. 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，目前仅支持国产终端。

7.1.3. 补丁号

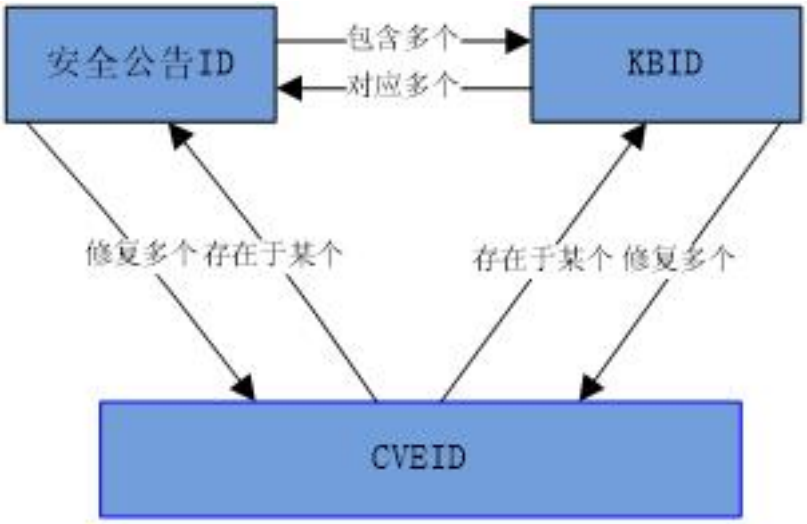
补丁号，也就是通常所说的 KBID。因为每个微软补丁都有一个唯一对应的知识库文章，所以使用知识库文章的编号作为补丁号，方便查看统计补丁的安装情况。知识库文章中描述补丁的修复了哪些漏洞、功能缺陷、补丁的已知问题等详细信息。

7.1.4. 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。



7.1.5. 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。

7.1.6. 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。

国产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。如果有针对国产系统/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。

7.1.7. 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。国产终端暂不涉及。

7.1.8. 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。

7.1.9. 天擎 EDR 补丁通告

天擎 EDR 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

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。

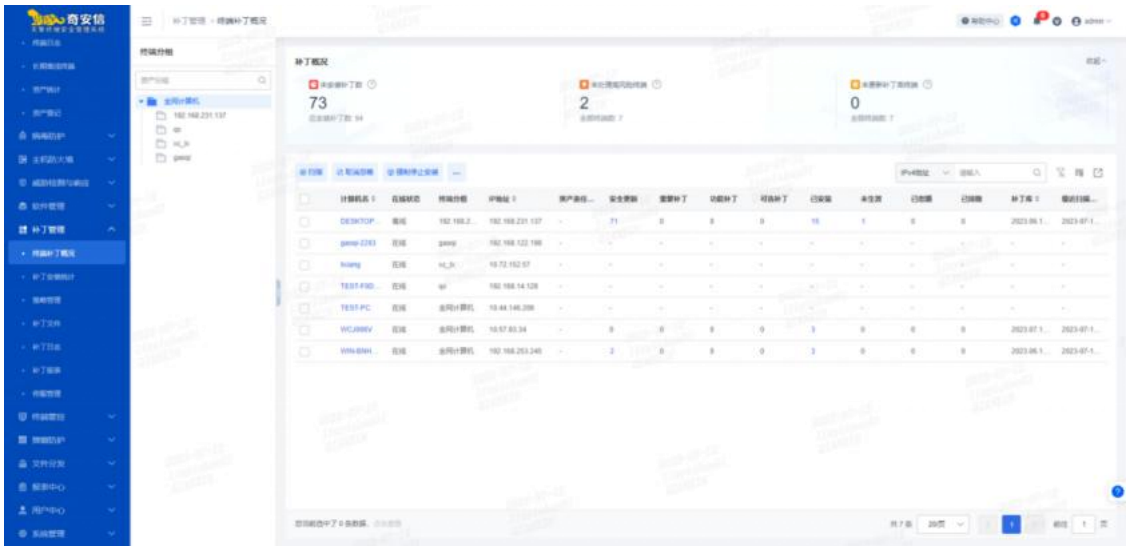
第4章 漏洞补丁详细列表

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

7.2. 终端补丁概况

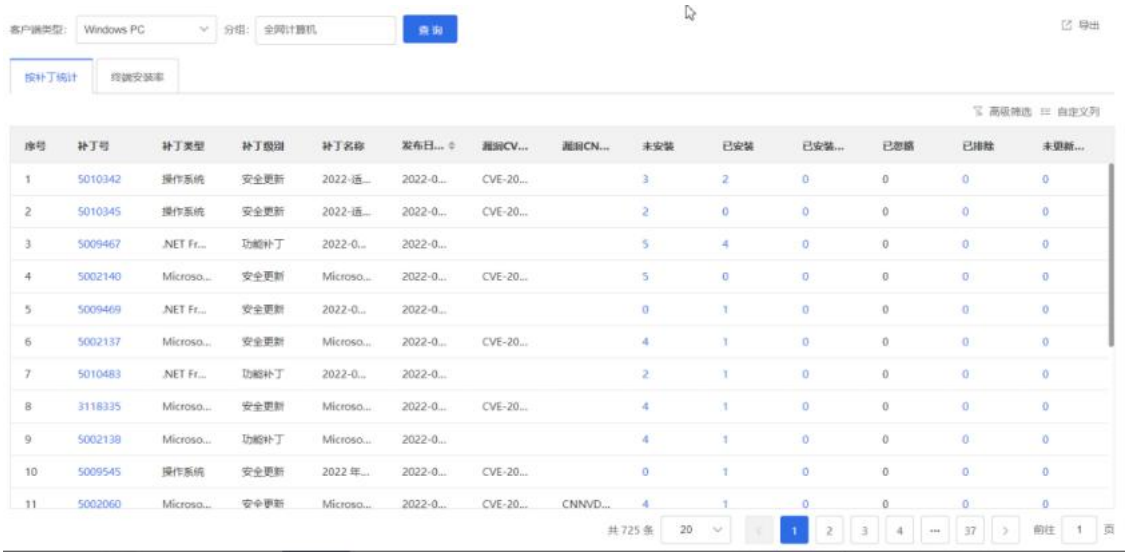
终端补丁概况用来展示全网终端（也可指定分组）的补丁安装情况，以帮助管理员了解终端的安全现状。



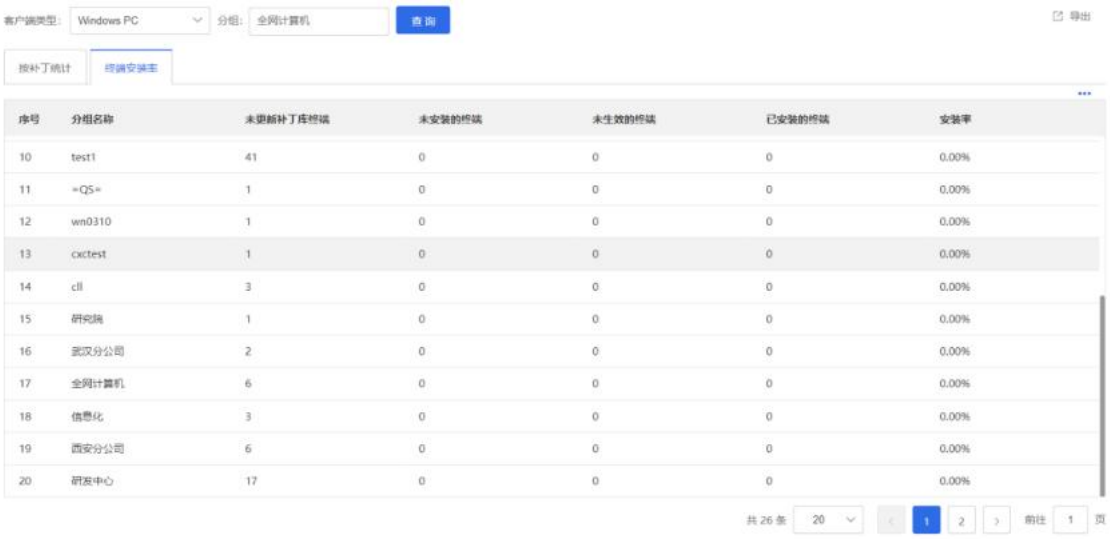
展示全网补丁及漏洞情况，分为：未处理漏洞数、未处理高风险终端、未更新补丁库终端。帮助管理者快速知悉全网情况。

7.3. 补丁安装统计

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。



7.4. 补丁策略管理

补丁策略设置，位于补丁管理>策略管理，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。

7.4.1. 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、卸载补丁。

扫描补丁：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。

自动安装补丁模式：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。

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。

7.4.2. 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，除非取消排除。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。

7.4.3. 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”和”下载完成全部补丁后，再安装”。

7.4.4. 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，以便让补丁及时生效修复漏洞。

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。

7.4.5. 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。

智能忽略：自动忽略 5 次都安装失败的补丁。

7.5. 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。

点击更新按钮：在更新完补丁后，手动刷新快速查看最新补丁内容。

7.6. 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。

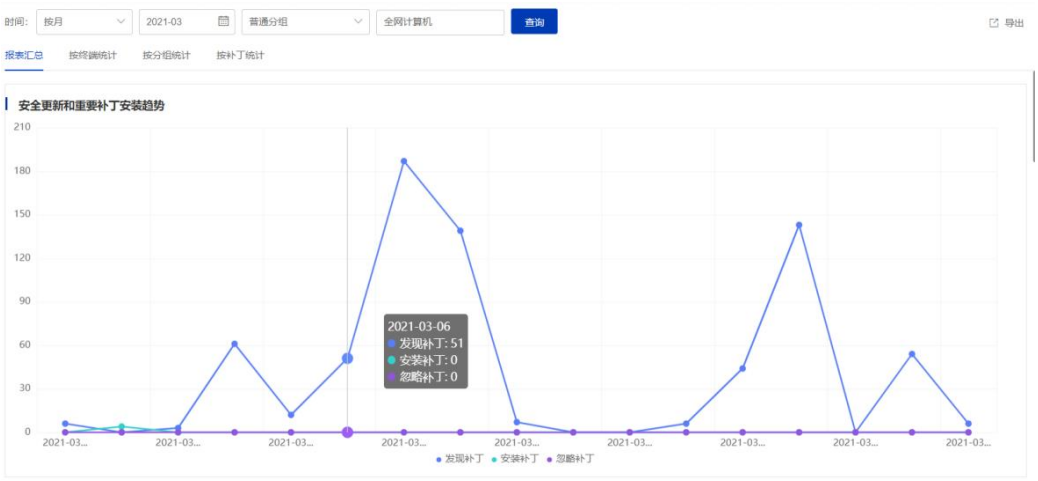
补丁日志展示扫描终端的信息，补丁日志主要信息有：补丁号、补丁级别、补丁类型、事件类型、补丁安装结果详情。

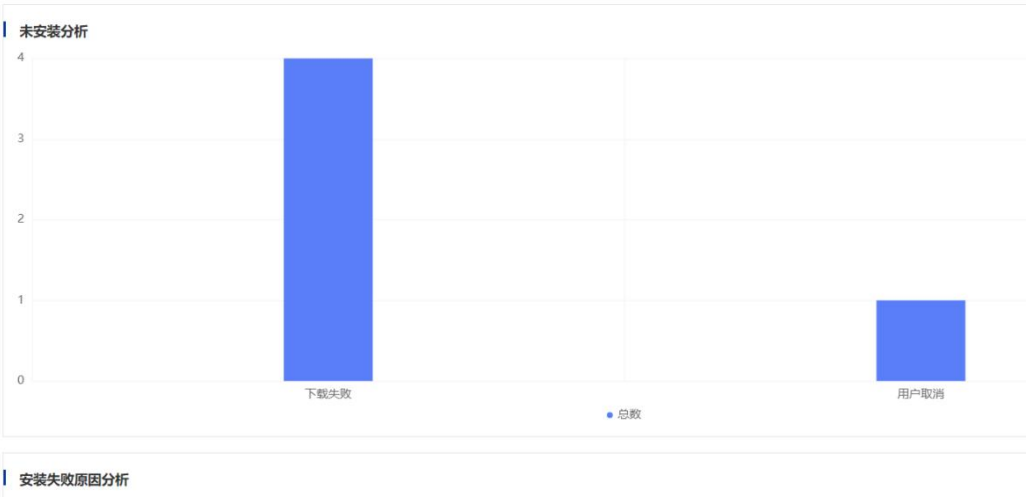
7.7. 补丁报表

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。

7.7.1. 报表汇总

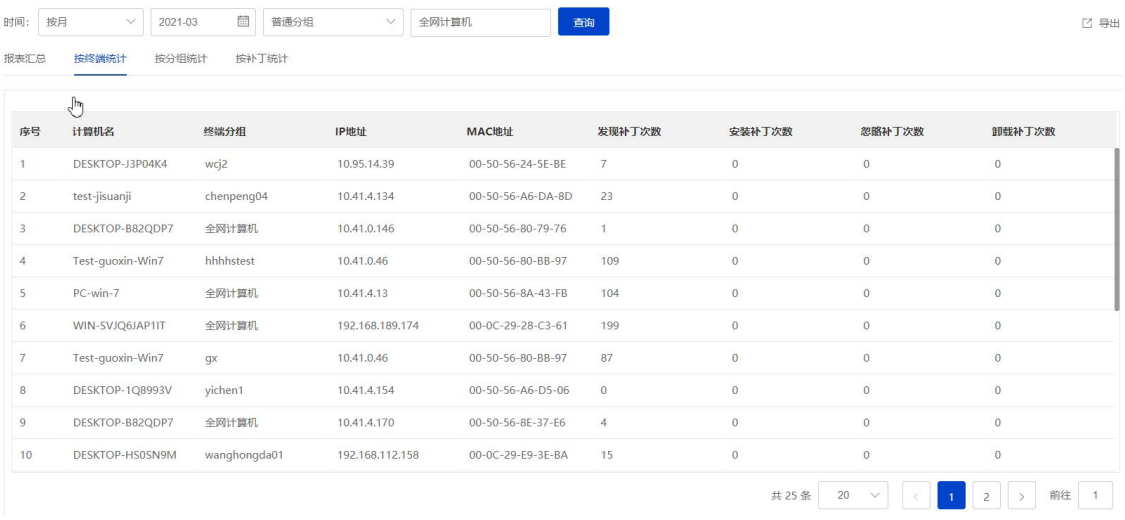
报表汇总提供了补丁安装的趋势图、未安装分析以及安装失败原因、安装补丁 TOP10 的分析数据。





7.7.2. 按终端统计

该功能提供终端维度的统计补丁的安装情况。

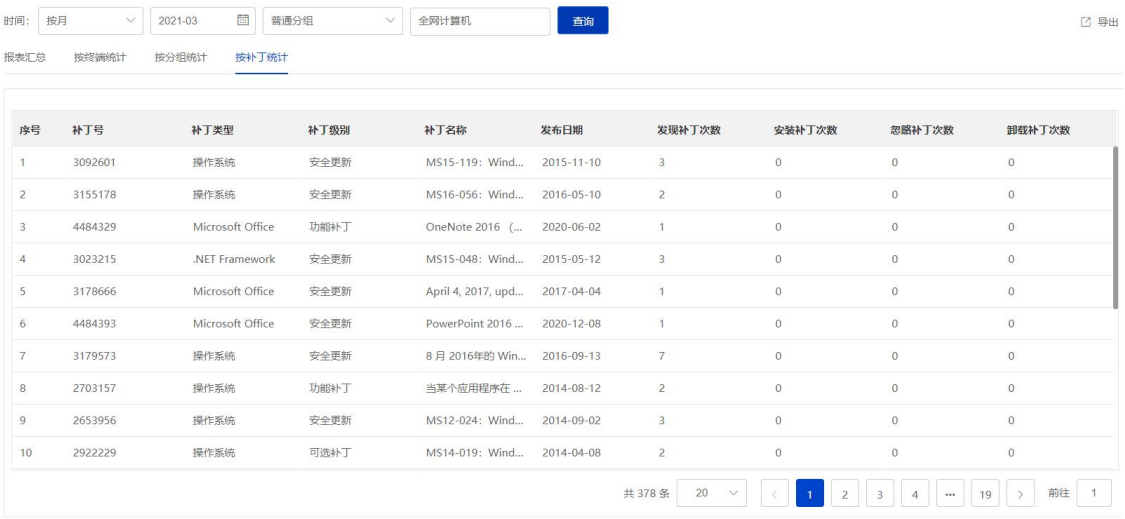


7.7.3. 按分组统计

该功能提供终端分组维度的统计补丁的安装情况分析。

7.7.4. 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。



7.8. 停服管理

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。

7.9. 终端补丁任务

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、卸载补丁、取消忽略、强制停止安装、升级停服系统、修复。（任务使用方法详见终端概况>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。

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。

修复：支持针对指定补丁下发修复的任务，可以定性快速解决目标补丁安装问题。

7.10. 补丁分发自动化运维思路

天擎 EDR 先锋版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。根据天擎 EDR 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。

7.11. 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。

7.12. 典型场景

7.12.1. 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。

7.12.2. 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“服务器可连接互联网”时的配置方式。

7.12.3. 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。

7.13. FAQ

7.13.1. 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。

7.13.2. 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:）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。

8. 终端管控

8.1. 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。

8.2. Windows 终端管控

8.2.1. 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。

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。

8.2.2. 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。

8.2.3. 网络管控

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

8.2.4. 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。

8.2.5. 外发管理

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。

8.3. 信创终端管控

8.3.1. 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。

设备禁用：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。

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。

8.3.2. 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。

8.3.3. 远程协助

管理员主动对在线的信创终端发起远程协助。支持 Windows 与信创终端相互建立远程连接。

远程协助入口：数据安全>终端管控>管控概况>远程协助。

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。

8.4. macOS 终端管控

8.4.1. 外设管控

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。

蓝牙设备使用管理：禁止通过蓝牙连接其他手机、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）

8.4.2. 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。

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。

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。

9. 弹窗防护

9.1. 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。

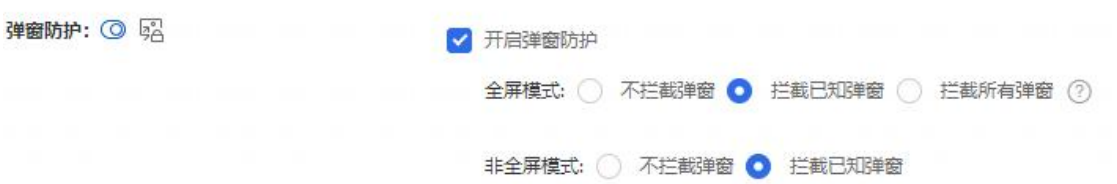
9.2. 弹窗策略管理

入口：弹窗防护>策略管理

9.2.1. 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。在此模式下，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”。

9.2.2. 拦截询问设置

通过历史数据统计发现，终端部分弹窗需要用户根据自身情况自行判断如何处理当前弹窗。用户选择处理方式后，后续弹窗将沿用用户的处理方式 忽略/阻断，不再显示拦截提示条。

注：显示拦截提示条的弹窗规则，目前运营团队持续维护，弹窗防护规则库中定义需要用户二次确认的弹窗，终端识别后才会显示拦截提示条。

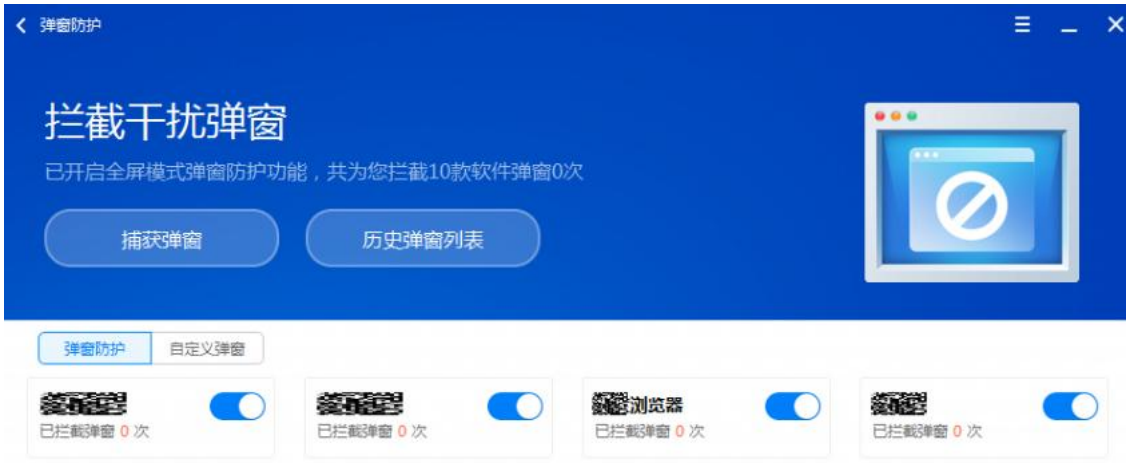
9.2.3. 终端关闭软件拦截设置

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。



9.2.4. 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。

9.3. 本地规则

入口：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。

9.3.1. 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：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。

9.3.2. 手动添加规则

入口：弹窗防护>弹窗防护本地规则>弹窗阻止规则/弹窗例外规则。

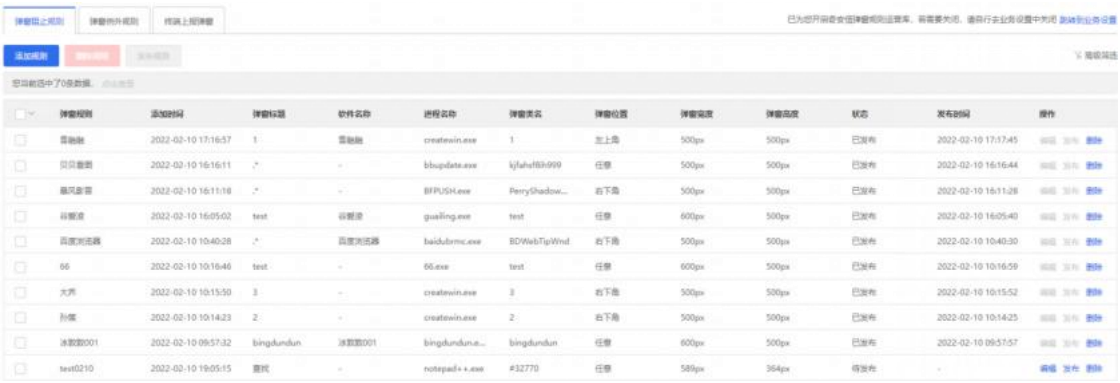
管理员可通过点击”添加规则”进行弹窗规则的添加。

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。

9.3.3. 规则的发布

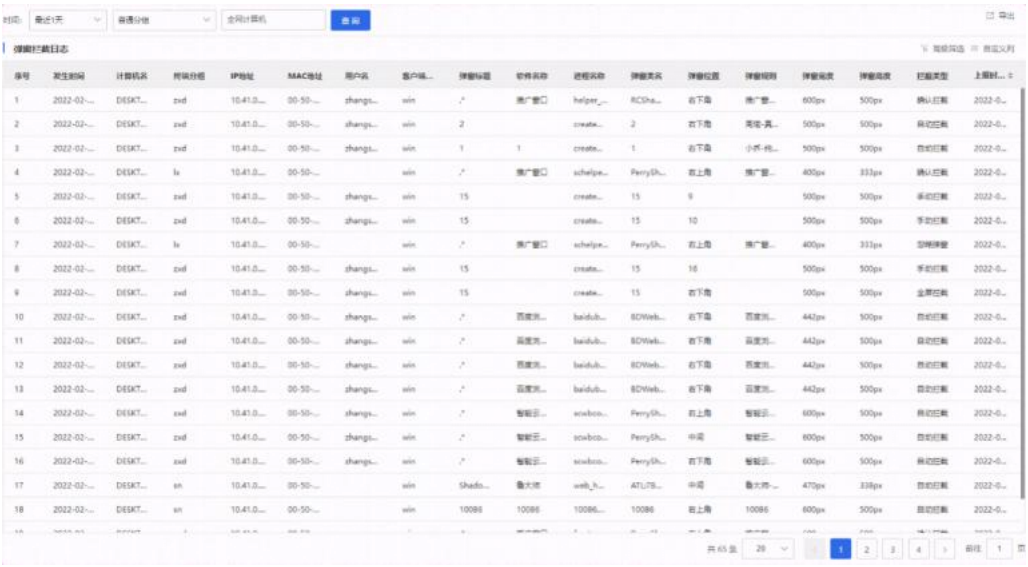
规则添加成功后，管理员需要针对已添加的规则执行发布操作。发布成功后，此规则将在终端立即生效。



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。

9.4. 防护日志

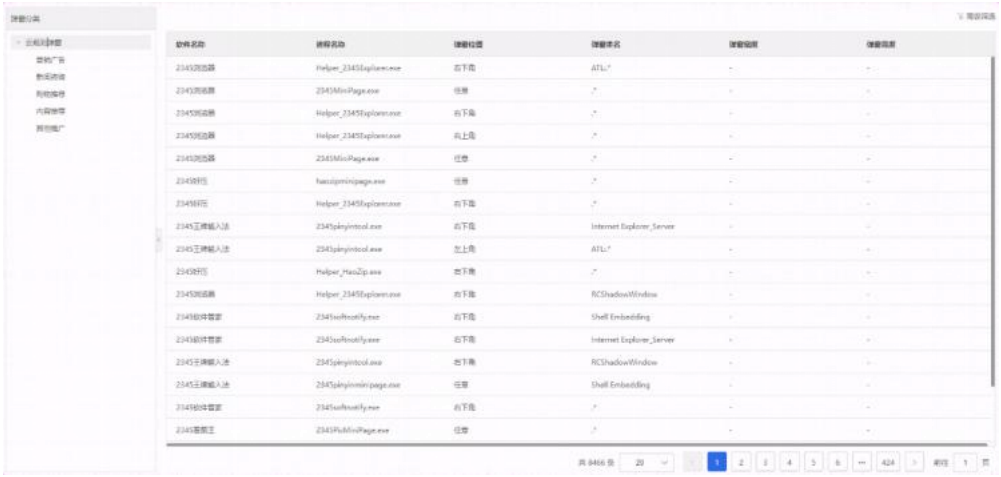
终端匹配相关弹窗规则进行拦截后，会上报被拦截弹窗相关信息，可按分组、按时间查询弹窗拦截日志，日志中详细记录被拦截弹窗的信息，如下图：



9.5. 云规则

入口：系统管理>业务设置>弹窗防护。

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。

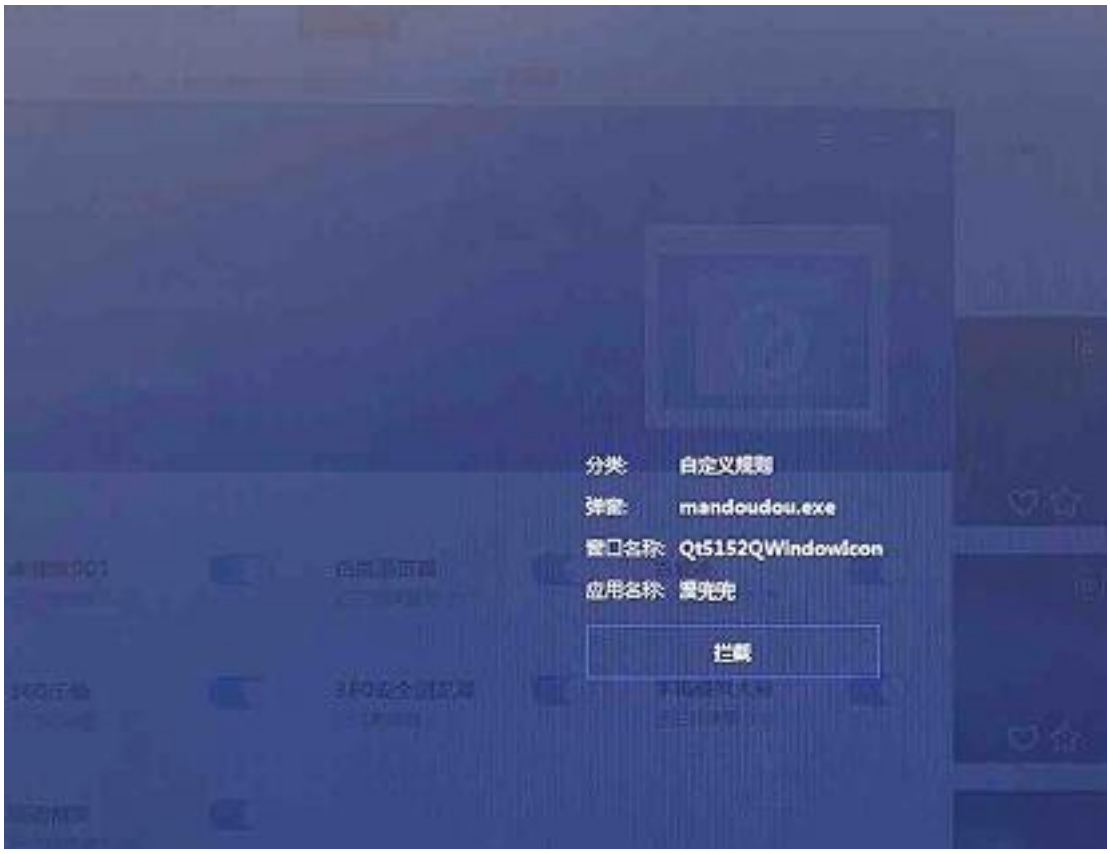
9.6. 客户端弹窗防护说明

9.6.1. 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：

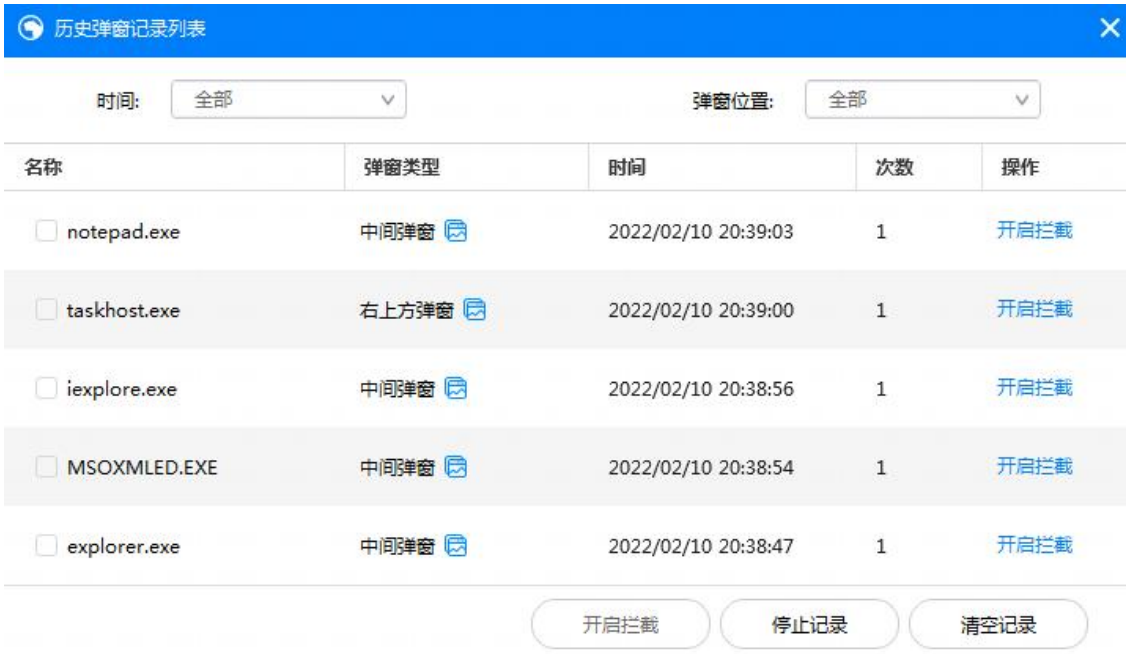
注：对于已添加的弹窗信息，支持查看和取消拦截。

9.6.2. 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。

9.7. 弹窗规则库更新设置

9.7.1. 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，支持按周、天、小时周期性自动更新。

9.7.2. 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。

9.8. 典型场景

9.8.1. 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。

9.8.2. 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。

9.8.3. 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。

10. 文件分发

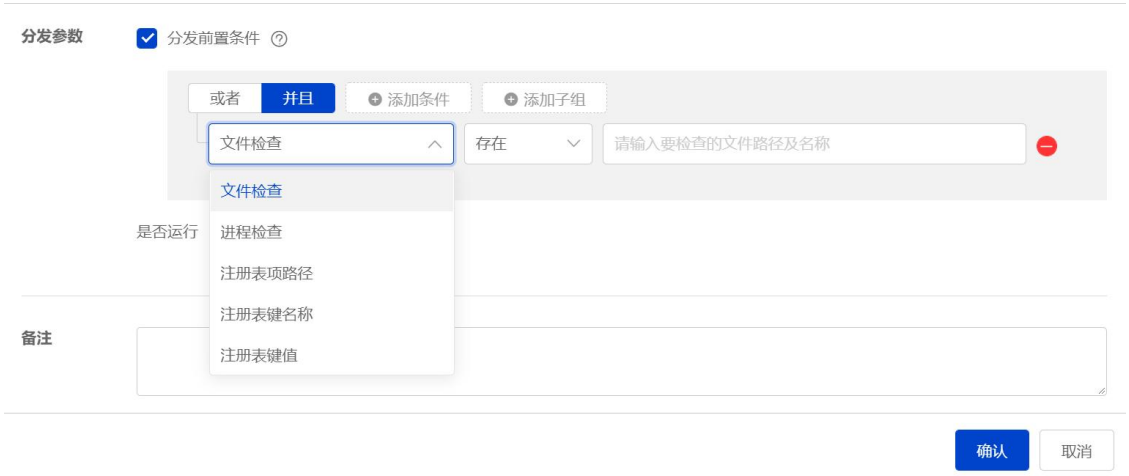
10.1. 基本概念

10.1.1. 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。

10.1.2. 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。

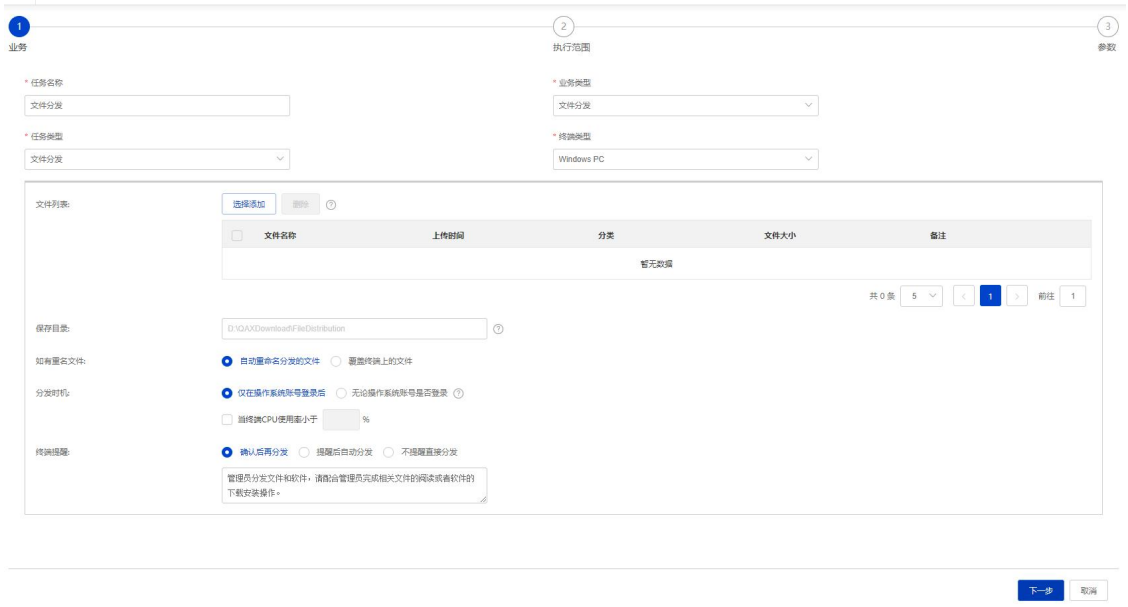


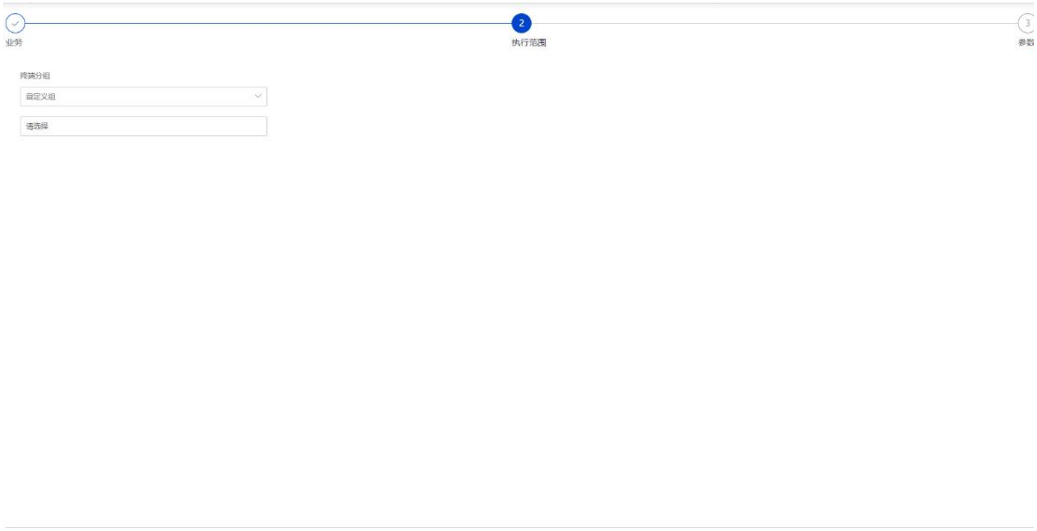
10.1.3. 筛选

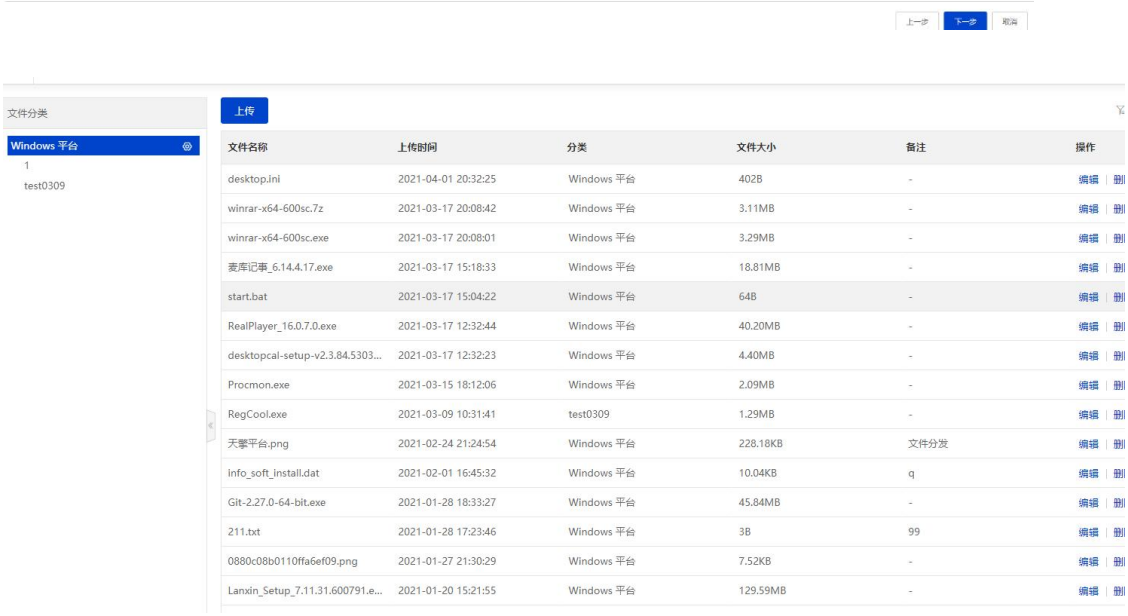
筛选是根据文件的文件名称，备注，文件大小，上传时间对当前分组中的文件进行筛选。筛选规则包括"包含"和"不包含"两种。

10.2. 分发策略管理

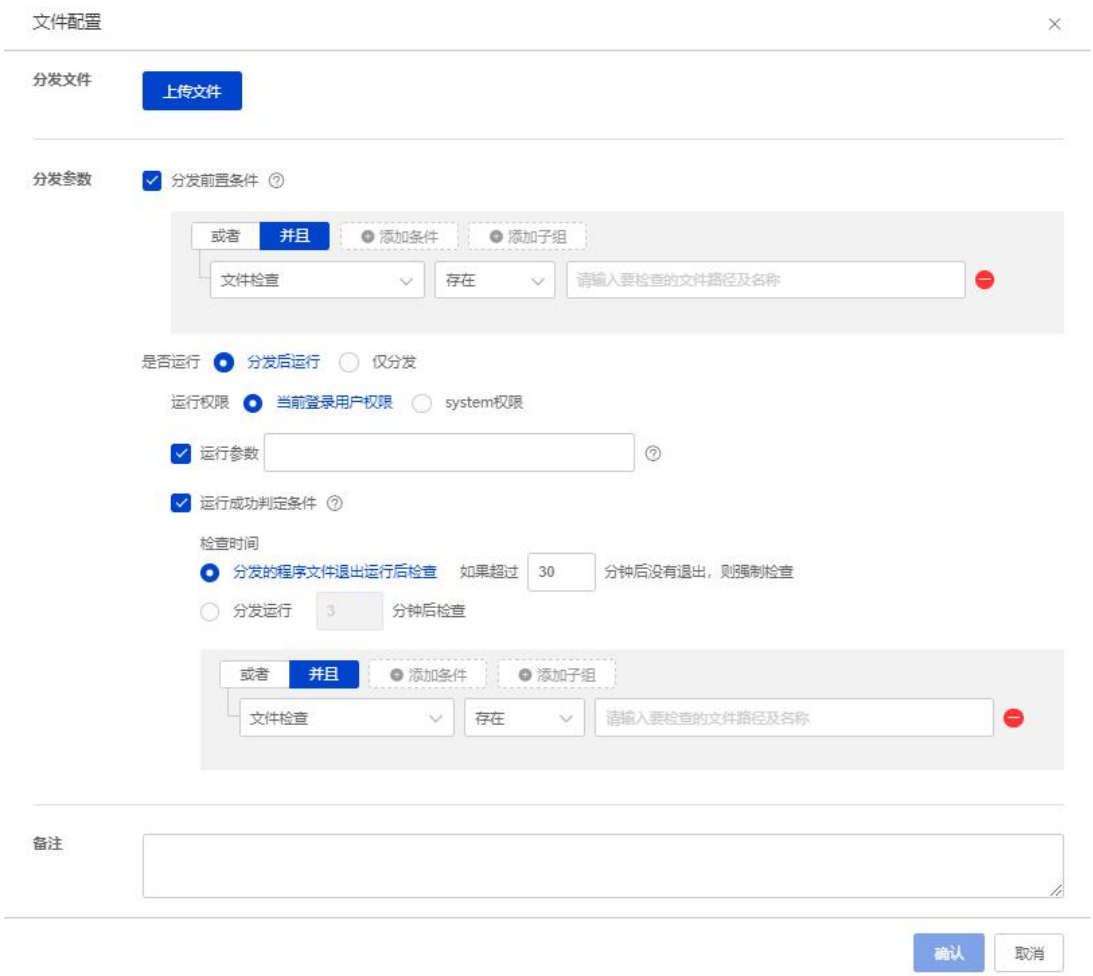
文件分发配置：在终端管理>终端任务中新建一个文件分发任务。在文件列表中添加已上传好的文件，设置保存路径和分发时间。最后选择需要下发的终端即可完成设置。







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。



10.3. 文件管理

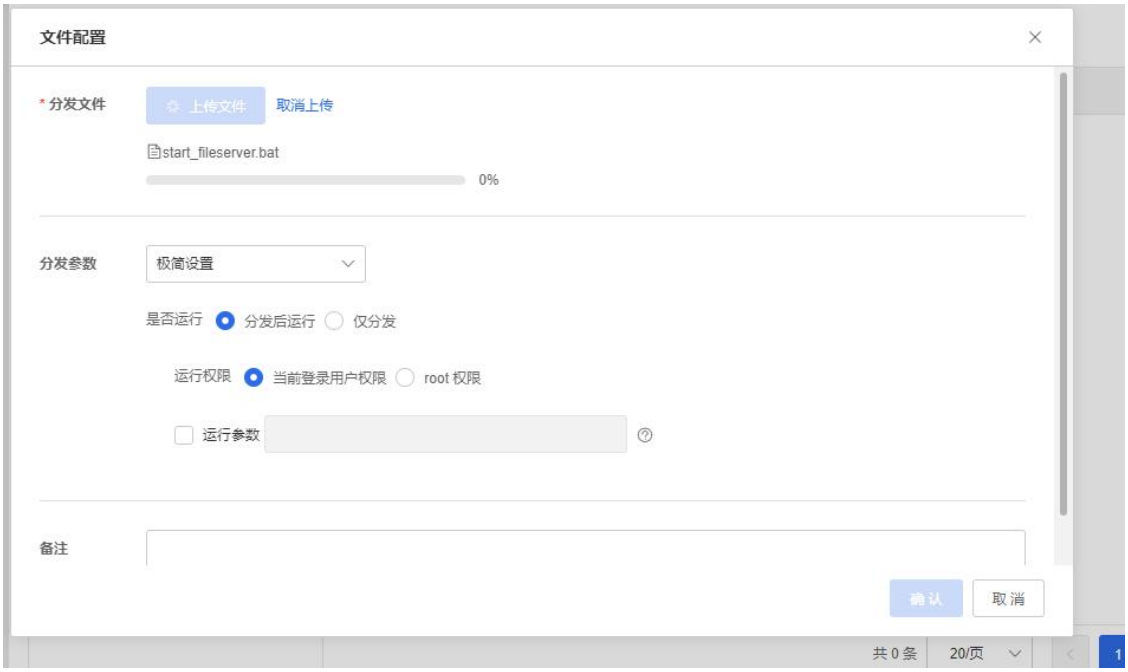
10.3.1. 文件分类

可以针对不同平台增加子分类

10.3.2. 上传文件

在对应分类下上传文件

上传前可对分发参数进行配置



11. 报表中心

基于仪表板可创建周期报告。

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。

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。

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。

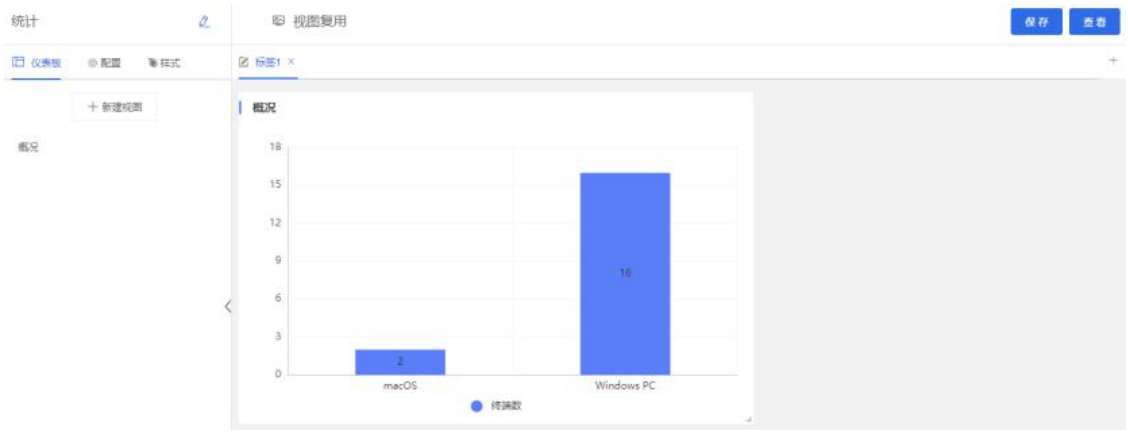
5)对单个仪表板支持查看、编辑、重命名、公开、复制、移动到、删除操作。

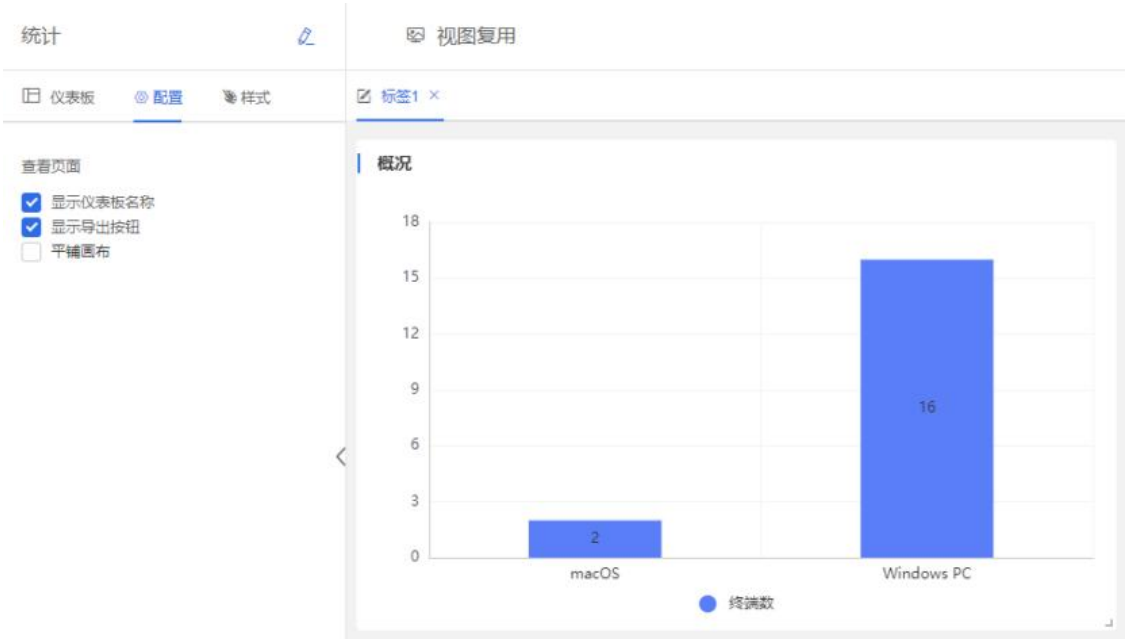
6)选择某个目录，点击[授权]，可将该目录下的仪表板授权给其他管理员查看、编辑的权限，有授权的管理员可在已授权目录查看到该仪表板。

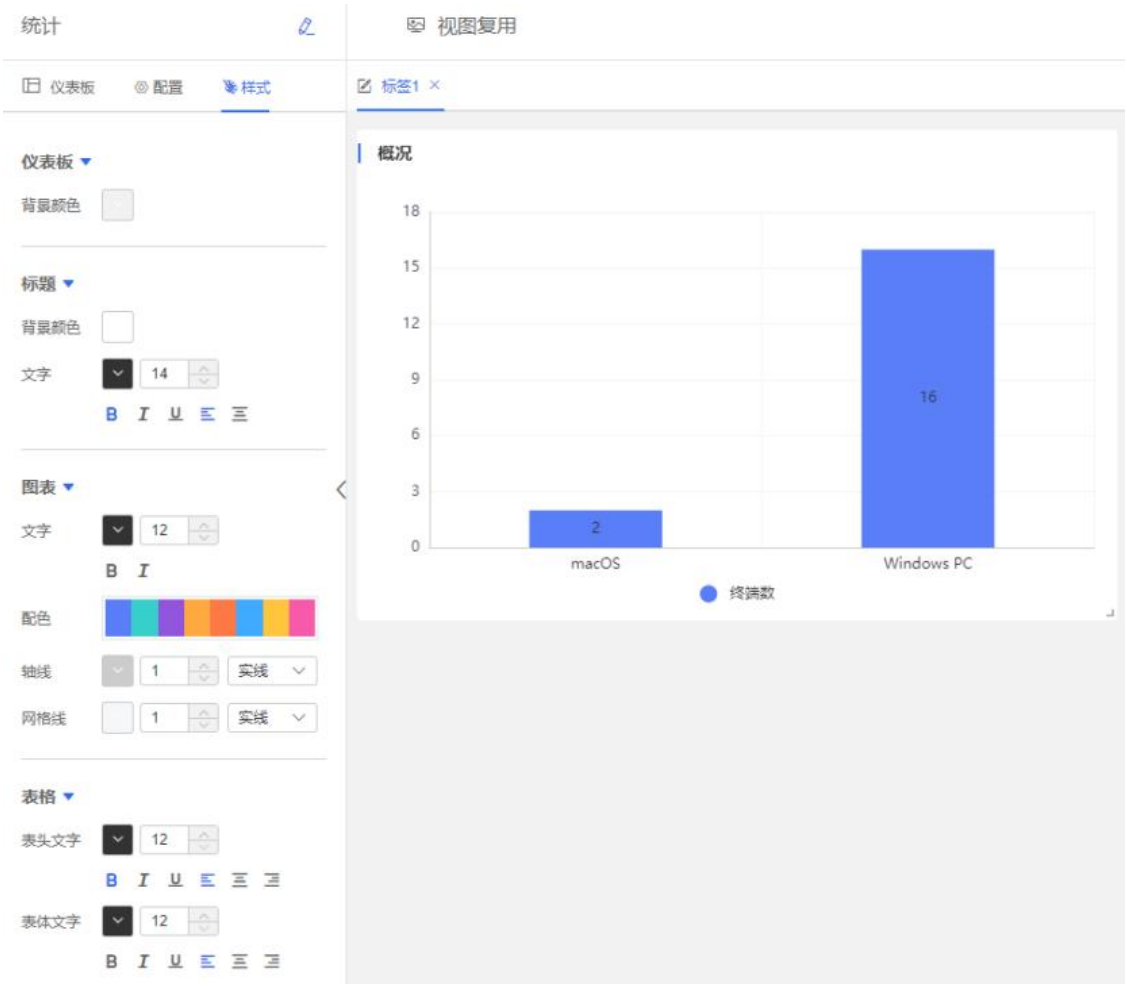
7)对仪表板进行公开操作，则所有管理员均可在公开目录下查看该仪表板。

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。

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。

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。

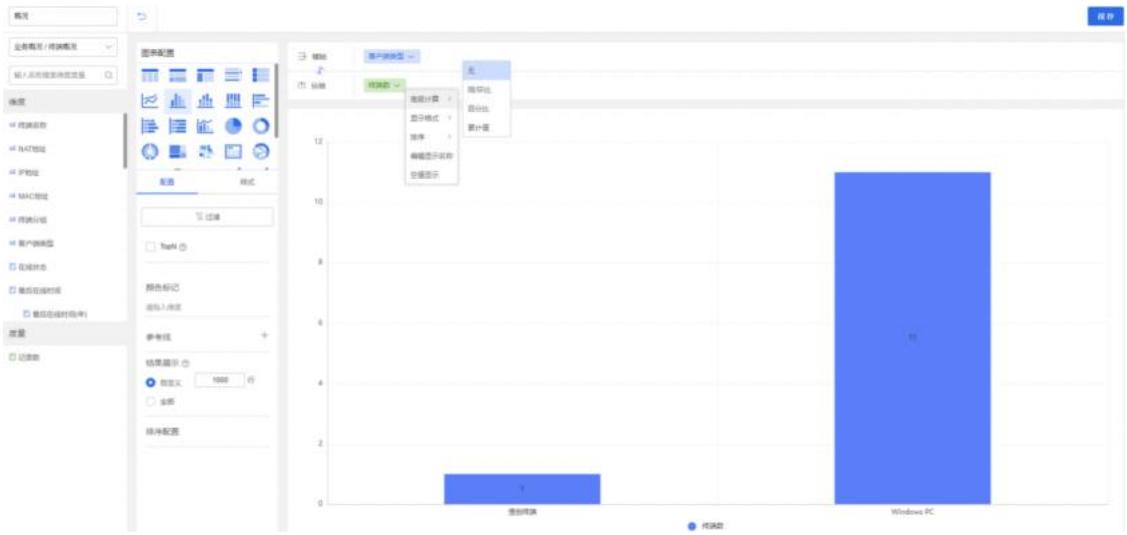
3)通过目录树可对视图进行分类管理。

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：

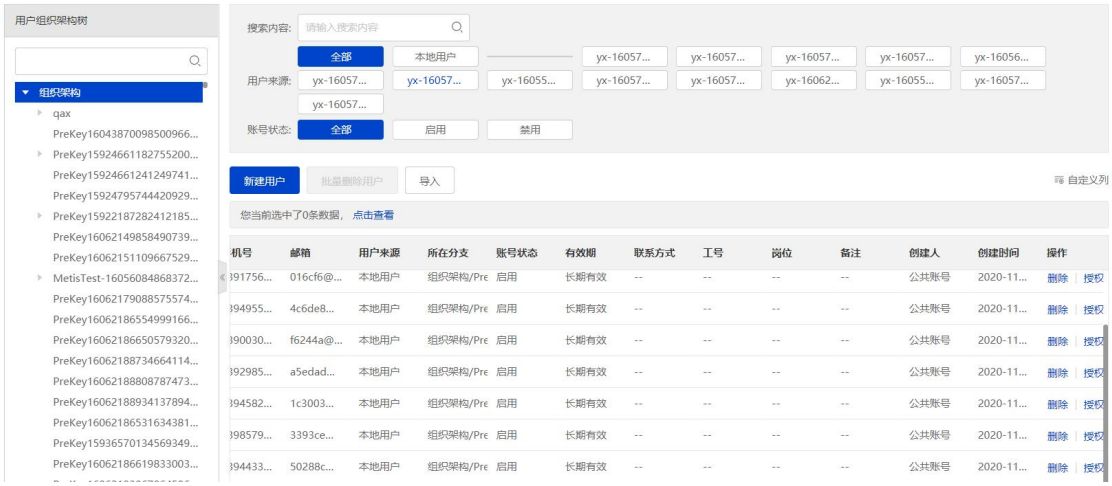
- 在左上角选择业务数据集
- 选择业务数据集后，在业务数据集下方展示该数据集下的维度字段和度量字段
- 在图表配置区域，选择图表类型后，在右侧区域上方展示该图表涉及的字段分类，将维度字段、度量字段拖拽到图表的字段分类后，在右侧区域的下方展示图表
- 在图表配置区域，可对图表进行配置、样式设置。
- 图表选择的字段，支持设置：显示格式、排序、显示名称，数值类型的字段支持设置高级计算。



12. 用户中心

12.1. 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。

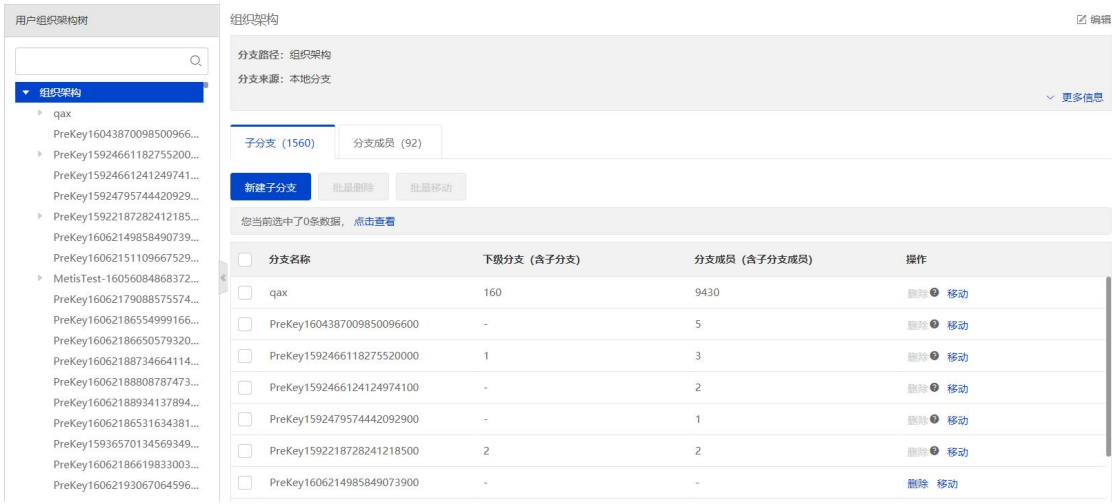


12.2. 组织架构

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。



12.3. 角色与权限

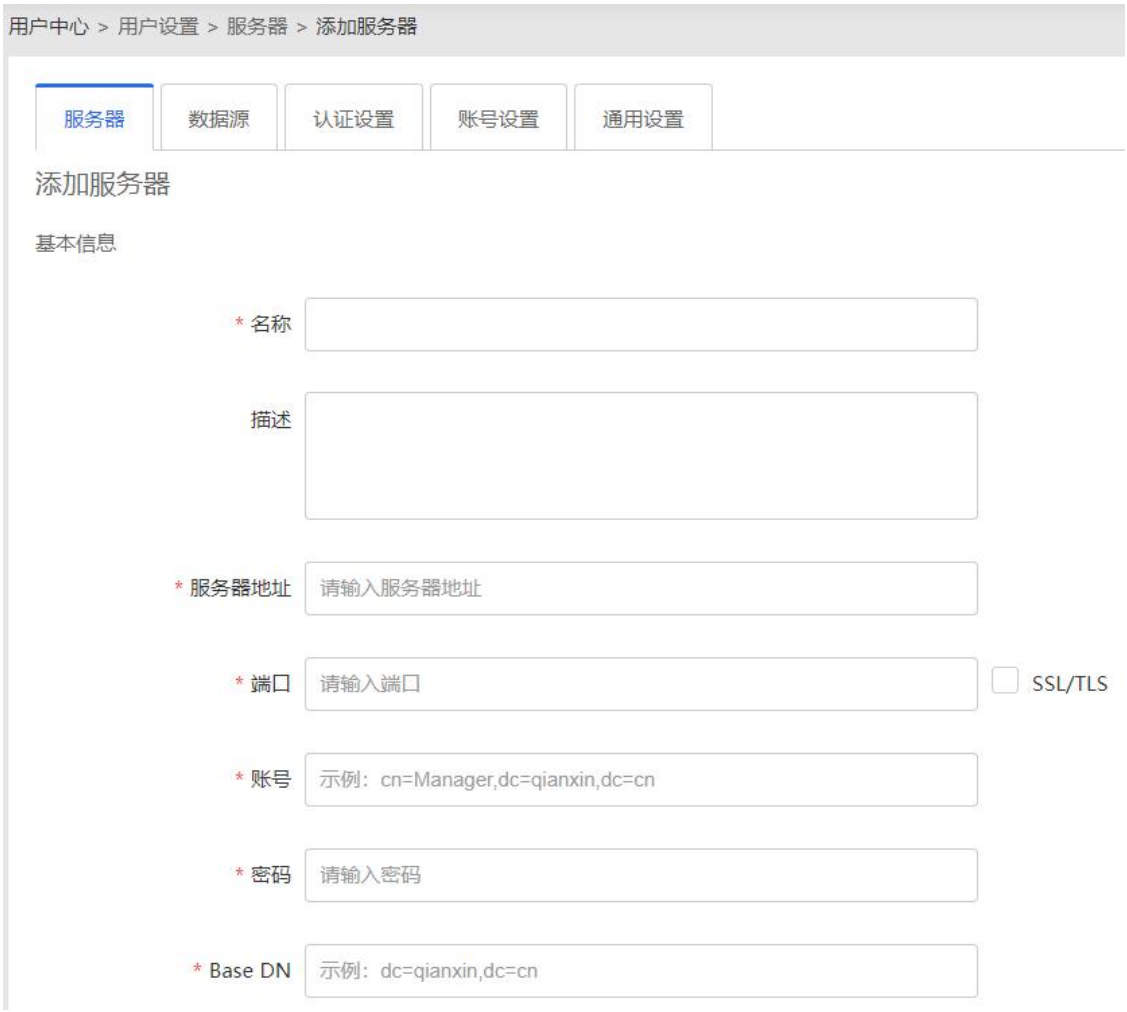
权限管理即管理员的权限管理，普通用户被授予管理员权限后则变为既是管理员也是普通用户。

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，可获得管理员权限

12.4. 用户设置

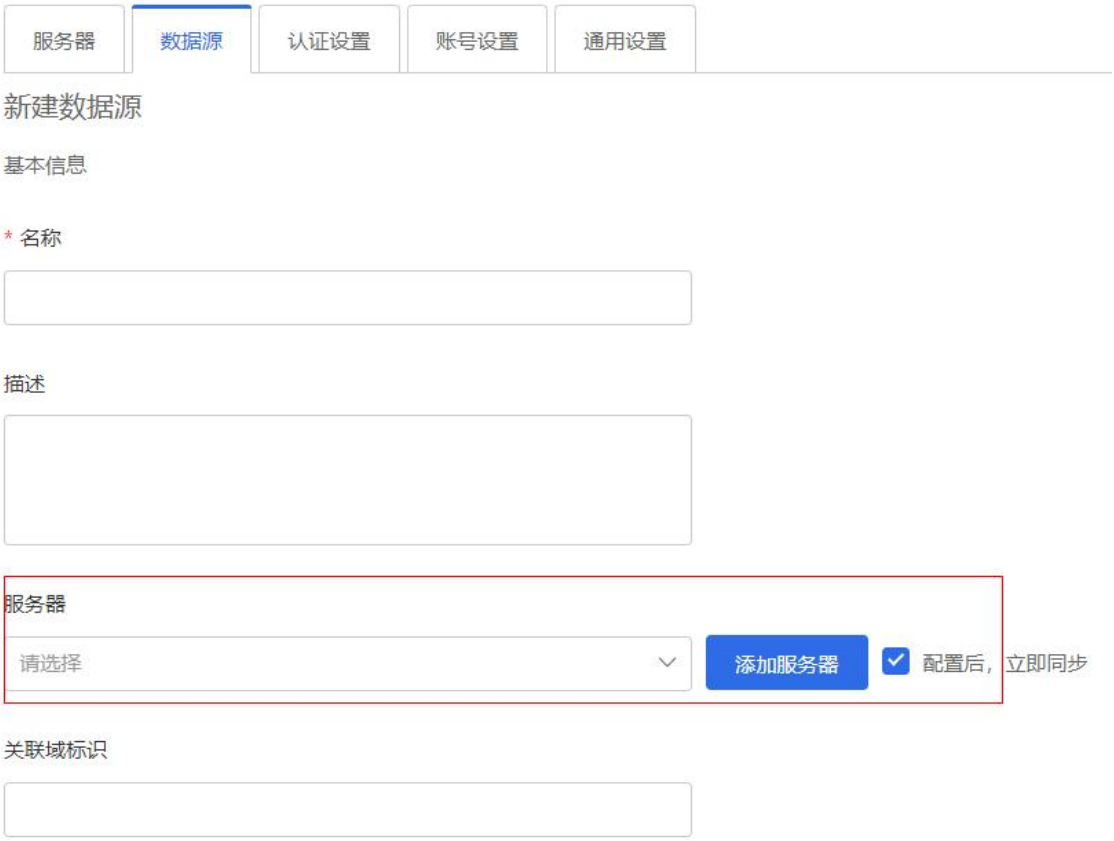
与用户相关的配置信息都在用户设置中，包含：服务器、数据源、账号设置、通用设置。

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。

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。

12.5. 个人中心

普通用户查看用户个人信息和修改密码。

13. 安全小助手

13.1. 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。

13.2. 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。

13.2.1. 基本功能

13.2.1.1. 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。

13.2.1.2. 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。

13.3. 垃圾清理库更新设置

13.3.1. 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。

13.3.2. 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。

13.4. 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。

13.4.1. 基本功能

13.4.1.1. 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" 

"，可自动隐藏已设置为禁用的启动项。

13.4.1.2. 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" 

"，可直接进行当前启动项的关闭/开启；

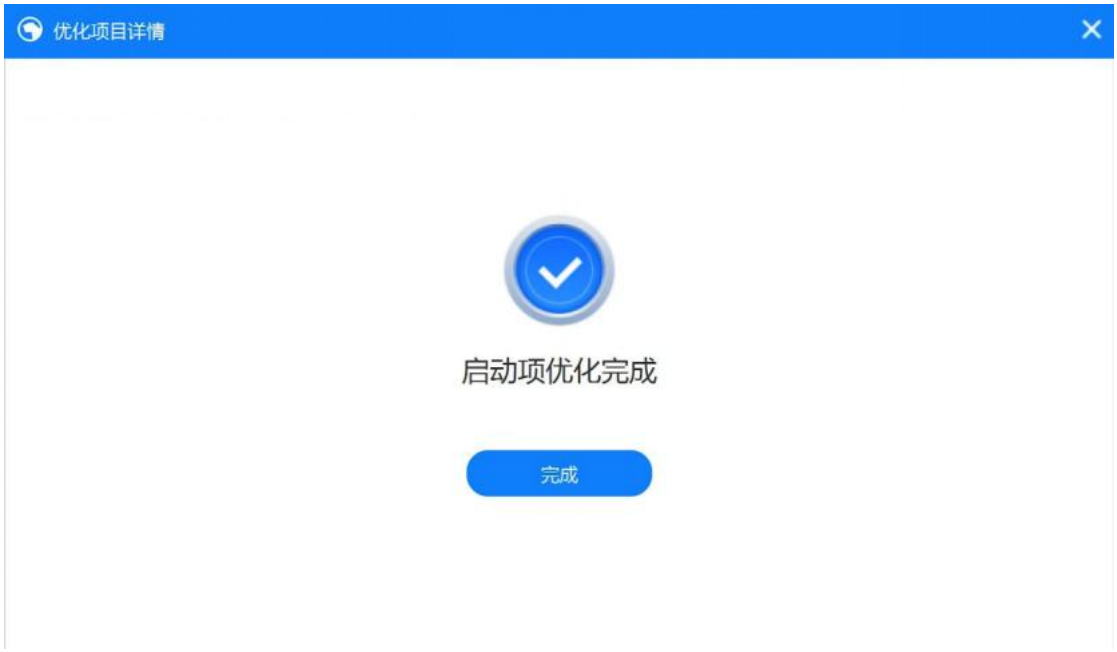
- 点击”  “，可展示当前启动项对应的操作菜单； 

- 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。

13.5. 启动项管理更新设置

13.5.1. 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。

13.5.2. 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。

14. 系统管理

14.1. 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、系统个性化设置等。

14.1.1. 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. 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。

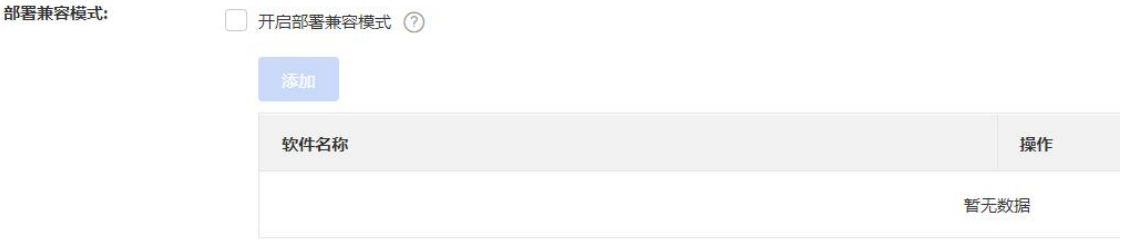
d. 管理中心语言设置可以限制支持的语言类型，设定后会影响登录页的语言选择。

e. 从管理中心下载文件限速。支持按照时间、终端 IP 地址网段、下载、上传限速。

f. 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。

g. 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。

h. 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。



i. 用户改善计划是为了持续改善天擎 EDR 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。

14.1.2. 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：终端管理>基础策略>资产登记

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

14.1.3. 个性化

个性化定制管理中心显示的产品名称和 Logo。

14.2. 业务设置

14.2.1. 文件分发

可以限制上传文件的类型、限制单个文件大小。

14.2.2. 补丁管理

若为隔离网部署，可设置自动清理过期的补丁文件。

14.2.3. 弹窗防护

可开启/管理弹窗防护云规则

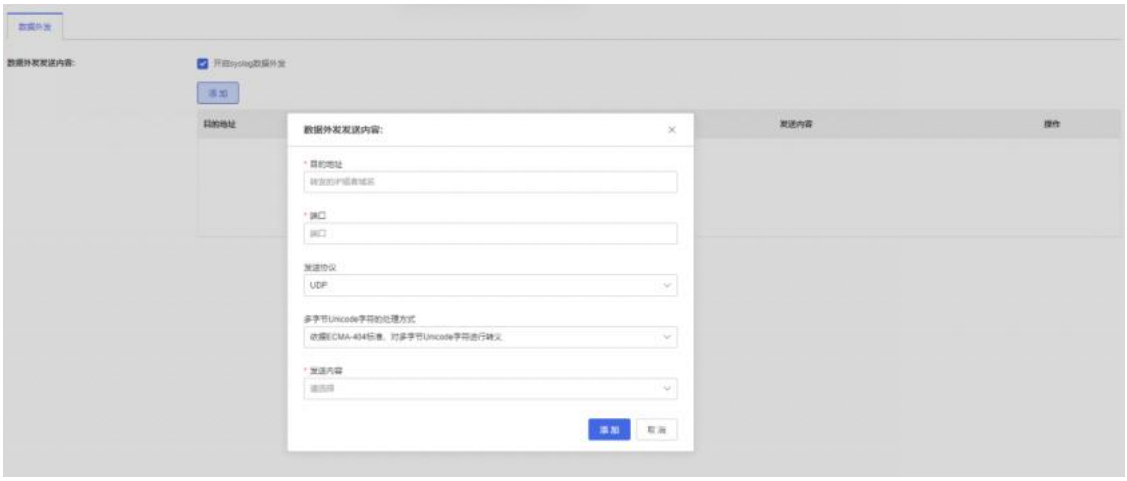
14.3. 安全设置

安全设置：云安全防护开关和并发云查数量限制、密码加密设置、验证码有效期设置。

在许可证管理中可查询客户的信任 ID。

14.4. 数据外发

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、补丁管理等等，有对应业务许可时方可展示和选择。



14.5. 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。

14.6. 更新管理

14.6.1. 基本概念

版本号

用于表示天擎 EDR 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，表示天擎 EDR 管理中心产品版本号。

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。

在线更新

在线更新指已经部署的天擎 EDR 管理中心统通过互联网获取奇安信公司云端最新版本的更新操作。

此操作主要对应天擎 EDR 管理中心上系统管理>更新管理菜单下服务器更新部分。具体操作可参考管理中心更新。

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。具体操作可参考离线工具更新。

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。天擎 EDR 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 **9200**。

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。

自动更新

自动更新包括天擎 EDR 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。

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。具体操作可参考终端更新。

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，同样包括天擎 EDR 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 2.2.1 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，具体操作可参考终端更新。

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，具体操作可参考管理系统更新。

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。

覆盖安装

覆盖安装是指使用同版本或高版本的天擎 EDR 安装包在本地再次执行安装过程。

14.6.2. 管理中心更新

天擎 EDR 管理中心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。

14.6.2.1. 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. 打开天擎 EDR 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。

14.6.2.2. 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. 打开天擎 EDR 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。打开天擎 EDR 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。


奇安信天擎离线升级工具
离线更新步骤
1
获取管理中心信息
2
从互联网下载更新数据
3
将更新数据更新到管理中心
版本：V10.1.0.2200
配置
中文(简体)

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。

14.6.2.3. 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. 打开天擎 EDR 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。

14.6.3. 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。

14.6.3.1. 终端更新配置

终端更新配置步骤（以主程序更新为例）：

1. 开启终端更新主程序并设置终端类型和例外。进入”系统管理>更新管理”，然后切换至”主程序更新”页面，勾选允许更新的终端类型，并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. 确定主程序的更新版本。开启灰度更新，并选择需灰度观察的版本；
    a. 选择”自动更新到最新版本”则可更新的灰度版本为当前管理中心的最新版本。

b. 选择”手动更新到指定版本”则需确定一个版本并指定为可更新版本（标记黄色星星且仅能指定一个），若切换更新方式需保证切换过去的版本高于当前版本。

3. 添加观察批次和观察时长。开启批次更新的按钮后，添加可以优先更新的组织结构或自定义组，让其下的终端优先更新并观察是否有重大问题；

4. 阻止有问题的版本在网内扩散。当发现当前更新的版本有问题时可以选择”回退稳定版本”，防止事态进一步在全网扩散；

5. 重新观察新的版本。支持选择配置当检查到新版本时，“等待所有批次完成观察后更新新版本”、“从第一批次重新开始灰度更新”。

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。

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**。

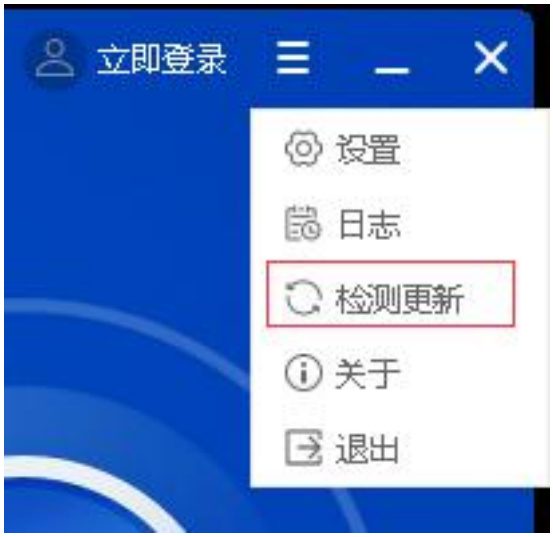
配置入口：终端管理-基础策略-通讯设置-下载源设置；

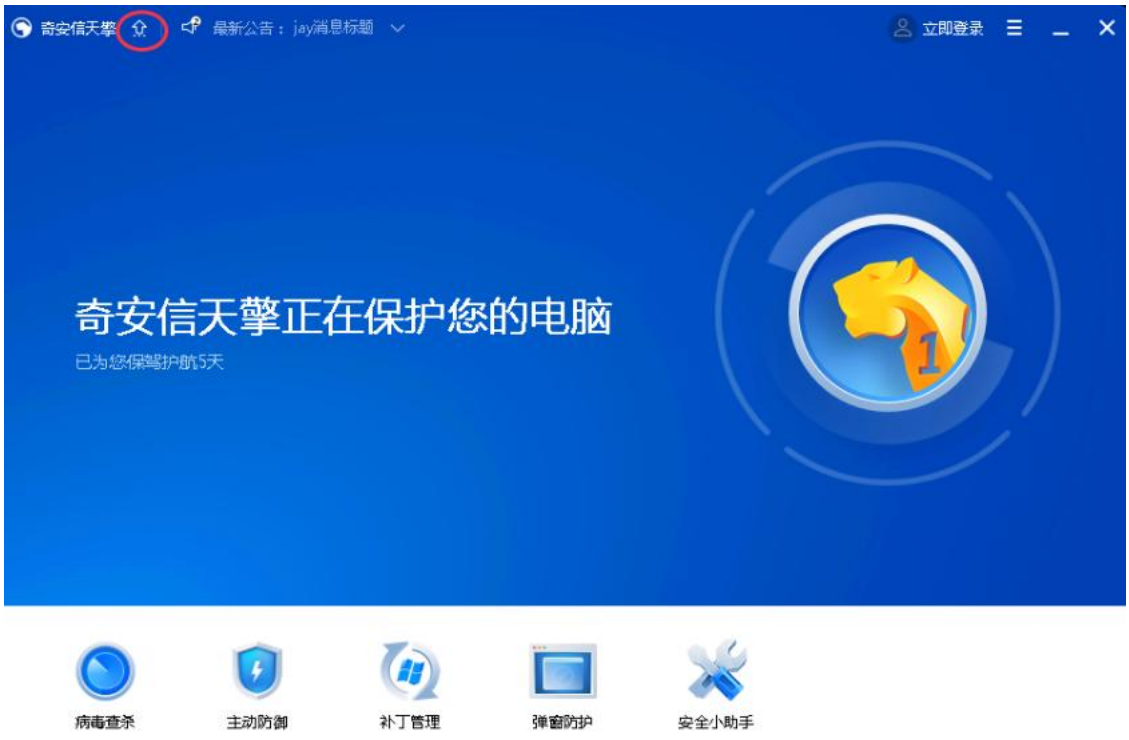
14.6.3.2. 在线更新

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。

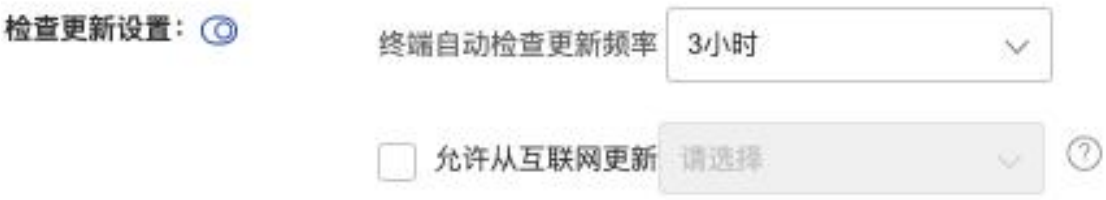
2. 触发更新后会弹出升级进度对话框，无更新则直接提示，有更新则等待更新完成即可。


立即登录
设置
日志
检测更新
关于
退出


奇安信天擎
最新公告：jay消息标题
立即登录
奇安信天擎正在保护您的电脑
已为您保驾护航5天
病毒查杀
主动防御
补丁管理
弹窗防护
安全小助手

在线自动更新步骤：

1. 在终端管理>基础策略>通讯设置中，设置终端自动更新检查频率；

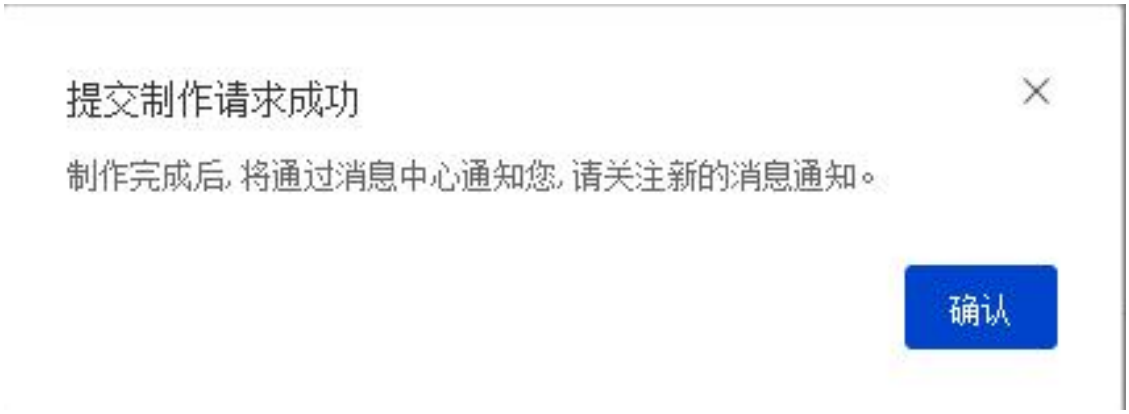


2. 在系统管理>更新管理，开启”允许终端更新主程序”等配置；

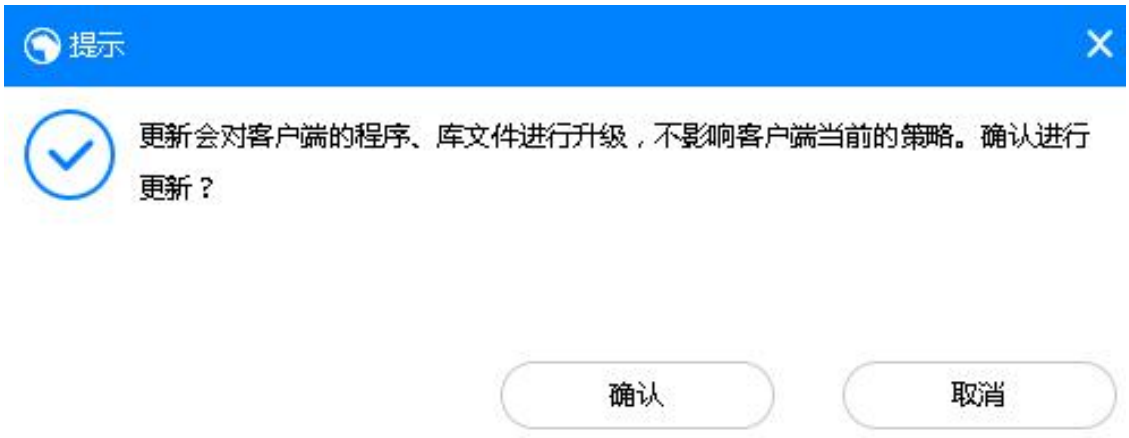
14.6.3.3. 离线更新

离线更新步骤：

1. 在管理中心制作离线更新包。打开天擎 EDR 管理中心并进入终端管理>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。

14.6.4. 典型场景

14.6.4.1. 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，在天擎 EDR 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. 打开天擎 EDR 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。

14.6.4.2. 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天擎 EDR 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基础设置>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）。

14.6.4.3. 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。

14.7. 运维管理

14.7.1. 系统备份与还原

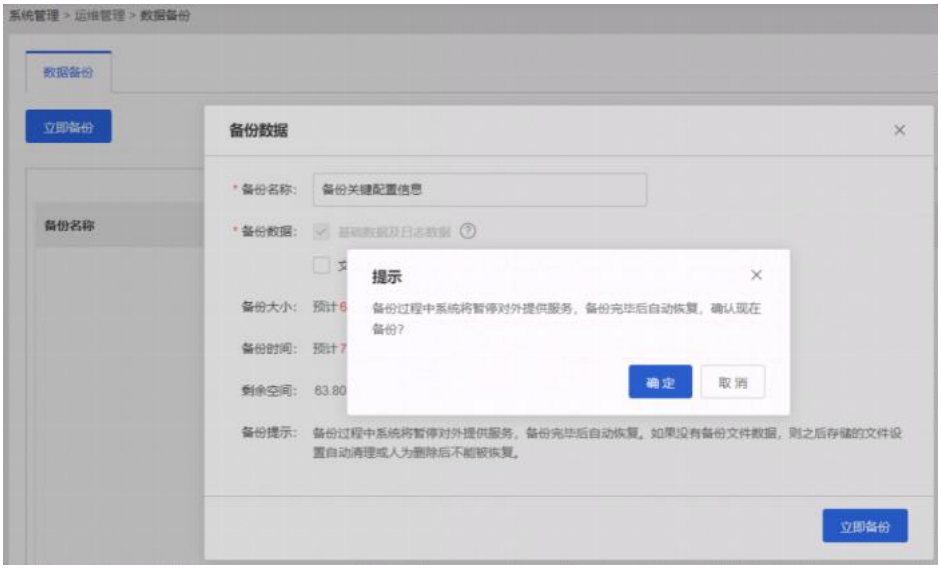
支持手动和自动定期备份管理系统所有的数据，包括系统配置、策略、日志。（暂时仅支持 Windows 服务器单机部署）

导航到”系统管理>运维管理”。

1. 打开”备份计划与配置”，配置备份文件保持路径(路径的末尾也需要配置分隔符)，目前仅支持备份在本机。

2. 配置自动备份周期或者手动备份。

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。



备份过程中展示备份进度。

备份成功之后将跳转到登录页。

3. 如有需要将备份的文件复制其他服务器保存,恢复数据时需要将备份文件复制到备份路径下。

4. 还原时，在管理中心选择已经备份的记录，点击还原按钮进行还原。（暂不支持重新部署管理系统后进行还原数据）。

14.8. 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。

14.9. 系统运行日志

14.9.1. 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。

14.9.2. 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。

14.10. 许可证管理

14.10.1. 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。

14.10.2. 许可证使用情况

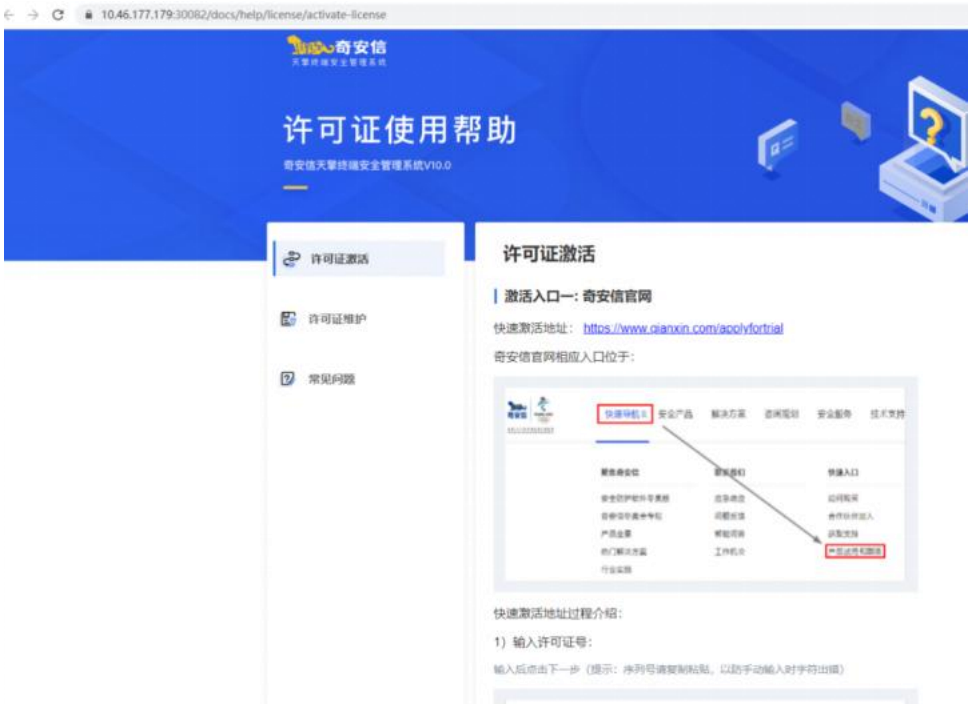
许可证使用情况主要提供购买模块在终端侧的使用情况的查看，支持分组搜索和查看自定义展示列及导出。

入口：系统管理>许可证管理>许可证使用情况。

14.10.3. 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。



14.11. 典型场景

14.11.1. 如何清理服务器磁盘空间

1. 可以在系统管理>业务设置功能中，清理补丁数据，节省磁盘空间；可以设置自动清理。

2. 可进入系统管理>日志清理，通过清理管理中心存储的历史日志数据，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。可参考系统管理>日志清理

14.11.2. 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。

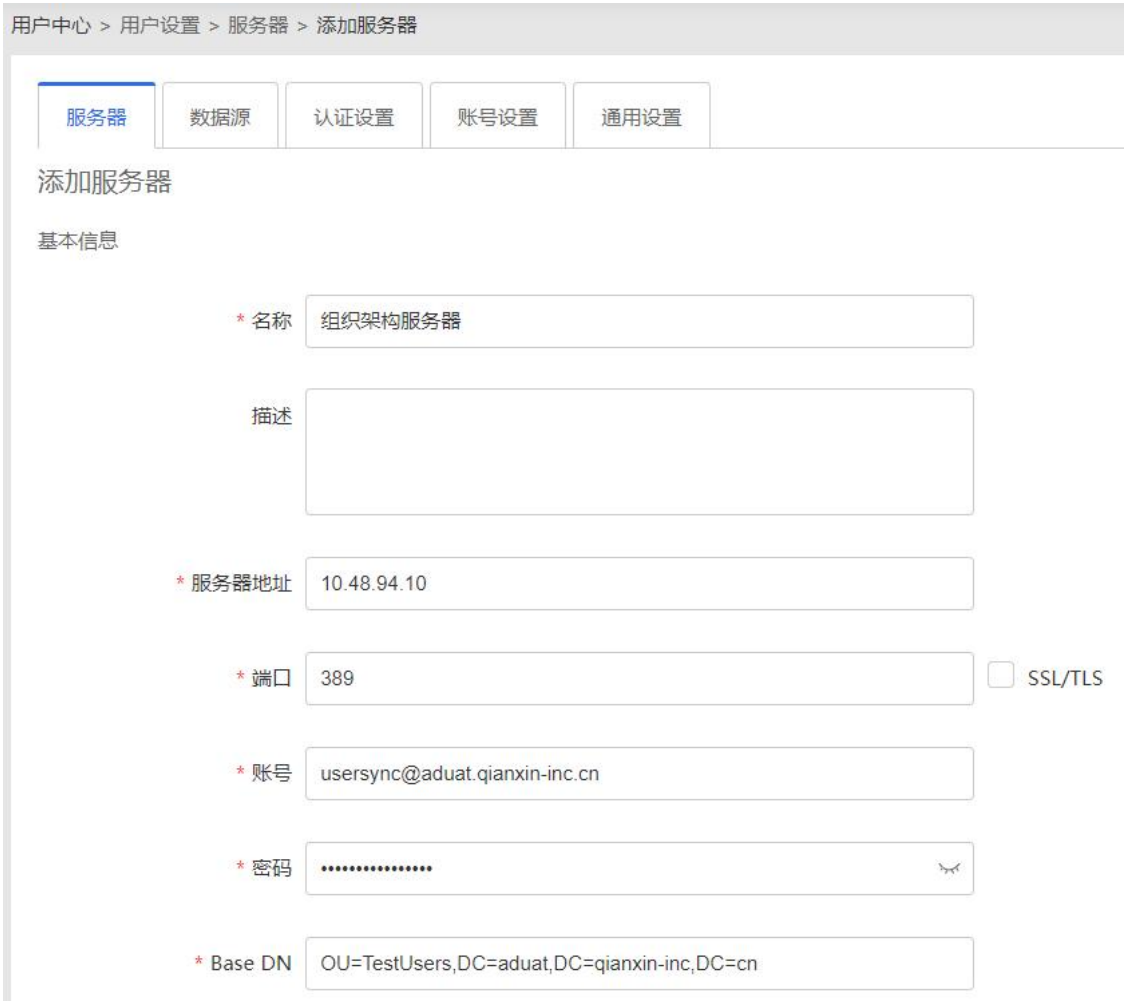
1. 配置 LDAP 服务器和认证源。

   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”管理中心>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：

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。

用户设置

完成服务器添加

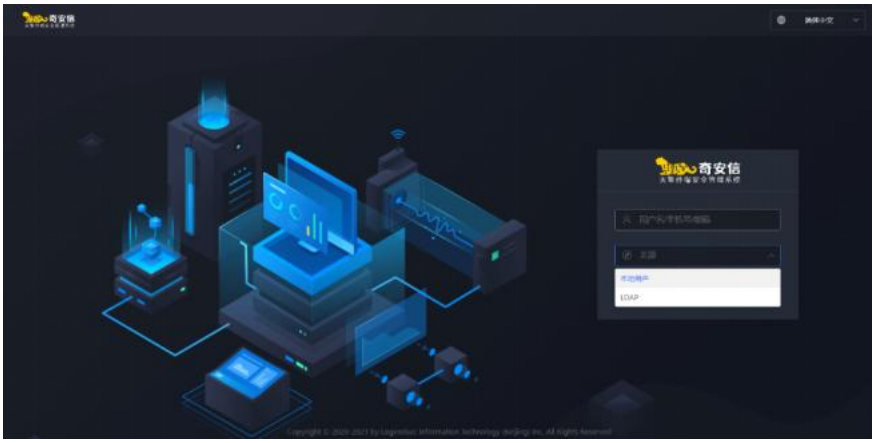
b. 添加数据源，同步组织架构。

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”管理中心>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。 |

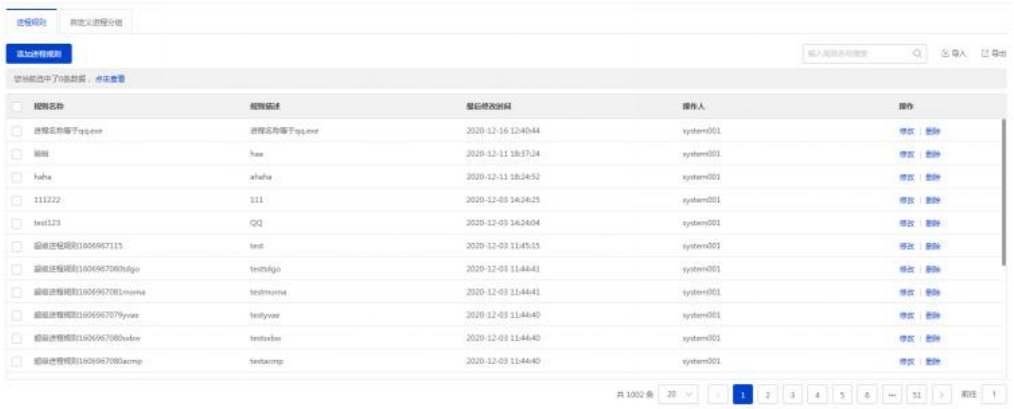
14.12. 知识库

14.12.1. 进程知识库

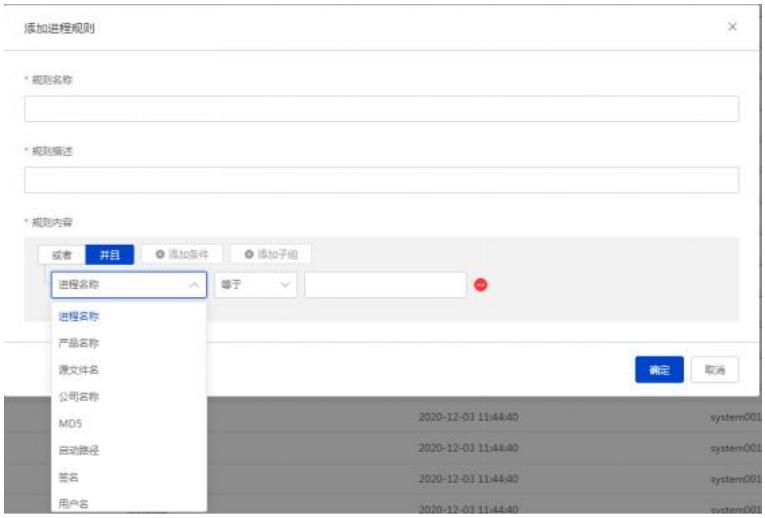
14.12.1.1. 基本概念

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。

14.12.1.2. 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。



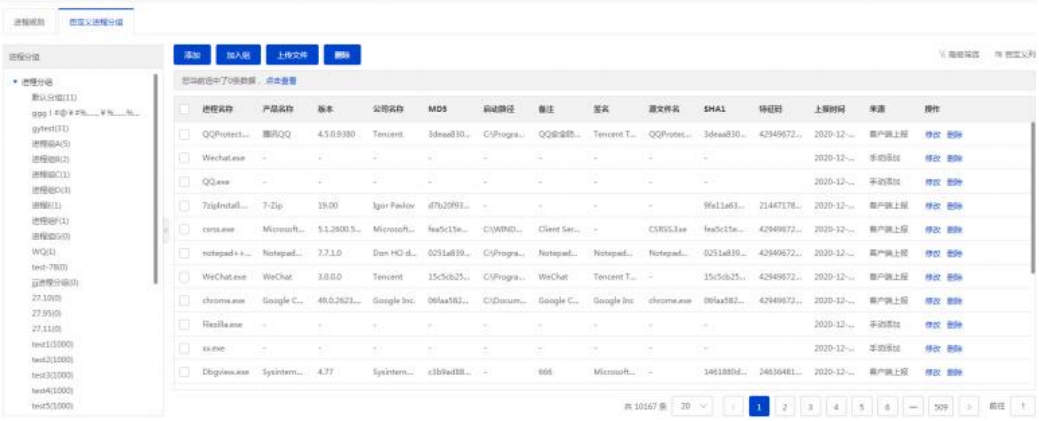
点击记录行的按钮[修改]，可对进程规则进行修改。

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。

14.12.1.3. 自定义进程规则

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）。

14.12.2. 外设库

14.12.2.1. 基本概念

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。

14.12.2.2. 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

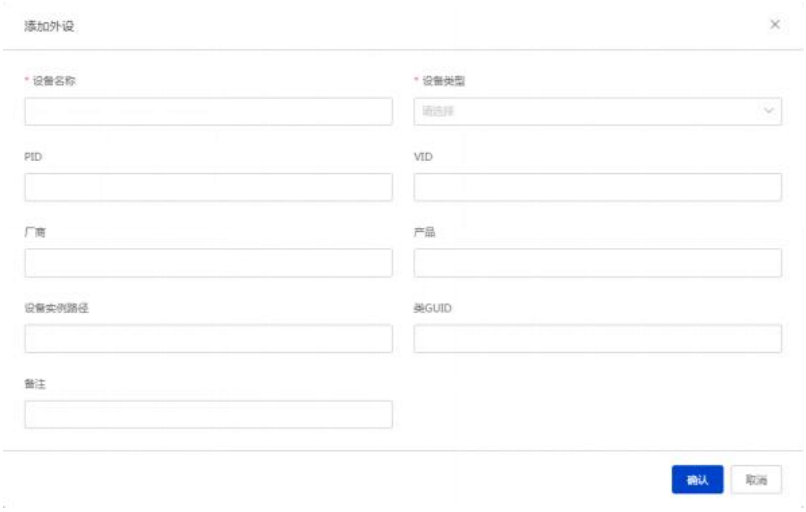
1）手工添加设备类型：鼠标移到左侧设备类型树的图标，点击弹出按钮[新建设备类型]，在弹出界面上输入类型名，点击[确定]，即可自定义设备类型。

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。

14.12.2.3. 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）。

14.12.2.4. 外设明细

仅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）。

14.12.2.5. 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。

14.12.3. WiFi 库

14.12.3.1. 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。

14.12.3.2. 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）

14.12.3.3. 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。


SSID导入
导入SSID数据信息
1. 请下载导入模板
下载模板
2. 在模板上按照以下规则填写
请下载模板，使用txt格式文件进行导入;
请按照模板中的格式，添加SSID信息再导入;
重复的数据会被覆盖;
3. 上传文件
上传文件
只能上传txt文件