瑞星 ESM 365

用户手册

北京瑞星网安技术股份有限公司

2019 年 8 月　中国·北京

目 录

1 账号注册

使用瑞星 ESM 365 前，需要先注册超级企业管理员账号。操作步骤如下：

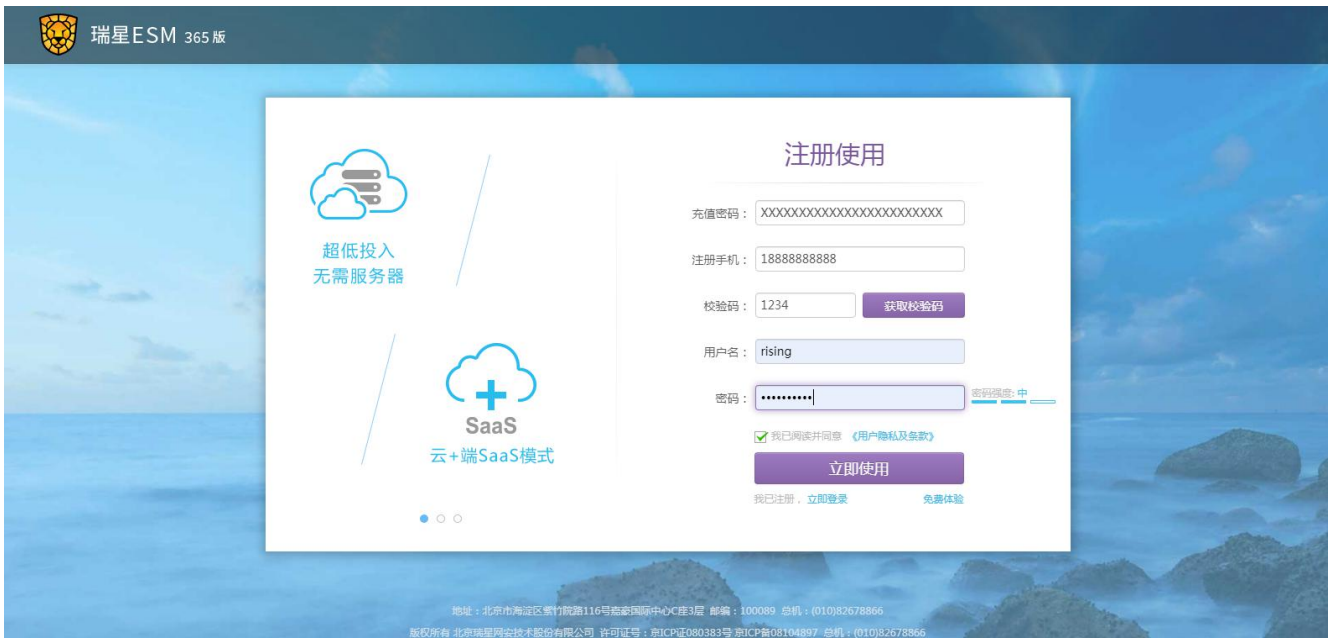
- **账号注册**

用浏览器访问 ESM 365 的注册地址：https://365.rising.cn/register，进入后界面如下图所示。

购买瑞星 ESM 365 后会获得充值卡，刮开充值卡背面的密码涂层，获得一组 20 位的充值密码。如下图。

在注册页面的【充值密码】处填入充值卡上的 20 位充值密码，输入手机号，点击【发送验证码】，将手机上收到的验证码输入【校验码】处。

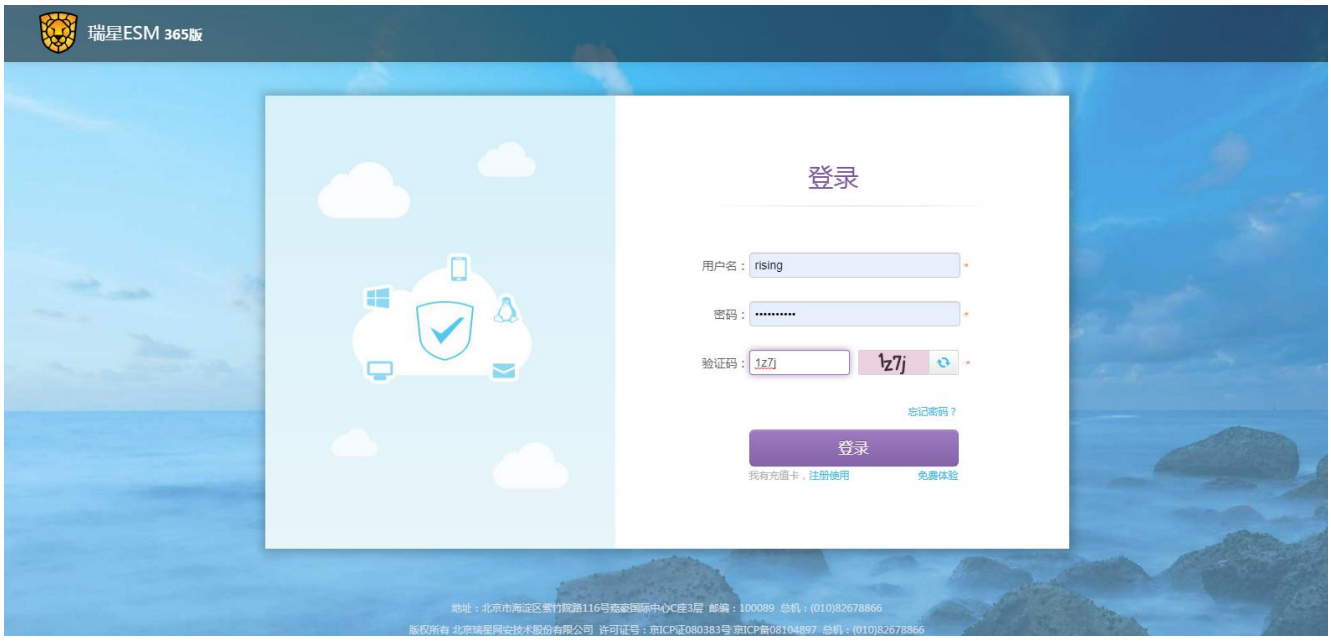
设置用户名（即超级企业管理员账号）和登录密码，勾选【用户服务协议】，点击【立即使用】，注册成功。以后可以通过手机号或者用户名登录账户。如图所示。



- **系统登录**

在浏览器访问 ESM 365 管理中心登录地址：https://esm365.rising.cn/login.html。

输入超级企业管理员账号（注册时的手机号或者用户名），输入密码和验证码，点击【登录】。



- **邮箱绑定**

需要绑定邮箱的用户，请登录系统后，在系统中心的账户信息中进行邮箱绑定。邮箱和手机号可用于密码找回，提高账号的安全性。

2 卡号充值

用注册时的账号登录管理中心，在安全中心或者授权管理页面，点击【立即充值】，进入充值页面。刮开充值卡涂层，将得到的密码输入输入框，点击【检测】，测试密码是否有效。充值成功后，可以在余额中查看余额增加。充值步骤如图所示。

授权管理页面可以查看用户授权状态。在账户概览中查阅账户的实时余额，消费详情等。

如下图所示为账户实时概览。展示了账户余额和赠送点数，今日消费点数，预计可使用天数，账户余额有效期等。

点击【收费标准】，可以查看最新的活动和基础服务收费标准以及拓展服务收费标准。

3 管理中心

成功注册超级管理员账户后，可以使用注册时的手机或者用户名登录系统，创建一个或多个安全管理员账号。安全管理员用于日常的终端管理和维护，超级企业管理员用于授权的维护和安全管理员的创建删除。

安全管理员的创建方式参考 3.1.7.3 用户管理。

3.1 超级企业管理员

使用超级企业管理员账号登录瑞星 ESM365 管理中心（地址：https://esm365.rising.cn/login.html），开始管理授权和账号。

3.1.1 安全中心

登录管理中心后，在安全中心页面可以看到终端的消息、通知、终端的流量、威胁数量、威胁类型和操作系统分布等。如图所示。

1.消息中心

消息中心可以查看中心的所有消息，包括已经绑定到中心的客户端的消息，通过点击消息分类进行分类查看，分类如图所示。

删除消息：将鼠标移动到某条消息上，消息右下角将显示图标，点击即可删除该条消息。

点击【查看更多】，进入消息中心的详细页面。

2.终端部署情况

终端部署情况主要展示的终端部署统计数据，如图所示。

区域上部展示的是 PC 端在线和离线数量及其百分比，移动端在线和离线数量及其百分比。加入中心的终端数量。

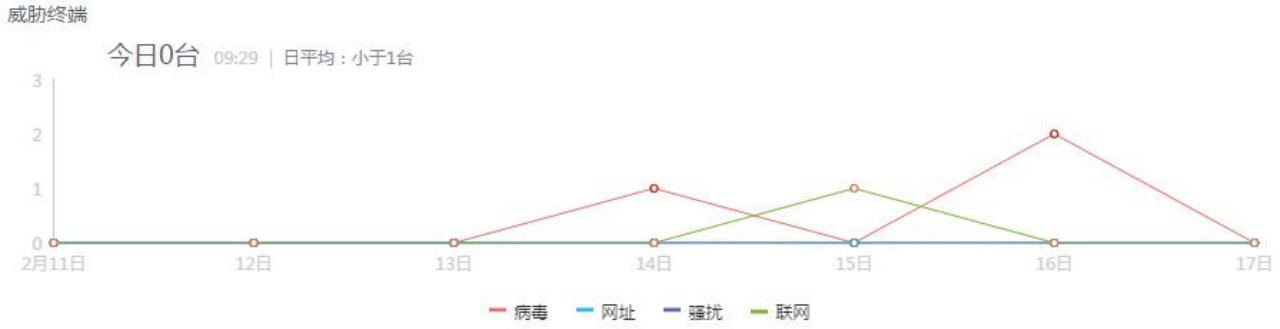
点击【全网升级】快捷键，可以快速进行全网升级，终端收到升级命令后自动更新客户端和病毒库。

点击【安装包下载】，可以进入安装包下载界面。将页面地址复制给客户端用户下载安装。例如地址为：https://esm365.rising.cn/Install/index/122。如图所示。

3.全网数据统计

全网数据统计展示了服务器性能监控、威胁终端、操作系统分布、病毒数量的统计图表。如图所示。

威胁终端：通过点击折线图下方的病毒、网址、骚扰和联网，让字体由灰色变成黑色，表示选中该项目，折线图将展示相应项目的图形。

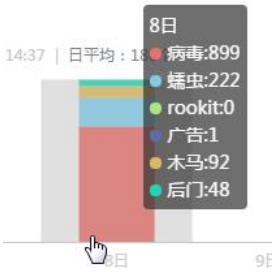


- **病毒数量**

病毒数量统计图表，展示了当日病毒数量，并计算出了本月日平均病毒数量。

下方图表则详细展示了每日病毒数量，每一类病毒各自的数量。如图所示。

将鼠标放在某日的统计图上，能看到当日病毒的详情，如图所示。



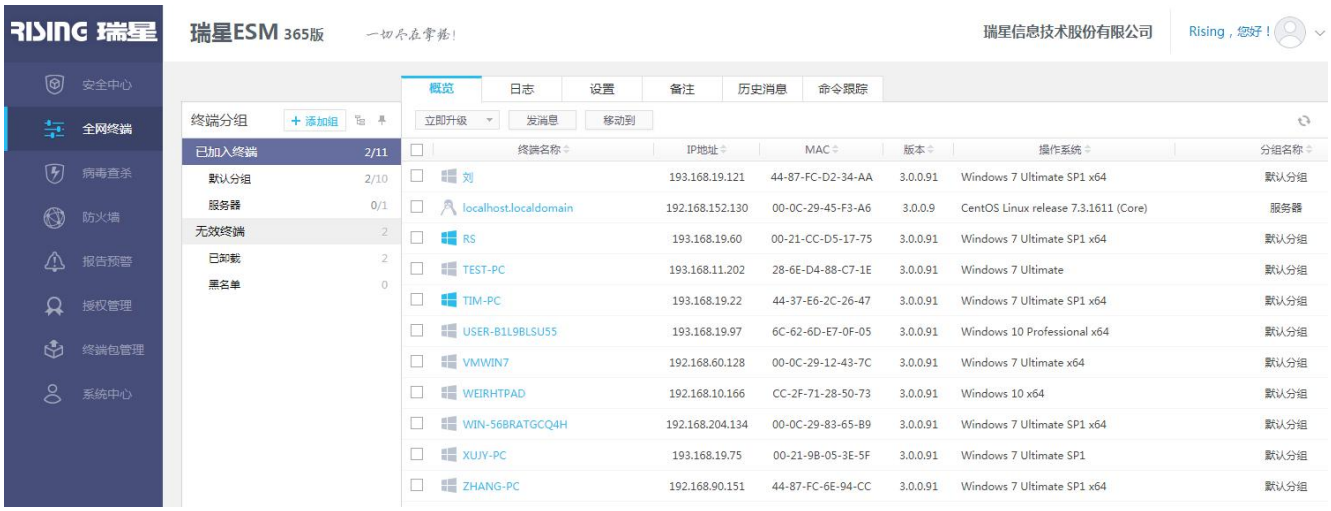
点击图表下的病毒、蠕虫、rookit、广告、木马和后门，可以选择（再次点击是取消）展示该类病毒统计图。

点击图表右上角的按染毒次数，图表则按染毒次数统计；点击按染毒文件，图表则按染毒文件数量统计。

点击某日的统计图表立方图，则进入该日病毒详情页面。

3.1.2 全网终端

全网终端展示网络内所有的终端的管理和升级情况，以及历史消息和终端执行命令的情况。选中已加入终端，可以查看所有终端，给所有终端发命令和消息，可以设置终端的入组和入组规则已经查看所有终端的历史消息和命令跟踪。

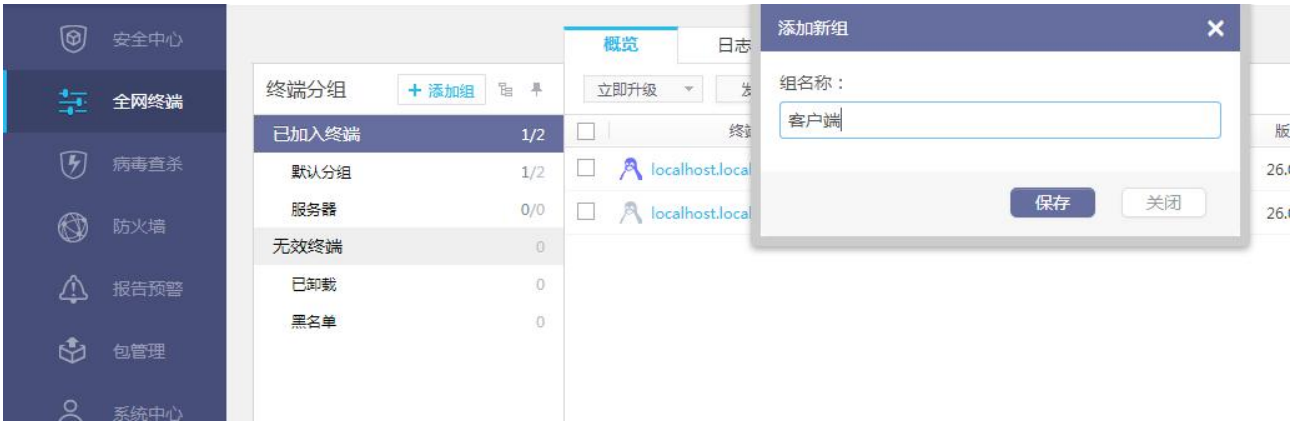


3.1.2.1 创建分组

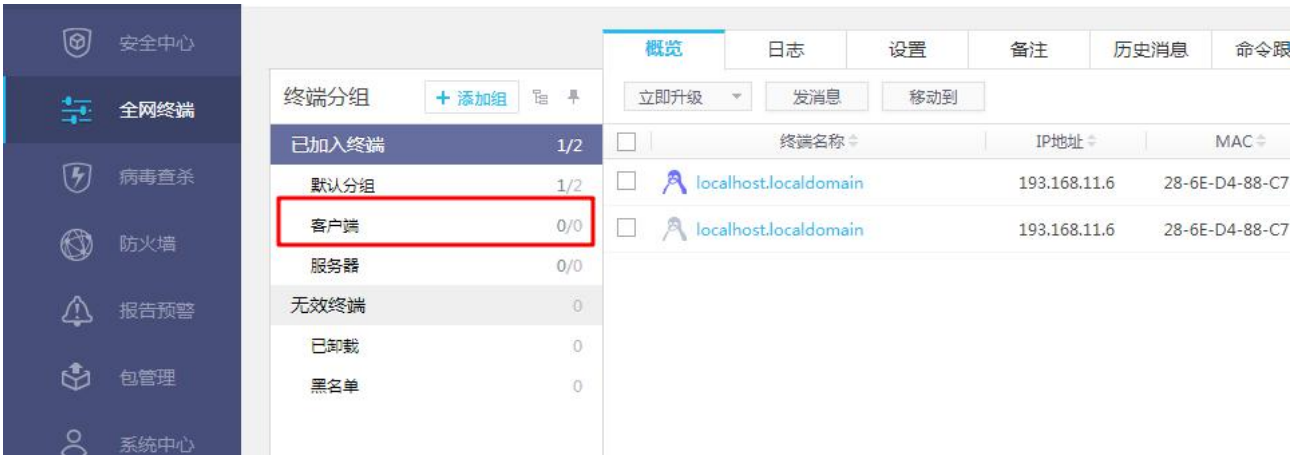
软件默认情况下有两类，一类是已加入终端，包括默认分组和服务器；另一类是无效终端，中心不能对失效的终端进行管理，包括已卸载和黑名单。

进入全网终端，在终端分组处点击【+添加分组】。位置如图中红框所示。

然后再弹出的框中填入分组名称，并保存。如：客户端。

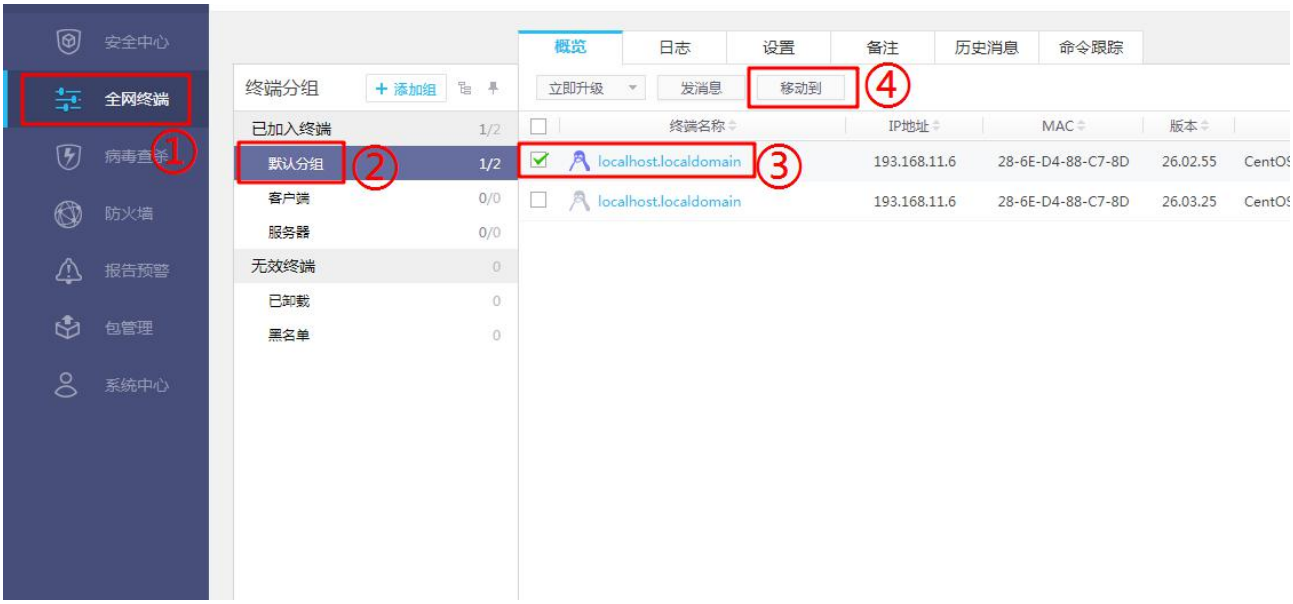


提示“分组添加成功”，在分组中也出现客户端的分组。

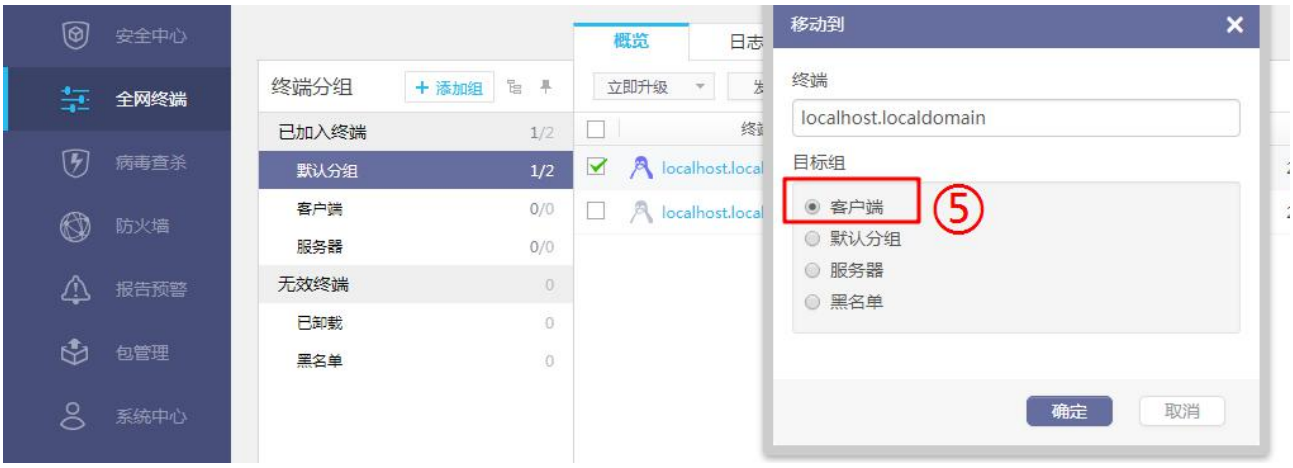


3.1.2.2 手动入组

当少量的终端需要换一个分组时，可用手动入组的方式实现。步骤如图序号所示。



依次点击全网终端->需要移动终端所在组->选中终端->移动到。然后选择新的分组，点击【确定】。



3.1.2.3 自动入组规则

依次点击全网终端->已加入终端->设置->自动入组，可以看到自动入组的服务器规则列表。如图。

自动入组规则设置步骤：

点击图中①处的【添加】，然后选择②处的分组。最后点击【选择】。创建新的入组规则。规则名为服务器。

创建新入组规则后，点击【IP 匹配规则】、【操作系统规则】、【计算机名称规则】等，可快捷设置入组规则。选择匹配条件（等于、包含等），填入匹配关键词。点击【应用】，以后符合匹配条件的客户端和服务器将自动进入规则所在组。

注意：多条规则的匹配关系是“且”，即必须同时匹配所有规则，才能入组。未匹配到分组规则的终端将留在默认分组中。

若要删除匹配规则中的某条规则，点击图中①处删除即可。若要删除整个规则，点击图中②处删除。图中③是让该规则优先级上升一位。图中④是让该规则优先级下降一位。

所有的自动入组规则设置完毕，点击右上角的【重新入组】，所有匹配条件的终端和服务器将自动进入到对应分组中，未匹配条件的终端将继续留在默认分组中。

3.1.2.4 概览

概览展示了所有终端，在列表中可以看到终端名称、终端 IP 地址、终端 MAC、终端软件版本、终端操作系统和分组名称。如图所示。

3.1.2.4.1终端升级

点击【全网终端】，在终端分组中点击需要升级的分组，列表中选择要升级的终端，点击标题栏的复选框可以一次性全选中（图中红框）。如图所示。

选择终端后，点击【立即升级】，可以对选择的瑞星终端升级，点击【立即修复】，可以对选择的终端进行修复。操作如图所示。

3.1.2.4.2发消息

点击【全网终端】，在终端分组中选择接收消息的分组，列表中选择目标组或者终端。在【概览】，点击

【发消息】，输入消息内容，点击【发送】，所选组或者终端将收到消息。

在历史消息中可以跟踪消息下发状态。如图所示。

3.1.2.4.3移动到

点击【全网终端】，选择分组，在终端列表中选择要移动的终端。在【概览】页面点击【移动到】，再选择窗口选择目标组，点击【确定】，所选终端将移动到目标组。如图所示。

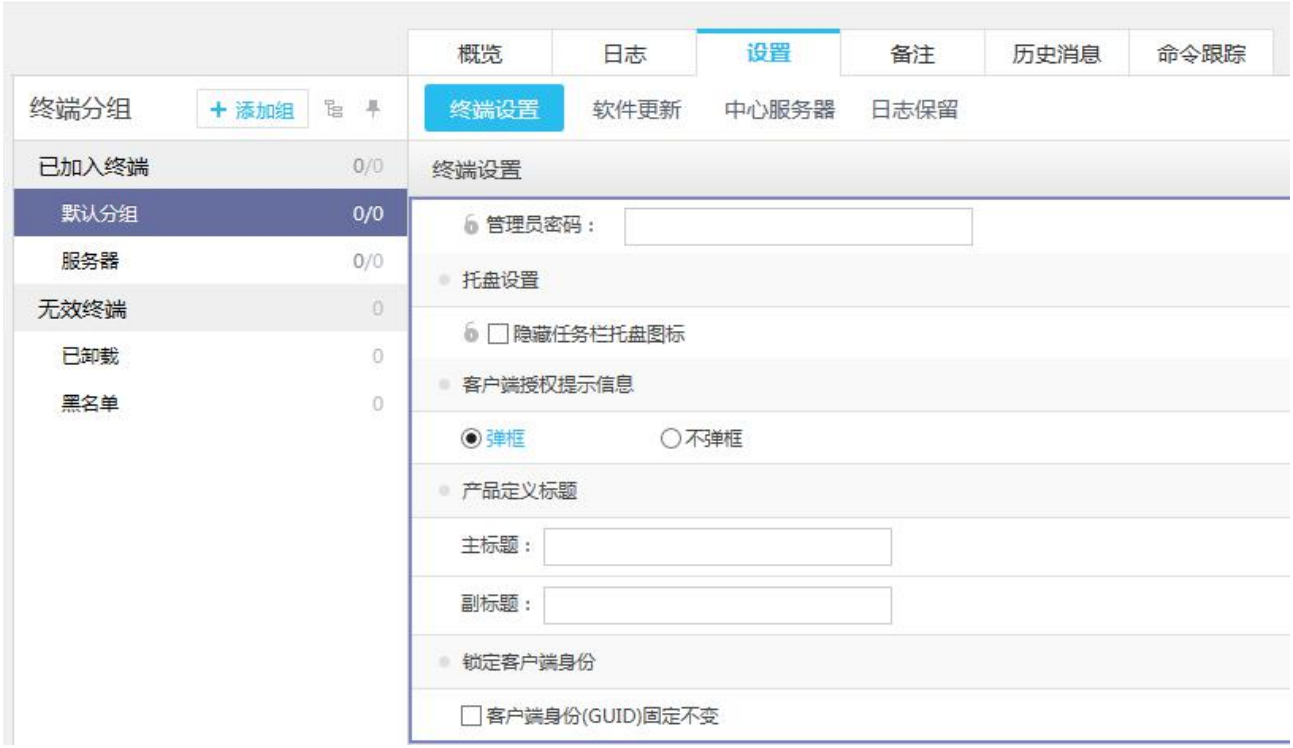
3.1.2.5 日志

日志界面集中显示所有终端的安装和升级日志信息。详细记录升级和安装记录，便于日志分析和问题排查。如图所示。

3.1.2.6 设置

3.1.2.6.1终端设置

首先进入需要设置的分组，然后点击【设置】，终端设置可设置终端的管理员密码和弹窗等。



管理员密码：设置管理员密码后，客户端的卸载和退出操作需要输入管理员密码才能完成。一般用于限制客户端自动退出和卸载。

托盘设置：可设置客户端任务栏的托盘图标显示或者隐藏。

客户端授权提示信息：根据实际需求设置客户端是否需要弹窗。

产品定义标题：主标题，用于设置客户端的主标题。副标题类似主标题。

锁定客户端身份：勾选锁定后，能保持客户端的 GUID 固定不变。针对某些客户端 GUID 频繁变化的弊端设置。

设置完成后，点击右下角【应用】。

3.1.2.6.2软件更新

软件更新用于设置更新内容、更新模式和代理设置。

升级内容：可选择升级所有组件或者仅仅升级病毒库。选择升级所有组件，可选择恶意网址库立即生效功能。

升级模式：三种模式，分别是手动、每天定时升级和指定日期定时升级。

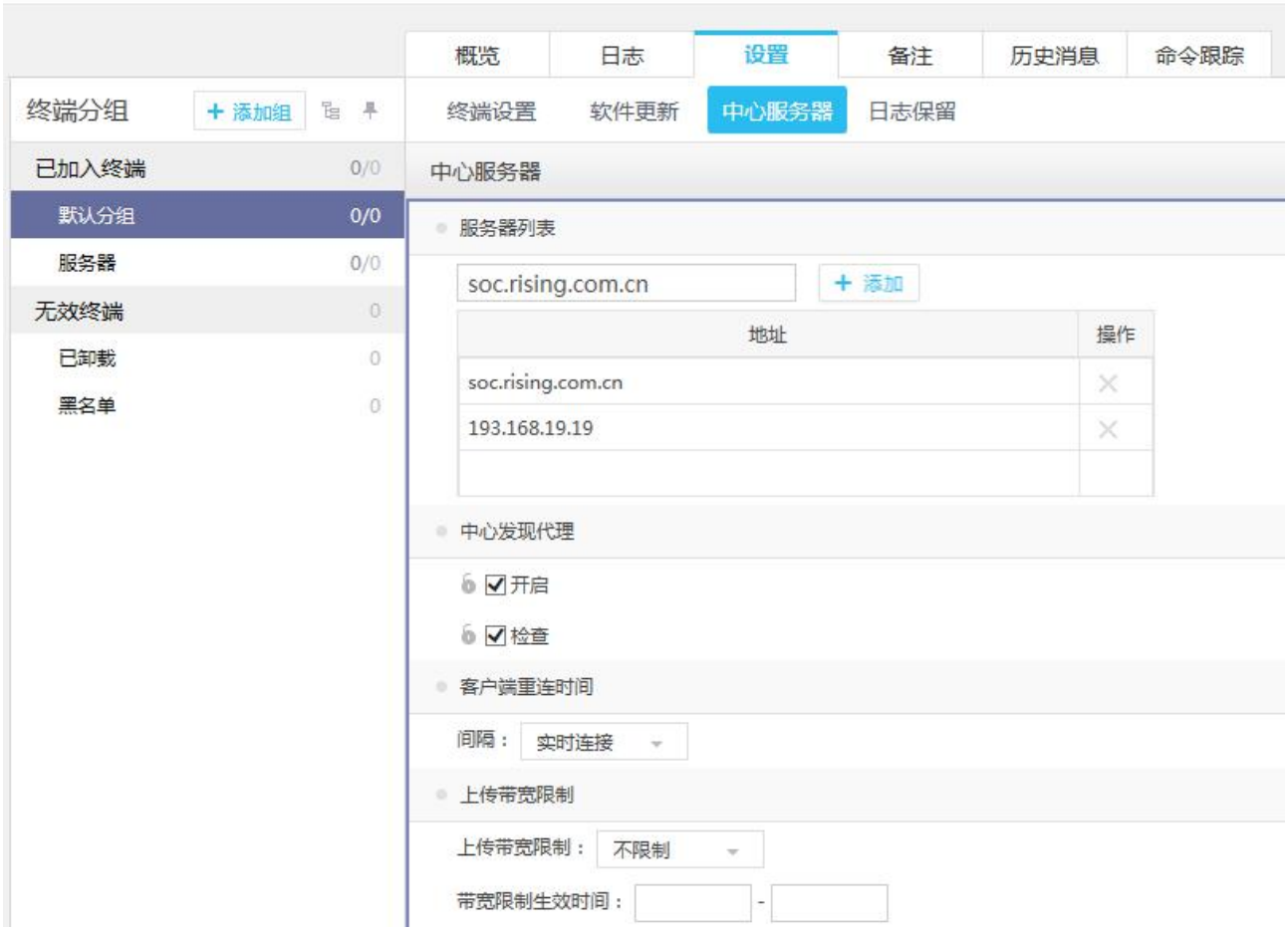
代理设置：需要通过代理联网的环境，请填写代理相关信息并保存。

设置完成后，点击右下角【应用】。

3.1.2.6.3中心服务器

服务器列表：用于添加中心服务的 IP 地址或者是域名。当前默认的中心服务器地址不能访问时，客户端将尝试访问列表中的地址。

中心发现代理：勾选【开启】，开启发现代理功能；勾选【检测】，实时检测代理服务器，发现后自动连接代理服务器。



客户端重连时间：可设置重连的时间间隔，可以为实时连接等

上传宽带限制：限制客户端上传的带宽，以及限制的生效时间范围。

设置完成后，点击右下角【应用】。

3.1.2.6.4日志保留

日志清理设置是定期清理日志，清理日志可以释放部分磁盘空间。

可以设置为定期自动清理，超过指定天数的日志会自动清理掉，还可以设置日志最大保留条数，请用户按需要进行设置。

3.1.2.7 备注

用于备注终端，便于识别和管理，直接在备注列输入备注内容，输入完毕自动保存。如图所示。

3.1.2.8 历史消息

历史消息记录的是中心对终端进行的操作，并显示操作执行状态。如图所示。

3.1.2.9 命令跟踪

命令跟踪记录了中心对终端发起的所有命令和命令执行情况，如图所示。

在命令跟踪列表中可以看到发起时间、命令类型、命令对象、下发状态和执行状态，便于企业管理员了解命令的执行情况。

3.1.3 病毒查杀

主要功能是远程操作终端，对终端进行设置。包括病毒查杀、文件监控、系统加固和应用加固等。还可以对病毒查杀的日志进行跟踪和操作。

3.1.3.1 概览

概览展示了所有终端的查杀情况，在列表中可以看到终端名称、IP 地址、病毒库版本、文件监控、系统加固和应用加固。如图所示。

在列表左上角，可以看到快速查杀、全盘查杀、文件监控、共享监控五个按钮。

在 Windows 端，当需要进行这五个操作时，在列表中勾选需要操作的终端，然后点击相应的操作按钮，则所勾选终端自动执行相应的操作，并弹出提示框，如图所示。

Linux 终端的命令执行方式类似。

3.1.3.1.1快速查杀

进入【病毒查杀】，选择终端分组，在【概览】列表中勾选目标组或者终端，点击快速查杀的【开始】。如图所示。

Windows 终端接收到中心的命令后，执行命令，进行快速查杀，如图所示。

要停止相应的操作，只需要将鼠标悬停在该操作上，然后点击弹出的【停止】按钮。

3.1.3.1.2全盘查杀

进入【病毒查杀】，选择终端分组，在【概览】列表中勾选目标组或者终端，点击全盘查杀的【开始】。如图所示。

Windows 终端接收到中心的命令后，执行命令，进行全盘杀，如图所示。

要停止相应的操作，只需要将鼠标悬停在该操作上，然后点击弹出的【停止】按钮。如图所示。

3.1.3.1.3文件监控

进入【病毒查杀】，选择终端分组，在【概览】列表中勾选目标组或者终端，点击文件监控的【开启】。如图所示。

Windows 终端接收到中心的命令后，启用文件监控功能，如图所示。

要停止相应的操作，只需要将鼠标悬停在该操作上，然后点击弹出的【关闭】按钮。如图所示。

终端的文件监控即关闭，如图所示。

3.1.3.1.4邮件监控

进入【病毒查杀】，选择终端分组，在【概览】列表中勾选目标组或者终端，点击邮件监控的【开启】。如图所示。

Windows 终端接收到中心的命令后，启用邮件监控功能，如图所示。

要停止相应的操作，只需要将鼠标悬停在该操作上，然后点击弹出的【关闭】按钮。如图所示。

终端的邮件监控即关闭，如图所示。

3.1.3.1.5共享监控

进入【病毒查杀】，选择终端分组，在【概览】列表中勾选目标组或者终端，点击共享监控的【开启】。如图所示。

Windows 终端接收到中心的命令后，启用共享监控功能，如图所示。

要停止相应的操作，只需要将鼠标悬停在该操作上，然后点击弹出的【关闭】按钮。如图所示。

终端的共享监控即关闭，如图所示。

3.1.3.2 日志

日志界面集中显示所有终端的病毒扫描等日志信息。如图所示。

日志主要显示病毒详情、扫描事件、系统加固和应用加固的日志。分别点击相应的项目，即可查看对应的日志，这里以病毒详情为例，其他项目类似。

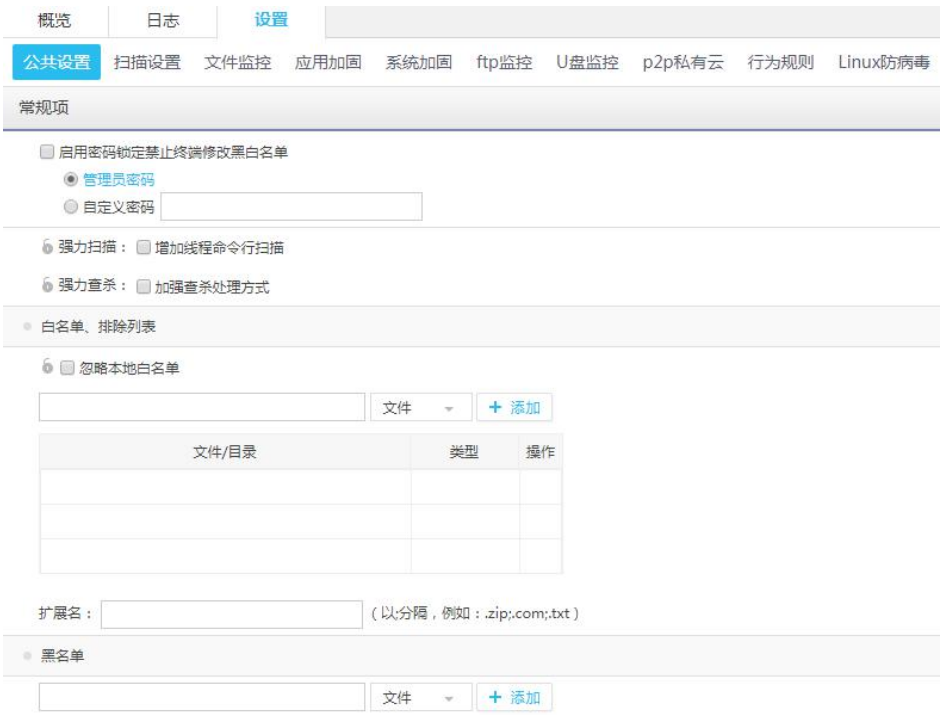
同样，可以通过点击右侧的分类显示按钮【按病毒显示】、【按终端显示】、【按详情显示】，实现按照不同按钮显示日志。如图所示为【按详情显示】。

按病毒显示 按终端显示 按详情显示

时间	终端名称	IP地址	染毒文件	威胁类型	病毒名	来源	状态
2016-12-14 09:49:21	最新加入的Win...	192.168.43.129	C:\USERS\ADMINI...	病毒	Win32.Expiro.b	文件监控	清除成功
2016-12-14 09:49:21	最新加入的Win...	192.168.43.129	C:\USERS\ADMINI...	病毒	Win32.Expiro.b	文件监控	清除成功
2016-12-14 09:49:21	最新加入的Win...	192.168.43.129	C:\USERS\ADMINI...	病毒	Win32.Expiro.b	文件监控	清除成功
2016-12-14 09:49:20	最新加入的Win...	192.168.43.129	C:\USERS\ADMINI...	病毒	Win32.Expiro.b	文件监控	清除成功
2016-12-14 09:49:20	最新加入的Win...	192.168.43.129	C:\USERS\ADMINI...	病毒	Win32.Expiro.b	文件监控	清除成功
2016-12-14 09:49:20	最新加入的Win...	192.168.43.129	C:\USERS\ADMINI...	病毒	Win32.Expiro.b	文件监控	清除成功
2016-12-14 09:49:20	最新加入的Win...	192.168.43.129	C:\USERS\ADMINI...	病毒	Win32.Expiro.b	文件监控	清除成功
2016-12-14 09:49:20	最新加入的Win...	192.168.43.129	C:\USERS\ADMINI...	病毒	Win32.Expiro.b	文件监控	清除成功
2016-12-14 09:49:20	最新加入的Win...	192.168.43.129	C:\USERS\ADMINI...	病毒	Win32.Expiro.b	文件监控	清除成功
2016-12-14 09:49:20	最新加入的Win...	192.168.43.129	C:\USERS\ADMINI...	病毒	Win32.Expiro.b	文件监控	清除成功

3.1.3.3 设置

设置可对组、终端进行设置，可以分别为每个组、终端设置不同的规则，这些规则包括常规项、扫描设置、文件监控、系统加固、应用加固、ftp 监控、U 盘监控、P2P 私有云、行为规则、Linux 防病毒。如图所示。



可以点击相应的按钮，进入相应的详细设置项，或者向下滑动滚动条（滚动鼠标滚轮），找到对应设置项。

3.1.3.3.1常规项

常规项项包括：禁止终端修改黑名单锁、白名单/排除列表、黑名单、云查杀、专项查杀和杀毒备份。

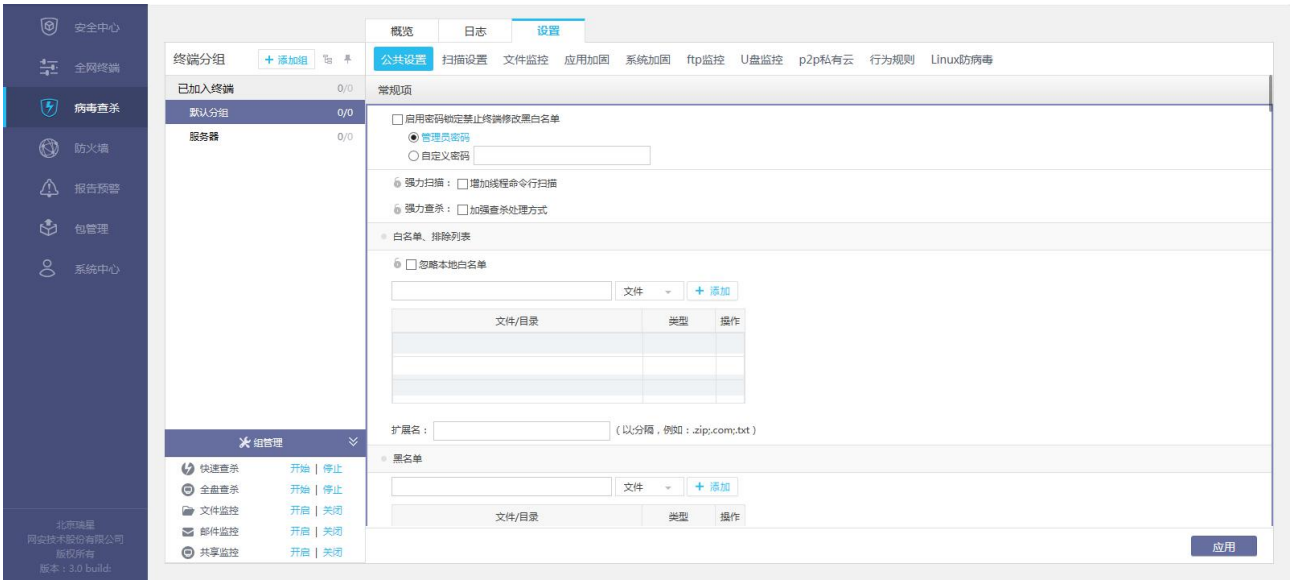
启用密码锁定禁止终端修改黑白名单：勾选启用后，禁止终端进行黑名单和白名单的修改。可为该条目设置密码，密码可默认为管理员密码，亦可自定义密码。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.1.1 白名单、排除列表

白名单用于添加那些不需要扫描和查杀的文件，添加白名单后，软件扫描和监控时将智能跳过这些文件。白名单添加方式分为两种：一种是以文件/目录方式，另一种是以文件后缀方式。

点击【病毒查杀】->【默认分组】->【设置】->【常规项】->【白名单】，进入白名单设置，如图所示。



忽略本地白名单：勾选后，本地已经设置的白名单、排除列表失效，进行病毒扫描和查杀时，会对白名单中的文件目录和程序进行扫描查杀；取消勾选，白名单、排除列表重新生效，病毒扫描查杀时，将跳过白名单中的目录和文件。

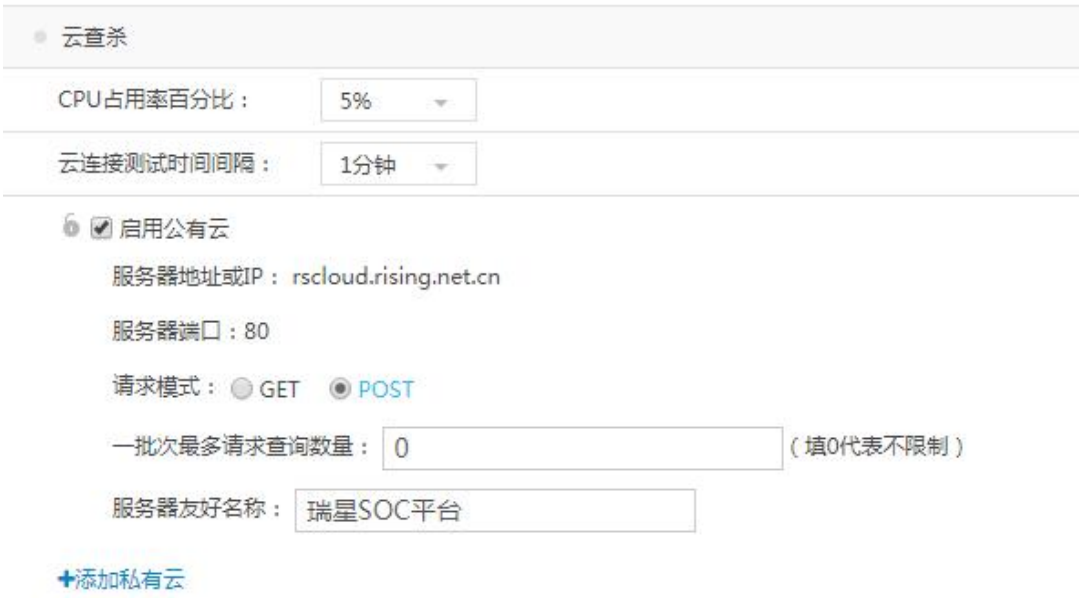
3.1.3.3.1.2 黑名单

黑名单：与白名单相反，黑名单用于添加那些必须要扫描和查杀的文件，添加黑名单后，软件扫描和监控时将立即隔离这些文件，这些文件将不能够打开、复制、删除和执行。如果要从黑名单中删除项目，点击“操作”一栏中对应项的删除 。

点击【病毒查杀】->【默认分组】->【设置】->【常规项】->【黑名单】，进入黑名单设置，如图所示。

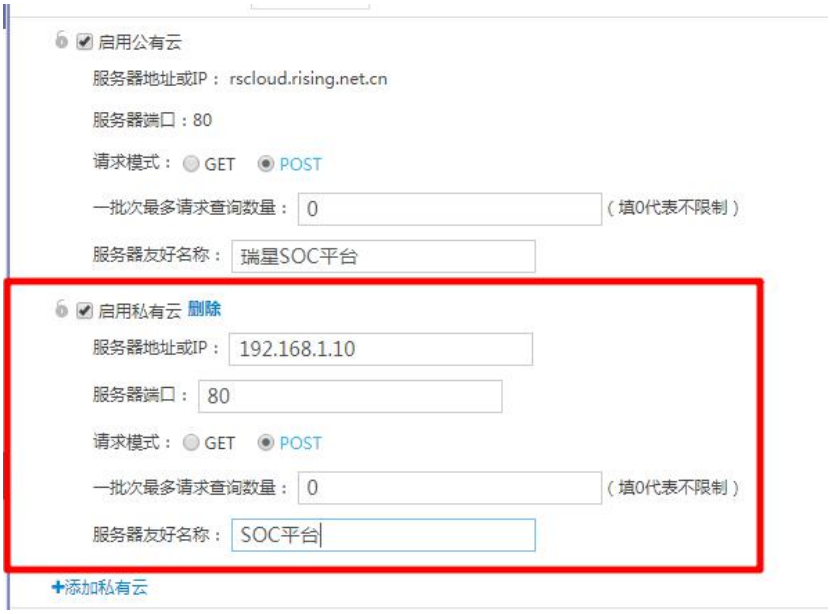
3.1.3.3.1.3 云查杀

云查杀相关设置：可对 CPU 占用率、云连接测试时间间隔、公有云及私有云进行设置。点击对应的下拉列表，选择需要的百分比和时间间隔。



公有云：公选启用公有云后，请求模式可以在 GET 和 POST 中二选一。设置一批次最多请求查询次数，默认填写“0”，（填 0 代表不限制）。

服务器友好名称：请填写为有利于用户的名称。



添加私有云：默认采用的是瑞星的公有云服务器，需自定义公有云服务器的用户，请点击【+添加私有云】，填写服务器地址和 IP，端口号等，点击【应用】，完成设置。取消勾选【启用私有云】，暂时取消私有云功能。如需要删除私有云，点击【删除】，删除该条设置。请谨慎进行删除操作。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.1.4 杀毒备份

杀毒备份是进行病毒查杀时，在隔离区对病毒文件进行备份，防止文件丢失。

点击【病毒查杀】->【默认分组】->【设置】->【常规项】->【杀毒备份】，进入杀毒备份设置，如图所示。

杀毒时备份原文件：勾选【杀毒时备份原文件】，即可将病毒文件备份到隔离区，供以后恢复数据时使用。

空间不足的处理方式：当隔离区备份的文件过多，导致隔离区空间不够时，空间的处理方式可以自动覆

盖老文件，或者空间自动增长。用户根据具体环境进行选择。

隔离失败时的处理方式：当备份病毒文件失败时，可以设置询问用户、删除文件（不隔离）和不处理的方式。用户根据具体环境进行选择。

大文件（超过 100M）处理方式：查杀时，文件很大，可以设置询问用户、直接删除（不隔离）、不处理。

启动病毒跟踪功能：方便管理员了解病毒爆发的起始时间、机器、数量等情况。

启用内存模式病毒库：勾选启用后，将部分高频的病毒库加载到内存中，提高病毒库读取速度，可以加快病毒扫描的速度。

加载木马库：启用后，进行病毒扫描和查杀时，会调用木马库。取消勾选，停止使用木马库进行查杀。

记录病毒日志：记录病毒的日志，日志包括病毒名称，类型，爆发次数，感染文件数量等，方便管理员查询病毒日志。

扫描缓存：勾选【二次扫描加速】选项后，软件将开启二次扫描加速功能，对一段时间内的扫描状态进行缓存和优化，使成倍提高扫描速度，减少系统资源消耗。

监控缓存：勾选【监控缓存】后，对文件监控时，智能跳过未发生变化的文件和目录。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.1.5 专项查杀

勾选相应的病毒类型，进行云扫描时即可针对特定病毒类型定点查杀。专杀类防护主要包括：飞客虫蠕虫、雨云病毒、威客虫蠕虫免疫、DLL 劫持免疫。

飞客虫蠕虫：飞客虫蠕虫(Hack Exploit Win32 MS08-067)是一个利用微软 MS08-067 漏洞发起攻击的蠕虫病毒。该病毒会对随机生成的 IP 地址发起攻击，攻击成功后会下载一个木马病毒，通过修改注册表键值来使安全软件功能失效。病毒会修改 hosts 文件，使用户无法正常访问安全厂商网站及其服务。

雨云病毒：雨云病毒为蠕虫病毒，中毒后的表现为任务管理器中有 wscript.exe 运行，在桌面上有名为 yuyun_ca 的图标，并且无法删除。通过共享方式进行传播，在局域网中很容易传播。

威客虫蠕虫免疫：威客虫蠕虫病毒中毒表现为无法启动系统，若启动系统后进行全盘扫描，则直接死机，该蠕虫病毒主要针对硬盘，中毒后只能格式化整块硬盘。

DLL 劫持免疫：DLL 劫持表现为，当一个可执行文件运行时，Windows 加载器将可执行模块映射到进程的地址空间中，加载器分析可执行模块的输入表，并设法找出任何需要的 DLL，并将它们映射到进程的地址空间中。

设定扫描模式：指扫描时选择的扫描模式，可以是办公模式、自动模式和高速模式中的一种。“办公模式”可以降低 CPU 的占用率，查杀时电脑卡顿推荐使用该模式；“高速模式”可以提高查杀速度，需要节省查杀时间并且 CPU 频率较高可使用该模式；“自动模式”，自动根据系统环境和资源使用情况判断使用模式，当系统闲暇时采用高速模式，而系统繁忙时，采用办公模式。

运行环境智能判断：智能判断当前客户端运行的环境，识别是 Windows 操作系统平台还是国产 Linux 操作系统平台，为策略下发提供参考，运行环境智能判断在 Windows 和 Linux 混用的环境中尤为重要，默认开启该功能。

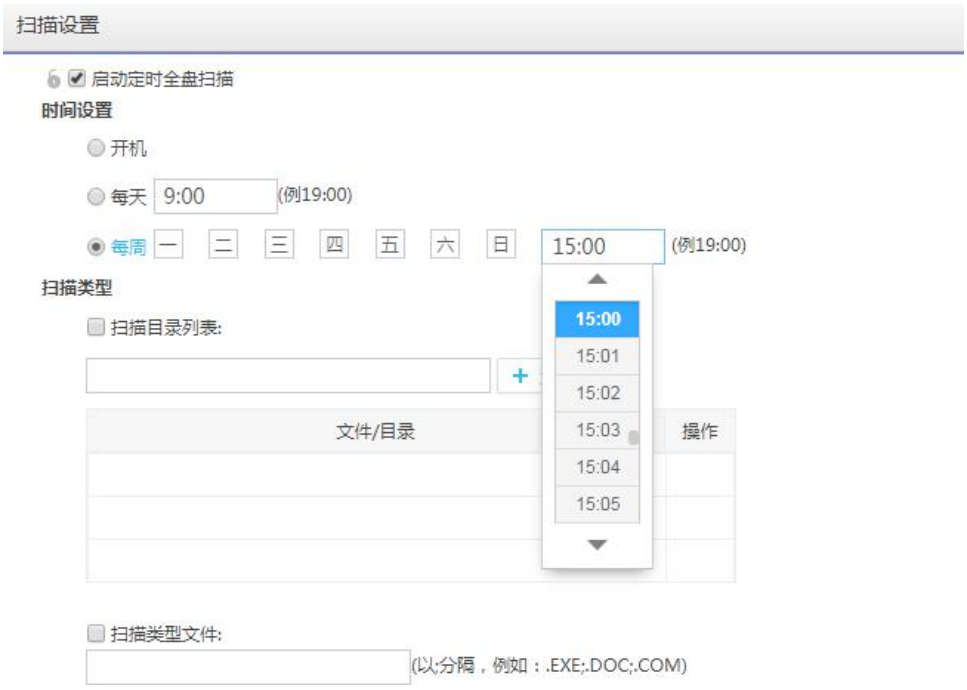
所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.2扫描设置

扫描设置可以设置扫描文件类型、定时查杀、查杀引擎的选择等。

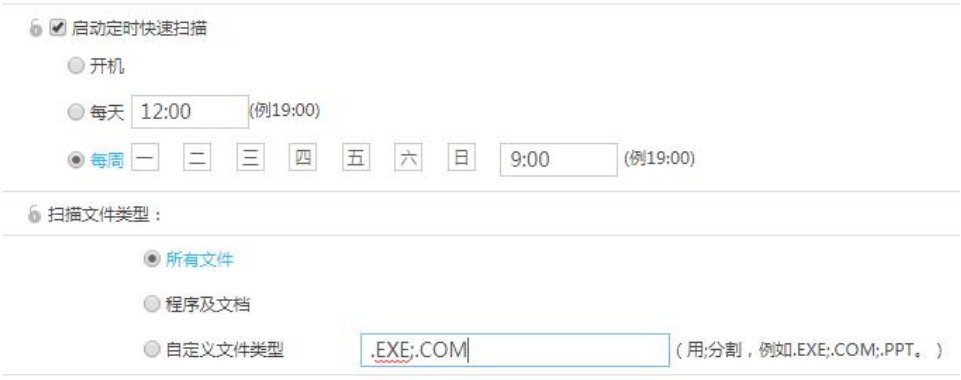
点击【病毒查杀】->【默认分组】->【设置】->【扫描设置】，进入扫描设置，如图所示。

启动定时全盘扫描：勾选【启动定时全盘扫描】，设置终端定时全盘扫描功能，可以设置为每天指定时间扫描；也可以设置为每周的特定日期和时间开始扫描；还可以设置为开机扫描。如图所示。



全盘查杀扫描类型：杀毒软件需要在查杀时扫描的文件类型，默认为“所有文件”，用户也可以自定义为“程序及文档”。勾选【扫描目录列表】，启用扫描类型。填写扫描目录或者文件，点击【添加】，在扫描类型文件中，填写需要扫描文件的类型，如图所示。

启动定时快速扫描：勾选【启动定时快速扫描】，设置终端定时快速扫描功能，可以设置为每天指定时间扫描；也可以设置为每周的特定日期和时间开始扫描；还可以设置为开机快速扫描。并设置扫描时扫描文件类型。默认扫描所有文件，也可以设置为仅扫描程序及文档或者自定义扫描文件类型。如图所示。



查杀引擎：杀毒软件带有 4 个查杀引擎，分别针对不同类型的病毒和安全威胁。勾选“仅查杀流行病毒”，会重点查杀最近比较活跃的病毒；勾选“启发式查杀”，可以有效的对可疑的文件查杀；勾选“压缩包检查”，并设置好压缩包的容量，查杀时可以嵌入到压缩包中查杀。勾选“启用云扫描引擎”，将针采用瑞星云引擎扫描病毒。

发现病毒：发现病毒的处理方式，可选自动或者手动。自动方式无需用户确认，自行清除病毒文件；手动处理方式，需要用户确认是保留还是删除病毒文件。

清除失败：指清除病毒失败时杀毒软件将要进行的操作，可设置为不处理或者直接删除带毒文件。

锁定管理员扫描任务：不锁定，在终端可以对管理员下达的命令进行暂停和停止；禁止停止，终端无法对管理员的命令停止操作，但是可以暂停；禁止暂停、停止，终端无法对管理员的命令做暂停、停止操作。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.3文件监控

文件监控能对终端的读写、文件、程序进行实时保护，一旦发现可疑文件和可疑操作立即拦截。

点击【病毒查杀】->【默认分组】->【设置】->【文件监控】，进入中心文件监控设置，如图所示。

开机启用：勾选开机启用，否则需要每次使用时手动打开文件监控功能。

锁定不允许终端关闭监控：这是文件监控锁定的总开关，勾选后，在终端软件设置里将不能关闭文件监控的所有功能，如终端需要关闭文件监控的某些功能，请去掉勾选。

启用内核监控：内核监控，能够对系统内核进行实时监控，保证系统安全，勾选开启后，客户端将在计算机启动时默认开启内核监控。

启用智能监控：智能监控，能够自动的监控重要文件，勾选开启后，根据系统算法选择需要监控的文件和类型。

开启智能黑名单：智能黑名单，自动拦截根据智能算法生成的程序和进程黑名单，勾选后，客户端将在计算机启动时默认开启智能黑名单。

启用嵌入式查杀：开启后，能对 outlook、邮件、office、IE 等软件、文件进行深入到内部的查杀，针对性的拦截病毒，监控文件进程是否正常，彻底保护常用软件的安全。

启用云扫描引擎：勾选后，查杀病毒将使用云引擎进行扫描，常用云引擎包括瑞星自主的云端引擎，通过利用瑞星云端服务器的强大性能和丰富全面的病毒库资源，全面快速的查杀文件，减轻本地引擎负担和资

源消耗，进一步提高查杀效率。

通知处理结果：勾选后，将通知管理员相关监控、扫描查杀的结果，能够提示扫描结果的危险等级，及时处理存在的安全隐患。

监控模式：文件监控模式，分为极速、标准、专业和增强。每一种模式适用于不同的场景和环境。

① 极速模式，可快速的监控常见文件和程序，监控使用的资源低，不会影响用户正常使用电脑；

② 标准模式，一般采用的模式，兼顾速度和监控效率，能够监控到大部分的威胁和病毒爆发；

③ 专业模式，为用户特殊需求设计，能够针对性的监控文件，如对 word 等 office 文档的增强监控，可以有效的降低宏病毒的影响。可以自定义文档类型，诸如 CFG;DAT；BIN 等 Windows 常见文件的增强监控。能有效拦截恶意脚本恶意配置文件。

④ 增强模式，为用户提供最全面的监控，对系统内所有文件和程序类型提供强力监控，缺点是占用系统资源相当高，可能会影响用户使用体验。

程序信任分析：通过分析用户系统中安装的程序，为用户展示潜在威胁的程序，能够识别恶意程序。

查杀引擎：勾选【仅查杀流行病毒】，即对活跃病毒进行重点的查杀；勾选【启发式查杀】，即将所有的可疑文件都列入查杀范围；勾选【启动压缩包查杀】，即可以查杀压缩包内的文件，同时对压缩包的大小可以进行限定。

发现病毒：选择发现病毒时的处理方式，可选择【自动处理】，如需手动处理，则选择【询问用户】。

清除失败：指清除病毒失败时杀毒软件将要进行的操作，可设置为不处理或者直接删除带毒文件。

共享文档：启用文档服务器查杀，能专门查杀共享文档，防止通过共享文档传播病毒。

在输入框中输入文档服务器中需要监控的文档类型，如.doc;.xml.ppt 等，点击添加按钮，添加到监控列表中。

驱动缓存：勾选后，策略变动时重置驱动缓存。经常性变动策略时，勾选此项，可以加快策略的生效速度。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.4应用加固

应用加固对 IE 浏览器和办公软件进行实时检测，防止恶意插件捆绑 IE 浏览器和恶意程序破坏办公软件。

点击【病毒查杀】->【默认分组】->【设置】->【应用加固】，进入应用加固设置，如图所示。

启用加固：勾选后，应用加固功能才能生效。

发现威胁：选择【允许运行】，则威胁应用将继续运行，选择【禁止运行】，让威胁应用立即停止运行。

处理方式：发现威胁后通知用户的方式，要么选【自动处理】，即不通知；要么选【通知我】，即以弹窗的形式提醒用户威胁。

拦截日志：勾选【记录拦截日志】后，在日志中心将产生应用加固的日志信息。否则没有应用加固拦截日志。

被保护的软件启动：该功能用于提示软件启动时是否安全，选择【弹出保护框】，软件启动时会弹出安全提示，选择【不弹出保护框】，启动软件时则没有弹窗提示。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.5系统加固

对系统的重要文件进行加固防护，保护系统安全，对破坏系统文件类型病毒有很好的防护效果。

点击【病毒查杀】->【默认分组】->【设置】->【系统加固】，进入系统加固设置，如图所示。

启用系统加固：勾选后，开机自动启用系统加固功能，不勾选，系统加固功能失效。

发现威胁：发现威胁时的处理方式，【自动处理】或者【通知我】。

拦截日志：勾选【记录拦截日志】，则在日志中心产生日志记录，否则不生成日志。

监控灵敏度：分为【低】、【中】、【高】，灵敏度越高，CPU 的占用率越高，推荐选择【中】。

审计模式：勾选【开启】后，审计模式生效。开启审计模式后，对应监控灵敏度级别的规则，全都自动放过，并记录动作日志，方便监控、了解所有具体动作行为。

放过含数字签名的程序：勾选【放过带数字签名的程序】，对系统中已经获得安全数字签名认证的程序一律放行。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.6 ftp 监控

ftp 监控是对计算机 ftp 监控的设置，可设置 ftp 文件发现病毒时处理方式和提示方式。

点击【病毒查杀】->【默认分组】->【设置】->【ftp 监控】，进入 ftp 监控设置，如图所示。

ftp 监控：勾选启用 ftp 监控，则 ftp 监控功能在每次计算机启动时自动启用；否则要使用 ftp 监控时需手动打开 ftp 监控功能。

缓存类型：【自定义】，自行设置需要缓存的内存大小，硬盘空闲空间大的情况下可以设置大一点，否则请设置小一点。如：1024KB；【全部缓存】，表示 ftp 共享的所有文件都进行缓存，这将占用一些存储空间；还可以选择【不缓存】，就是不缓存任何的文件，每次查杀都重新扫描所有文件，不占用硬盘空间，缺点是扫描时间长。

文件大小：用于设置 ftp 监控时能扫描的最大文件，如设置为 1024M，表示只扫描小于等于 1024M 的文件。

IP：填写需要监控的 ftp 地址。端口号：填写监控的 ftp 对应的端口号。

填写完毕，点击后面的【+添加】，ftp 就加入到监控列表中了。如需添加更多 ftp 地址，重复之前操作即可。

在 ftp 服务器列表中，可以点击操作一栏的【删除】，删除不再需要监控的 ftp 地址。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.7U 盘监控

U 盘监控，对 U 盘进行防护，能有效的防止病毒从 U 盘感染计算机。

点击【病毒查杀】->【默认分组】->【设置】->【U 盘监控】，进入 U 盘监控设置，如图所示。

启用 U 盘监控：勾选后，启用 U 盘监控功能。

插入 U 盘时：选择【询问是否查杀】或者【立即查杀】。

查杀深度：可以设置对 U 盘文件的查杀递归层次，增加多少扫描层数，可以查杀多少层级的子目录。其中-1 代表查杀所选区域的所有目录及其子目录。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.8P2P 私有云

P2P 私有云是瑞星最新研发的点对点病毒查杀引擎，通过挂在私有云，在私有云上安装 P2P 查杀引擎，能够做到瞬间查杀，更快、更强的扫描文件。

点击【病毒查杀】->【默认分组】->【设置】->【P2P 私有云】，进入 P2P 私有设置界面，如图所示。

启用私有云：勾选后，开启 P2P 私有云引擎功能。设置服务器 IP 地址，设置服务器端口号，默认为 27017，设置便于记忆和理解的服务器友好名称。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.9行为规则

行为规则是为批量管理客户端定制的，可以批量下发规则。有管理员预先定制，使用时只需添加并勾选需要启用的规则，规则即可用。能大幅降低管理员的工作负担，也能提高规则下发的效率。

提示：要开启行为规则，必须首先启用对应的监控功能，行为规则才能生效。

点击【病毒查杀】->【默认分组】->【设置】->【行为规则】，进入行为规则设置界面，如图所示。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.9.1 文件监控-行为规则

启用规则：勾选后，才能启用文件监控-行为规则，说明：开启了文件监控此处规则才能生效!

通知用户：勾选后，能够收到触发行为规则的通知。

记录拦截日志：勾选后，系统开始将拦截记录写进日志中，为后期的分析和日志报告储存数据。

规则列表：在列表中，即为需要使用的文件监控规则，根据使用需求勾选相应项目即可。可以通过下拉进度条进行翻阅。可以增加规则、修改规则和删除规则。这些都是高级功能，最好是管理员来进行修改删除。

规则列表中，可以点击【删除】删除对应的规则。通过勾选规则前的复选框，选中规则生效，未选中的规则则无效。

点击右侧的【添加】按钮，可以添加新的规则。如图所示。

已经存在的规则，可以通过鼠标点击输入，直接进行修改。

说明：该规则是高级定制功能，请不要随意修改。如有需要请联系管理员定制化修改！

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.9.2 系统加固-行为规则

启用规则：勾选后，才能启用系统加固-行为规则，说明：开启了系统加固此处规则才能生效!

通知用户：勾选后，能够收到触发行为规则的通知。

记录拦截日志：勾选后，记录触发行为规则的拦截记录，在规则列表中，可以通过下拉进度条进行翻阅。

规则列表中，可以点击【删除】删除对应的规则。通过勾选规则前的复选框，选中规则生效，未选中的规则则无效。

点击右侧的【添加】按钮，可以添加新的规则。如图所示。

已经存在的规则，可以通过鼠标点击输入，直接进行修改。

说明：该规则是高级定制功能，请不要随意修改。如有需要请联系管理员定制化修改！

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.9.3 防勒索文件保护

防勒索文件保护，能够针对勒索病毒进行防护，如防护永恒之蓝等勒索病毒。

启用保护：勾选后，才能启用防勒索文件保护。

保护模式：学习模式：选取此模式后，用户确认不对某行为拦截时，自动将对应进程添加到白名单。标准模式：勾选后，将对所有疑似勒索的病毒和行为进行拦截。

拦截文件操作：勾选修改，拦截到中勒索病毒的文档时，依然可以对文档进行修改。勾选删除，则直接删除中勒索病毒的文档。

提示用户：勾选后，能够收到触发行为规则的通知。

记录日志：勾选后，记录触发行为规则的拦截记录，在规则列表中，可以通过下拉进度条进行翻阅。

源进程白名单(白名单里的进程才允许操作被保护文件)，勾选后，启用进程白名单功能，并设置保护目录或者文件，设置后，只有在白名单里的程序才能访问和操作保护目录的文件。

设置目标保护文件。针对特定的目标文件设置保护规则。也可选择排除目标文件设定规则。点击右侧的【添加】，添加特定保护目标文件和目录。在后缀输入框中输入特定的后缀名，包含该后缀的文件都将被纳入到特定保护目标。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.3.3.10Linux 防病毒

Linux 防病毒是专门针对 Linux 客户端的设置项，本设置只对 Linux 客户端生效。设置项包括：扫描优化、扫描路径、定时扫描和病毒设置。

点击【病毒查杀】->【默认分组】->【设置】->【Linux 防病毒】，进入中心 Linux 防病毒设置，如图所示。

扫描优化：勾选后，设置需要扫描的时间段（如：最近 3 天更新的文件），还可以设置扫描文件的大小。

扫描路径：在输入框中填写需要扫描的 Linux 文件路径，勾选忽略以下路径，然后添加需要忽略的路径。在路径列表中将显示已输入的路径列表。

定时扫描：勾选后，可以设定扫描的时间和日期，可以选择一周的任意一天。

病毒设置分三项，如下：

发现病毒时：可以选择清除病毒、删除病毒文件、不处理的任一项。

清除失败时：可以选择删除染毒文件、不处理的任一项。

隔离失败时：可以选择清除病毒、删除病毒文件、不处理的任一项。

所有设置项设置完成后，点击右下角【应用】，保存设置。

3.1.4 报告预警

报告预警用于生成报告，包括定制基础报告、定时报告、综合报告。能直观的反应终端的授权、安装、防护状态和病毒库版本情况。并且通过报告能够了解病毒感染情况，能进行病毒分类、汇总和排名。

3.1.4.1 定制报告

定时报告可以创建预警的报告，可以创建基本报告、定时报告和综合报告。

3.1.4.1.1定制基本报告

点击进入定制报告页面，鼠标悬于创建报告上，在下拉列表中选择基本报告。点击基本报告。如图。

在弹出的窗口中填写报告名称，选择报告分类。选择终端范围。勾选统计方式。

如果之前设置过，可以点击【载入历史设置】，在弹出的下拉列表中选择一个设置即可。

设置完成后，点击【创建】，报告列表中就有刚才报告的条目了。

过几分钟，报告就自动生成了。点击历史记录一栏的数字，可以下载对应的报告。选择时间段，可以筛选报告，如，点击【上月】，可以找到上月的所有报告。点击【↓】，下载对应的报告，点击【X】，则删除对应的报告。

下载报告格式为 PDF，可以直接用 Chrome 打开，也可以用 PDF 软件打开，如图。

电网北京分公司3

一、终端安装

报告生成条件

报告分类	终端安装
终端范围	全部
统计方式	按子产品安装统计

1、子产品安装统计

A Linux_glibc25_Intel　B IT资产管理　C Linux_General_Server　D 漏洞扫描
E UNIX_AIX6_RS6000　F UNIX_AIX7_RS6000　G UNIX_AIX5_RS6000　H 网络安全管理
I Linux_MIPS　J Linux_Professional_Secret　K Linux_China_Desktop　L 防病毒
M HPUX_PARISC　N UNIX_Solaris_Intel　O LinuxKernel_Intel26　P LinuxKernel_Intel24
Q 行为审计　R 舆情　S Linux_INTEL_X64　T 升级中心
U Linux_MIPSX64　V Linux_AARCH　W 漏洞补丁中心　S Linux_glibc27_Intel
Y 业务中心

子产品安装统计

序号	组名称	总终端数	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	S	Y
1	服务器	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	黑名单	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	默认分组	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

3.1.4.1.2定制定时报告

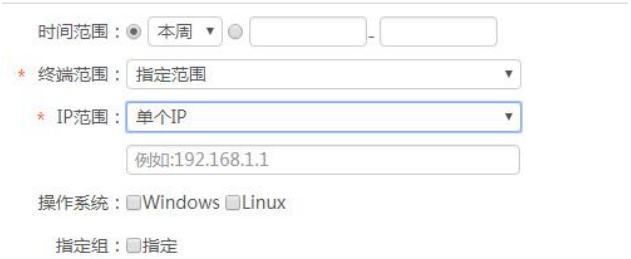
3.1.4.1.2.1 创建报告

点击进入定制报告页面，鼠标悬于创建报告上，在下拉列表中选择定时报告，填写名称，选择报告类型。这里以病毒感染情况为例。

时间范围：选择报告的事件起点和终止，可选择本周、本月、上周、上月，亦可自定义时间段。

终端范围：选择报告的终端，可选择全部终端，或者指定范围。

指定范围：选择指定范围的终端后，界面变化如图。



IP 范围：可以选择模糊搜索、单个 IP 或者 IP 段，如图。

操作系统：勾选需要报告的操作系统。

指定组：勾选指定组后，可以选择需要报告的组。如图。

病毒分类：默认勾选的是全部。若要统计某类病毒，请勾选对应病毒即可。如图。

病毒来源：点击下三角，在下拉列表中选择病毒来源，可以是扫描病毒，也可是文件监控等。默认来源为所有。

处理方式：点击下三角，在下拉列表中选择处理方式，暂未处理，忽略，清除，删除。

病毒状态：指病毒已经查杀或者扫描到的病毒，是否处理的状态。

指定病毒：可以填写病毒名称带有的关键字，出报告是会模糊搜索所有匹配的病毒。

统计方式：统计病毒的方式，包括按照感染终端数、终端病毒排行、病毒分类汇总等。

设置完成后，点击【下一步】，进入定时设置界面。

时间计划：设置定时重复频率，分为定时一次、定时每天、定时每周、定时每月。

生成时间：是定时的具体时间。比如选择 2018 年 10 月 22 日 14:00，定时一次，则会按照时间计划在该

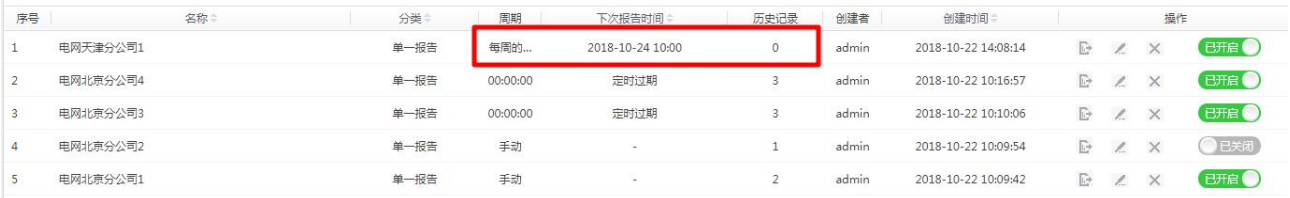
时间点生成报告，并只执行这一次。

若果选择每周定时，则选择哪一天执行即可。如图为每周的星期一、三、五、日的 10 点自动生成报告。

设置完成后，点击【下一步】。进入报告推送界面。选择报告消息的推送方式。推送方式可选择“消息中心推送”和“邮件推送”。若采用消息中心推送，则报告生成后会直接在首页消息栏中显示消息，直接点开消息即可查看报告内容。若设置邮件推送，则报告直接发送到所填写的邮箱中。

如上图所示方式填写接收报告的邮箱地址。如果需要设置多个接收邮箱，邮箱间用英文分号“;”隔开。

设置完成后，点击【创建】，弹出消息提示创建成功。创建完成后，在报告列表中将显示刚才创建的报告。红框中为定时报告的执行时间、频率和报告记录。



序号	名称	分类	周期	下次报告时间	历史记录	创建者	创建时间	操作	
1	电网天津分公司1	单一报告	每周的...	2018-10-24 10:00	0	admin	2018-10-22 14:08:14		已开启
2	电网北京分公司4	单一报告	00:00:00	定时过期	3	admin	2018-10-22 10:16:57		已开启
3	电网北京分公司3	单一报告	00:00:00	定时过期	3	admin	2018-10-22 10:10:06		已开启
4	电网北京分公司2	单一报告	手动	-	1	admin	2018-10-22 10:09:54		已关闭
5	电网北京分公司1	单一报告	手动	-	2	admin	2018-10-22 10:09:42		已开启

可以通过每个报告规则后面的快捷开关开启或者关闭定时报告。如图所示。

3.1.4.1.2.2 修改定时设置

在报告列表中，点击“ ”，修改报告设置。点击后界面如图所示。

在报告分类中，可以添加分类。点击【添加分类】，选择分类添加。可以同时添加多个分类。同分类也可以重复添加，并且有编号区别。

添加多个分类后，可以进行分类优先级的排列。点击【↑】或【↓】可向上或向下调整优先级。点击【X】删除分类。然后点击每个分类，分别设置分类的具体项目。

所有设置项修改完成后，点击下方的【保存】，保存修改。

3.1.4.1.3定制综合报告

3.1.4.1.3.1 创建综合报告

点击进入定制报告页面，鼠标悬于创建报告上，在下拉列表中选择综合报告，点击后界面如图所示。

在报告分类中，可以添加分类。点击【添加分类】，选择分类添加。可以同时添加多个分类。分类也可以重复添加，并且有编号区别。

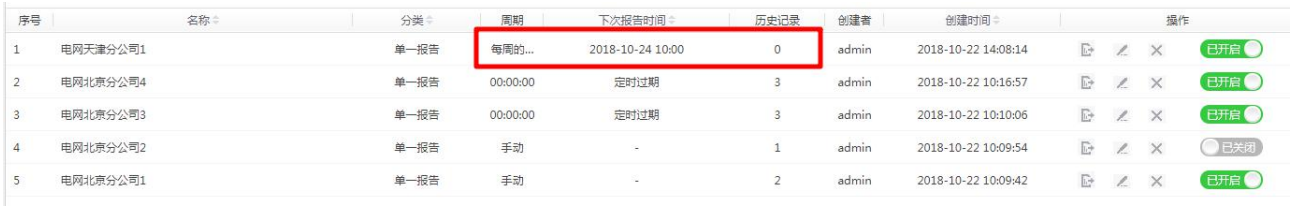
添加多个分类后，可以进行分类优先级的排列。点击【↑】和【↓】可向上或向下调整优先级。点击【X】删除分类。点击每个分类，分别设置分类的具体项目。

所有设置项修改完成后，点击下方的【下一步】，进入定时设置。

设置完成后，点击【下一步】。进入报告推送界面。选择报告消息的推送方式。推送方式可选择“消息中心推送”和“邮件推送”。若采用消息中心推送，则报告生成后会直接在首页消息栏中显示消息，直接点开消息即可查看报告内容。若设置邮件推送，则报告直接发送到所填写的邮箱中。

如上图所示方式填写接收报告的邮箱地址。如果需要设置多个接收邮箱，邮箱间用英文分号“;”隔开。

设置完成后，点击【创建】，弹出消息提示创建成功。创建完成后，在报告列表中将显示刚才创建的报告。红框中为定时报告的执行时间、频率和报告记录。



序号	名称	分类	周期	下次报告时间	历史记录	创建者	创建时间	操作	
1	电网天津分公司1	单一报告	每周的...	2018-10-24 10:00	0	admin	2018-10-22 14:08:14		已开启
2	电网北京分公司4	单一报告	00:00:00	定时过期	3	admin	2018-10-22 10:16:57		已开启
3	电网北京分公司3	单一报告	00:00:00	定时过期	3	admin	2018-10-22 10:10:06		已开启
4	电网北京分公司2	单一报告	手动	-	1	admin	2018-10-22 10:09:54		已关闭
5	电网北京分公司1	单一报告	手动	-	2	admin	2018-10-22 10:09:42		已开启

可以通过每个报告规则后面的快捷开关开启或者关闭定时报告。如图所示。

分类	周期	下次报告时间	历史记录	创建者	创建时间	操作	
单一报告	每周的...	2018-10-24 10:00	0	admin	2018-10-22 14:08:14		已开启
单一报告	00:00:00	定时过期	3	admin	2018-10-22 10:16:57		已开启
单一报告	00:00:00	定时过期	3	admin	2018-10-22 10:10:06		已开启
单一报告	手动	-	1	admin	2018-10-22 10:09:54		已关闭
单一报告	手动	-	2	admin	2018-10-22 10:09:42		已开启

3.1.4.1.3.2 修改综合报告

在报告列表中，点击“ ”，修改综合报告设置。点击后界面如图所示。

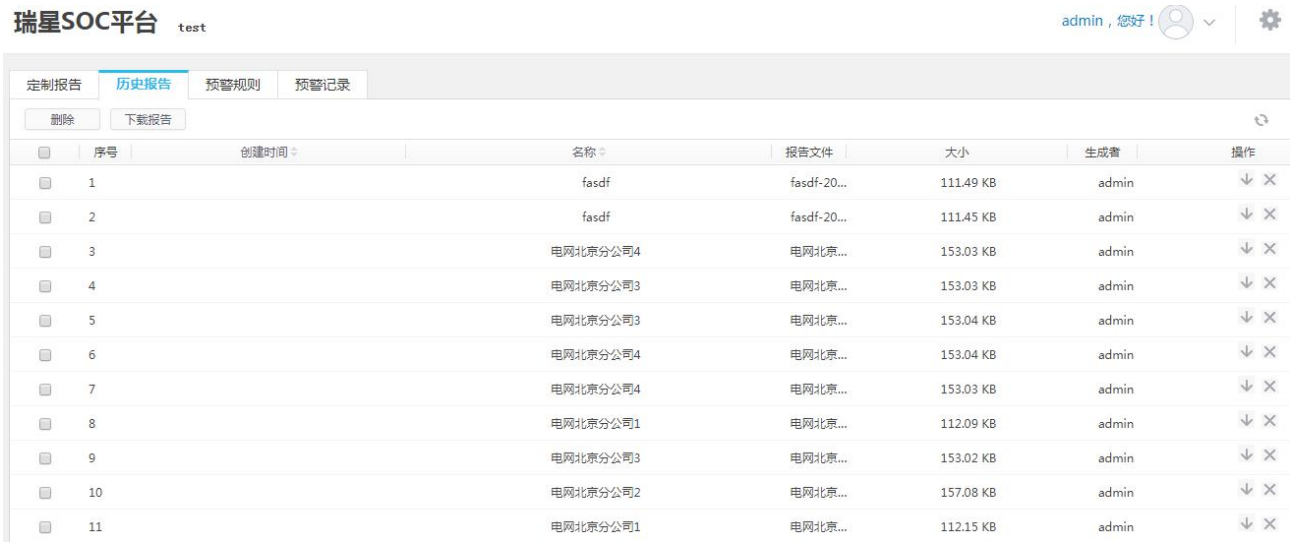
在报告分类中，可以添加分类。点击【添加分类】，选择分类添加。可以同时添加多个分类。分类也可以重复添加，并且有编号区别。

添加多个分类后，可以进行分类优先级的排列。点击【↑】或【↓】可向上或向下调整优先级。点击【X】删除分类。然后点击每个分类，分别设置分类的具体项目。

所有设置项修改完成后，点击下方的【保存】，保存修改。

3.1.4.2 历史报告

历史报告里可以查看以往生成的报告，可以进行下载和删除。如图。



点击【↓】，下载对应报告，点击【X】，删除对应报告。

3.1.4.3 预警规则

在预警规则列表，可以选择所需的预警规则。 

表示预警规则关闭，再次点击，变为 

，表示预警规则已开启。如图所示。

3.1.4.4 预警记录

预警记录是预警规则执行后产生日志，通过日志可以查阅那些预警规则被触发，有利于排查预警出现的问题。如图所示。

例如，病毒清理失败后，将会记录预警日志，预警内容如图所示。

3.1.5 授权管理

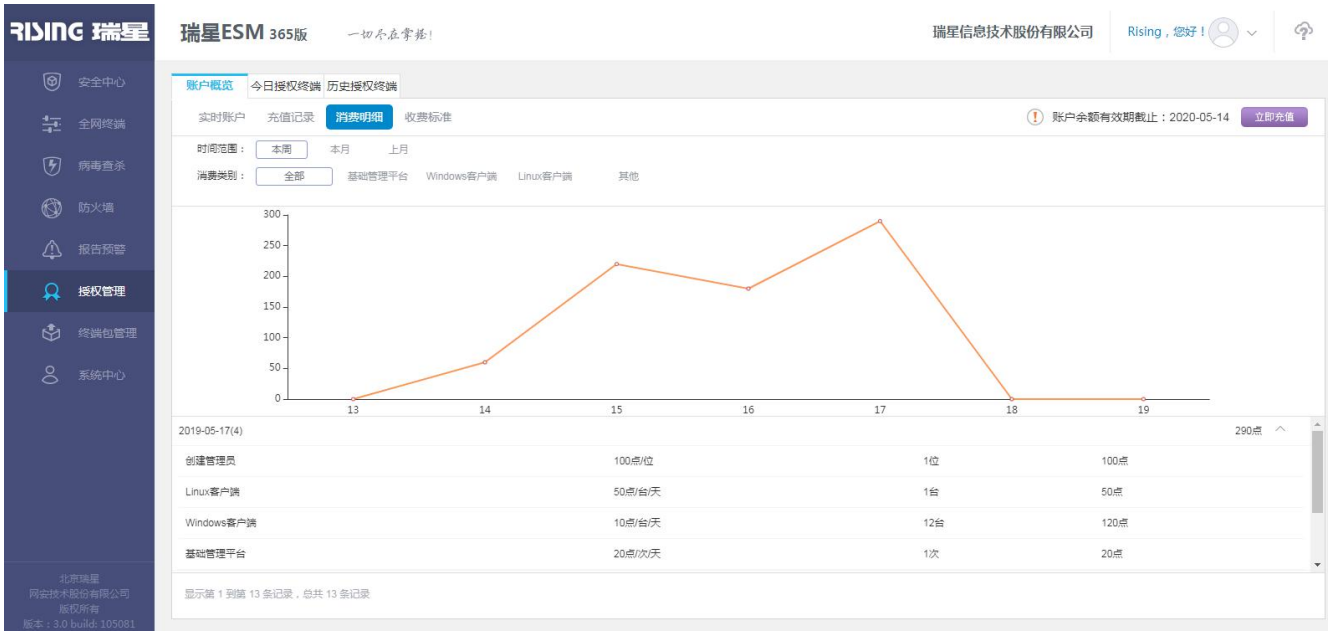
3.1.5.1 购买与扩容

授权管理可以集中管理和查看用户授权。在账户概览中查阅账户的实时余额，消费详情等。

如下图所示为账户实时概览。展示了账户余额和赠送点数，今日消费点数，预计可使用天数，账户余额

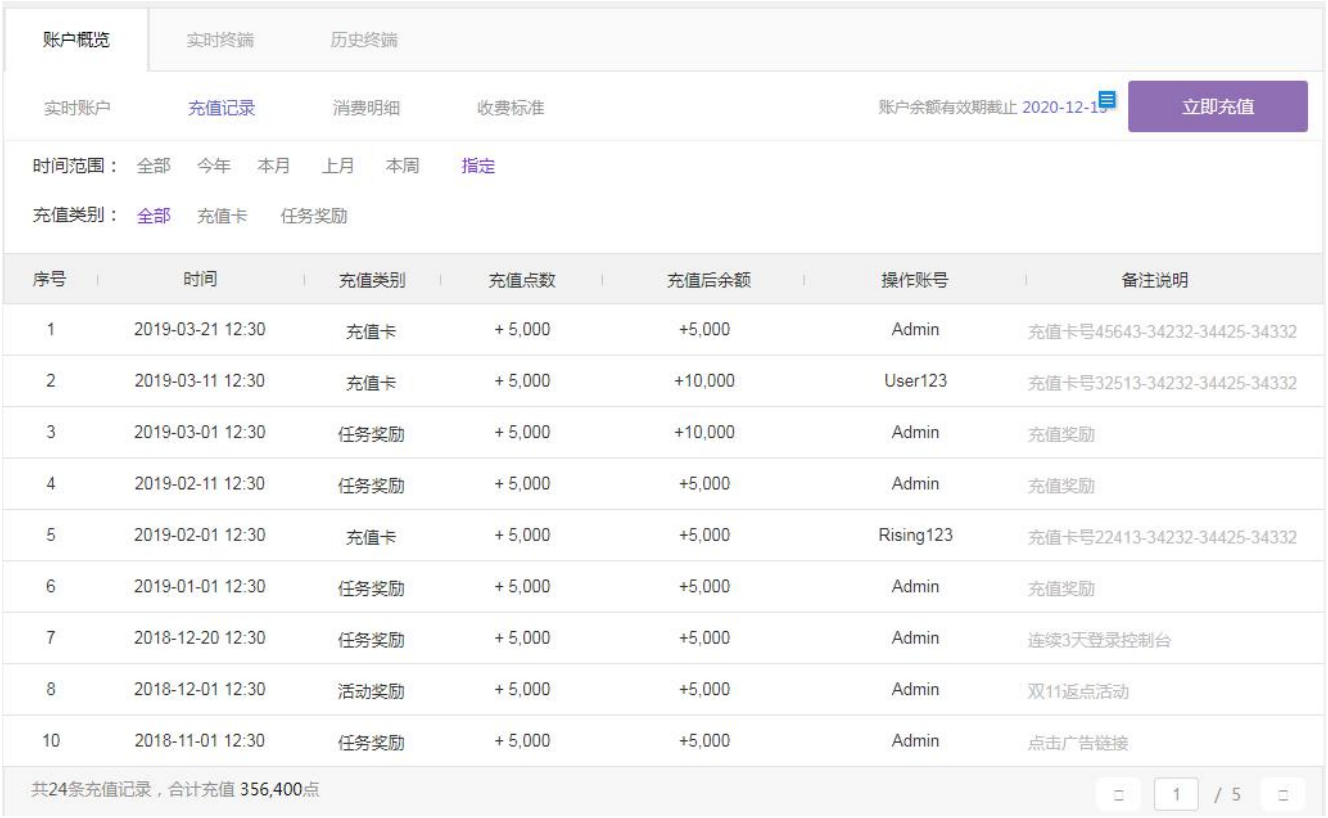
有效期。

点击【消费明细】，可查看当日的明细。如下图所示。



可通过切换本月和本年度，来查看不同时间段的消费统计饼状图。

点击【充值记录】，可以查阅详细的充值记录信息。可以指定充值的时间范围和充值的类型。



序号	时间	充值类别	充值点数	充值后余额	操作账号	备注说明
1	2019-03-21 12:30	充值卡	+ 5,000	+5,000	Admin	充值卡号45643-34232-34425-34332
2	2019-03-11 12:30	充值卡	+ 5,000	+10,000	User123	充值卡号32513-34232-34425-34332
3	2019-03-01 12:30	任务奖励	+ 5,000	+10,000	Admin	充值奖励
4	2019-02-11 12:30	任务奖励	+ 5,000	+5,000	Admin	充值奖励
5	2019-02-01 12:30	充值卡	+ 5,000	+5,000	Rising123	充值卡号22413-34232-34425-34332
6	2019-01-01 12:30	任务奖励	+ 5,000	+5,000	Admin	充值奖励
7	2018-12-20 12:30	任务奖励	+ 5,000	+5,000	Admin	连续3天登录控制台
8	2018-12-01 12:30	活动奖励	+ 5,000	+5,000	Admin	双11返点活动
10	2018-11-01 12:30	任务奖励	+ 5,000	+5,000	Admin	点击广告链接

点击【消费明细】，查阅消费的详情记录。通过选择不同时间段和不同的消费类型，不同的消费终端进行过滤。

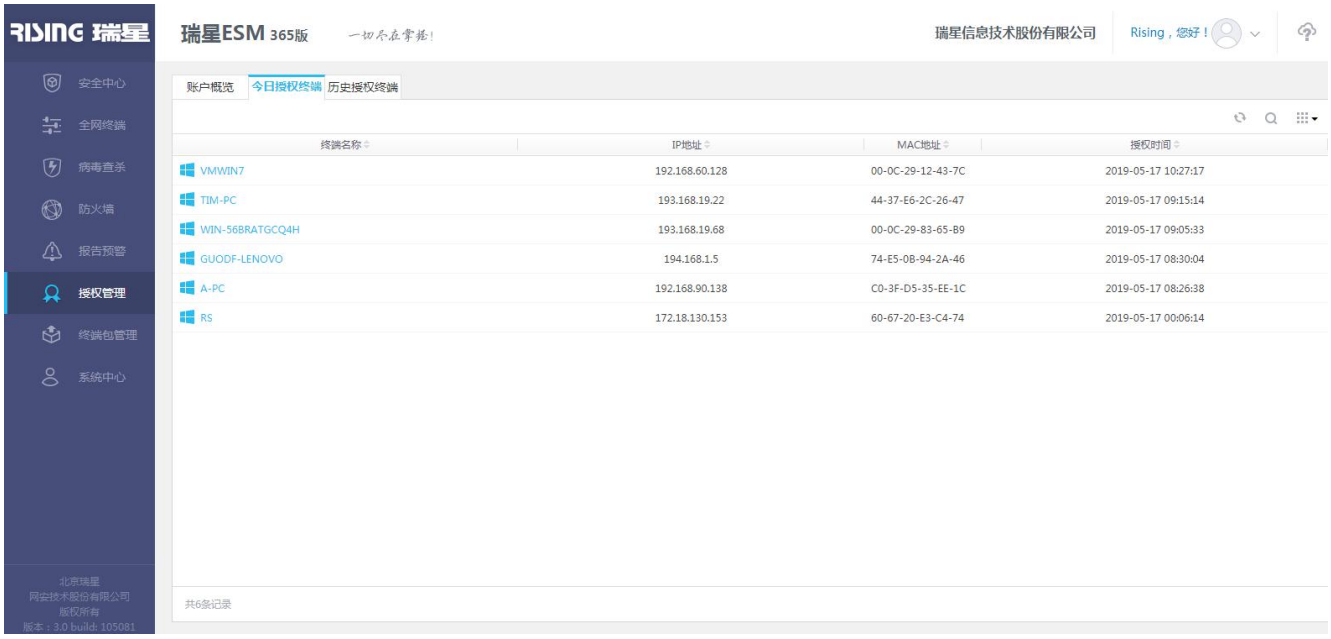
序号	消费时间	消费类型	收费标准	数量	累计消费点数
1	2019-03-24	管理平台服务	20点/天	1	30
2	2019-03-24	Windows客户端	10点/天/台	20	200
3	2019-03-24	Linux客户端	25点/天/台	30	300
4	2019-03-24	创建管理员	100点/次	1	100

点击【收费标准】，可以查看最新的活动和基础服务收费标准以及拓展服务收费标准。收费的单位为点/天/台，每个功能模块都需要消耗若干个点数。购买的总点数一定，消费后点数即减少，不可恢复。

点击【立即充值】，进入充值页面。输入充值卡密码，点击【检测】，测试密码是否正确有效。若在未使用的情况下发现密码错误或者无效，首先请检查密码输入是否正确，若准确无误，请通过右侧的购买联系方式和售后电话联系瑞星反馈问题。充值卡的购买方式也是通过瑞星销售电话购买。销售会帮助你进行购买，并协助充值。

3.1.5.2 今日授权终端

今日授权终端页面列出来今日消耗点数的终端。



3.1.5.3 历史授权终端

历史授权终端页面展示过去每天使用授权的终端数量。

3.1.6 终端包管理

终端包管理主要是用于安装包、升级包的管理和分发。包括上传基准离线包、上传升级包、定制安装包等。

第一步：上传基准离线包，后续才能进行包定制和升级，基准包分 Windows 和 Linux 两种。

下图为已经上传 Windows 基准离线包后的界面。

第二步：依次点击【终端包管理】/【终端基准包】，进入终端包定制页面，点击【安装包定制】。

选择需要升级的平台，选择升级包，点击【上传】，完成升级包上传。

上传升级包和病毒库升级包的操作类似。其中病毒库升级包仅支持 Windows 平台。包括组件、病毒库版本、恶意网址库版本、漏洞库版本等。如下图所示。

第三步：自定义包组件和功能。

安装包类型：分为完整包和下载器。完整包能够进行策略定制，下载器不能定制策略。

包名称：自定义合适的包名字即可。

中心地址：一般采用默认的中心地址即可，端口默认不填写，http 默认为 80 端口，https 默认为 443 端口。

必备组件：为客户端代理，是必须安装的组件。可以设置组件的策略为服务器模式或者默认分组模式。

子产品：子产品中目前支持的为防病毒组件、防火墙组件，选择后可以设置默认策略、安全管理策略和 P2P 策略。策略为服务器或者默认分组策略，具体以中心分组情况为准。即终端分组有多少个，就有多少种策略组合供选择。

安装路径：选用默认路径即可，也可设置为需要的路径。

安装方式：分为常规安装，即手动点击下一步的方式安装；自动，即自动下一步安装；后台静默，即在后台默默的安装，无需客户端用户进行任何操作。

安装完成时：可以选择【创建桌面快捷方式】、【添加到开始菜单】、【安装后自动启动程序】。

设置完成后，点击【添加】，保存设置。并弹出成功定制安装包提示。

点击【查看】，查看定制的安装包。

第四步：发布定制的安装包。

勾选刚才定制的安装包，点击【发布】。可以将安装包发布出去。也可以点击【删除】，删除不需要的定制包。发布界面如下图。

填写发布的内容描述，然后点击【发布】。

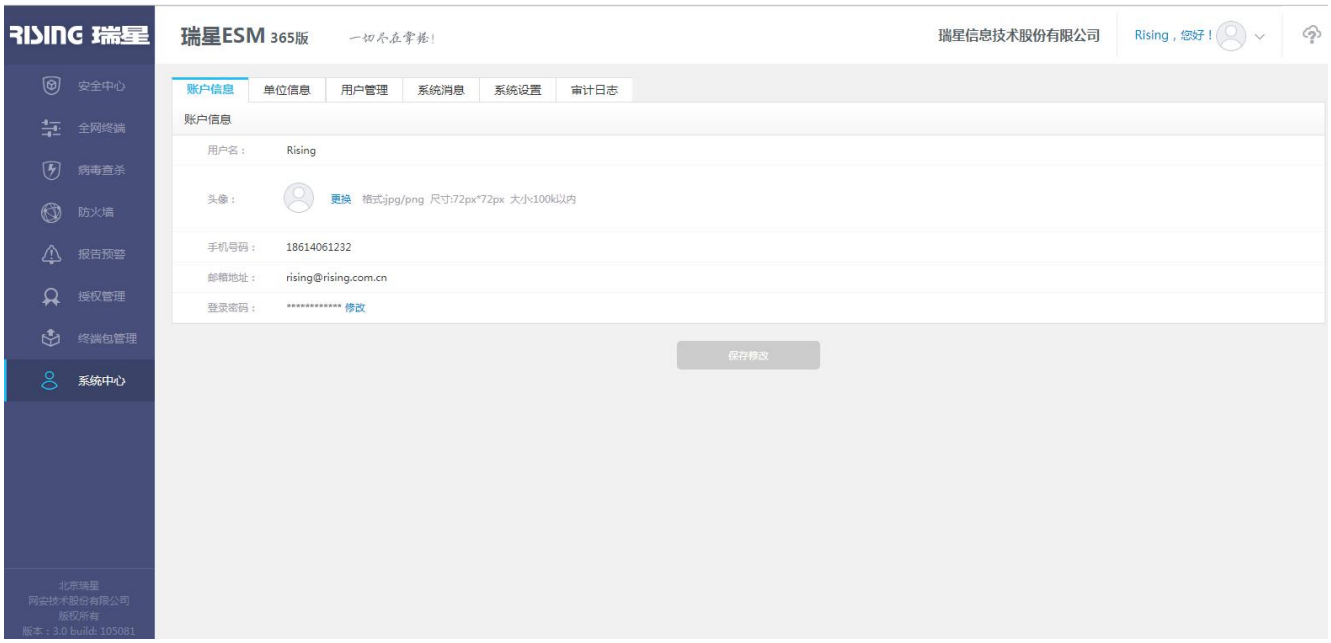
发布成功，点击【复制下载链接】，将链接发给客户端用户下载。客户端用户点击安装定制包，即可安装。

下载定制包界面如图。点击下载。

3.1.7 系统中心

3.1.7.1 账户信息

账户信息页面中可以设置用户名、头像、邮箱和修改登录密码等。



3.1.7.2 用户信息

用户信息页面可以进行单位信息自定义，同时，支持设置告警服务邮箱。在【发送邮件】栏目下，设置发送邮件的服务器地址和端口，邮箱账号，密码等。以后告警时就会使用该邮箱发送告警邮件。

3.1.7.3 用户管理

在用户管理界面，超级企业管理员可以添加安全管理员账户。

3.1.7.3.1添加安全管理员

点击【添加管理员】，填写账号、密码，选择状态。状态“已开启”表明该账号可以使用，若状态是“已关闭”，则临时停用账号。填写完毕，点击右下角【保存修改】。提示添加成功。

在操作列表中可对账号进行删除和修改。如图红框所示。在类型一栏可以看到账户所属类型。并可查阅每个账户最近登录时间、最近登录 IP 和登录 IP 限制。

点击用户管理下的【设置】，可以设置账户的属性。

账户安全设置包括：

超时退出：设置用户无操作后自动退出登录的时间间隔，如图为 30 分钟。

异常锁定：设置账户密码输入错误的最大次数，超过次数后锁定账户。还可以定制解锁的方式，一种是自定义一段时间后自动解锁，如 10 分钟后自动解锁；另一种方式为超级企业管理员手动解锁。

设置完毕后，点击右下角的【保存修改】。

当账号被锁定后状态如图中 rising3.，前面的图标变为橙色的锁。

3.1.7.3.2安全管理员账号解锁

安全管理员解锁必须用超级企业管理员登录管理中心，然后按如下步骤操作：

1.超级企业管理员登录中心，并定位到【系统中心】/【用户管理】/【账户列表】，找到被锁定的账号。如图中的 rising3。

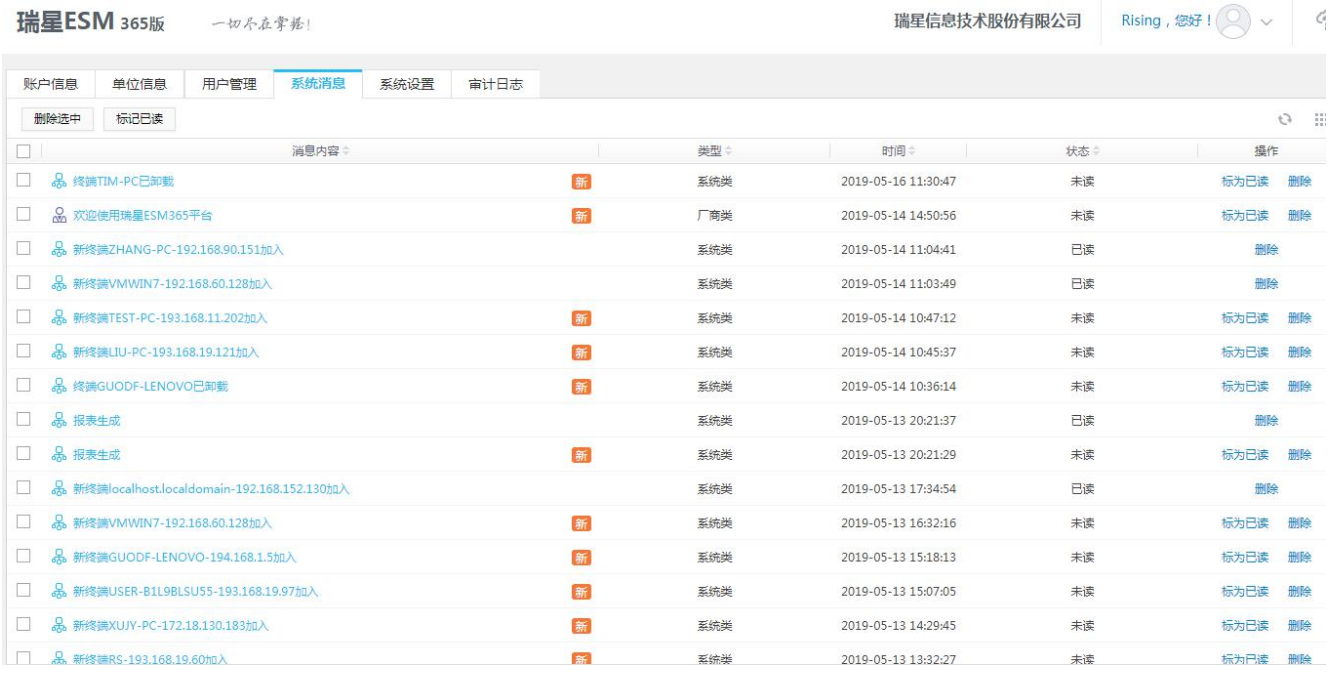
2.点击账号后操作栏中的解锁按钮，如图红框所示。

解锁后，账号状态又变为“正常”。

另一种方式就是自动解锁，等待超过设置的解锁时间后，账户自动解锁。

3.1.7.4 系统消息

系统消息是对中心所有的消息进行集中查询和管理。可标记消息状态，未读消息右侧都有【新】的图标，读取消息后图标消失，或者点击操作中的【标记已读】按钮，标记为已读。勾选多个消息记录，然后点击【标记已读】，可以批量将消息记录标记为已读；点击【删除】，可以批量将消息记录删除。如图所示。



在列表中勾选要删除的消息记录，点击【删除选中】可以进行批量删除。或者直接点击某条消息记录后的【删除】进行删除操作。

3.1.7.5 系统设置

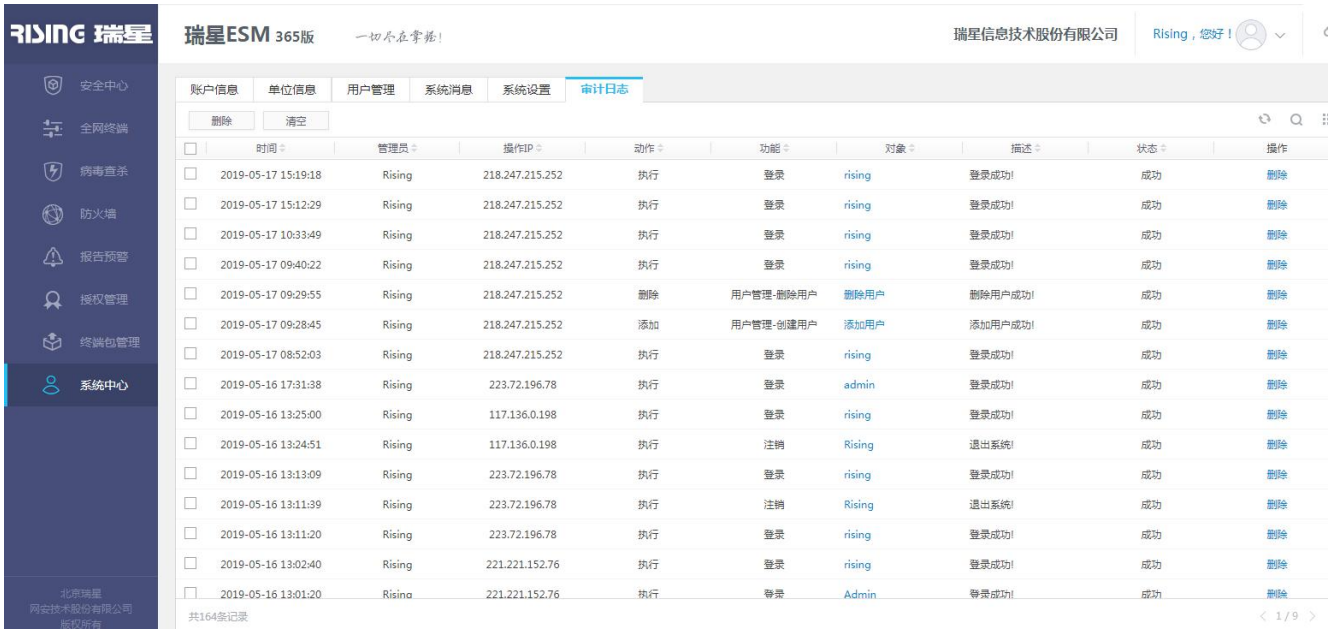
客户端清理，设置一定天数后，自动清理为连接中心的客户端，同时还可以同步清理客户端的日志。

可以设置自动入组的规则。

还可以设置服务端日志保存时间。

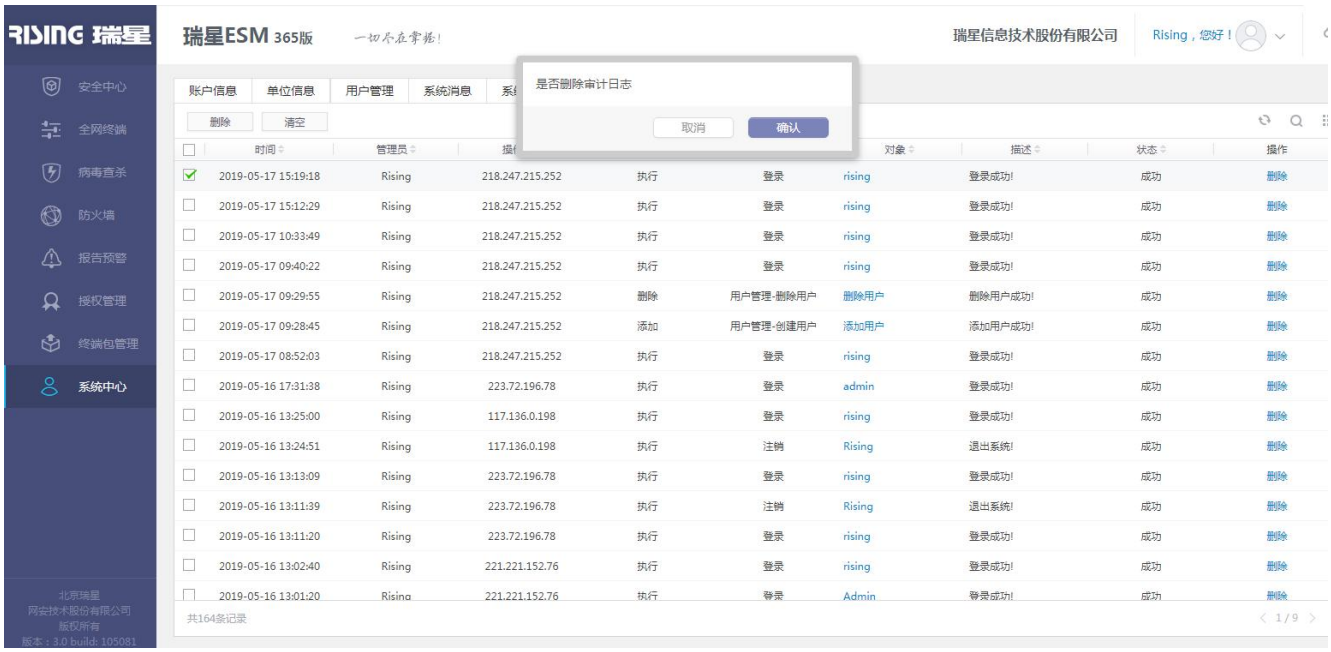
3.1.7.6 审计日志

进入审计日志界面，如图所示。



超级企业管理员可以查看中心的所有终端审计日志，记录中心账户的操作日志，包括客户端登录、客户端注销、生成报告历史记录、升级更新记录等。如图所示。

在列表中勾选不需要的日志，点击【删除】可以进行批量删除。如图所示。



点击【确认】，完成批量删除。

如需清空日志，直接点【清空】，弹出如图所示确认界面，点击【确认】，所有日志将被清空，请谨慎操作。

3.1.7.7 单位信息

初次登陆中心时，系统会提示企业信息不完整，请按照要求补充完整。

3.2 安全管理员

安全管理员由超级企业管理员创建，超级企业管理员可以同时创建多个安全管理员。使用安全管理员登录，可以使用除权限管理和账户管理外的大部分功能。管理中心的日常管理维护都由安全管理员来完成。

安全管理员登录管理中心后的操作和使用，请参考超级企业管理员部分内容，这里不再赘述。

4 Linux 客户端

4.1 安装

安装前，从安全管理员或者超级企业管理员处获得客户端下载链接。用浏览器访问获得的地址（例如：https://esm365.rising.cn/Install/index/XXX），点击【↓安装包下载】下载 Linux 客户端。

1.下载完 Linux 安装包后，打开 Linux 或者国产系统的终端（terminal），定位到安装包所在目录，使用如下命令进行解压（XXXX.tgz 为刚才下载的安装包名称）：

tar zvxf XXXX.tgz

2.进入解压后的目录，可以看到安装脚本 setup.sh，然后执行安装命令：

./setup.sh text

3.客户端自动安装完成，会提示“Install finished, enjoy it”，表明安装成功。安装过程如下图所示。

```
[root@localhost ~]# tar zvxf Linux终端默认全包_1561451281.tgz
3.0.0.9/
3.0.0.9/product.xml
3.0.0.9/setup.sh
3.0.0.9/common/
3.0.0.9/common/common.rpk
3.0.0.9/common/config.rpk
3.0.0.9/setup/
3.0.0.9/setup/aarch64/
3.0.0.9/setup/aarch64/ep.rpk
3.0.0.9/setup/aarch64/xav.rpk
3.0.0.9/setup/aarch64/xfw.rpk
3.0.0.9/setup/aarch64/ravsetup.bin
3.0.0.9/setup/x86_64/
3.0.0.9/setup/x86_64/ep.rpk
3.0.0.9/setup/x86_64/xav.rpk
3.0.0.9/setup/x86_64/xfw.rpk
3.0.0.9/setup/x86_64/ravsetup.bin
3.0.0.9/setup/mips64/
3.0.0.9/setup/mips64/ep.rpk
3.0.0.9/setup/mips64/xav.rpk
3.0.0.9/setup/mips64/xfw.rpk
3.0.0.9/setup/mips64/ravsetup.bin
3.0.0.9/antivirus.cfg
[root@localhost ~]# cd 3.0.0.9/
[root@localhost 3.0.0.9]# ls
antivirus.cfg  common  product.xml  setup  setup.sh
[root@localhost 3.0.0.9]# ./setup.sh text
************************************************************************
*                                                                      *
*                                                                      *
*                RISING ANTIVIRUS SETUP SOFTWARE                       *
*       COPYRIGHT FOR BEIJING RISING TECHNOLOGY CO.,LTD. 2015-2018     *
*                                                                      *
************************************************************************

Unpacking pack file xav.rpk ...
Unpacking pack file xfw.rpk ...
Install finished, enjoy it
```

4.等待程序自动安装完成后，可以在桌面的托盘看到软件图标，也可以在程序界面看到图标。如图为 CentOS 系统安装后，在系统工具里可以找到。

4.2 卸载

卸载需要用到安装时的安装包。进入安装包的解压目录，执行如下安装命令，开始卸载。

./setup.sh text

同意软件协议，输入“yes”并回车，软件将自动卸载完毕。如下图所示。

```
[root@localhost 3.0.0.10]# ./setup.sh text
*******************************************************************************
*                                                                             *
*                                                                             *
*                  RISING ANTIVIRUS SETUP SOFTWARE                            *
*       COPYRIGHT FOR BEIJING RISING TECHNOLOGY CO.,LTD. 2015-2018            *
*                                                                             *
*******************************************************************************
Do you agree the license of this software?(yes/no/view)[yes]>yes
```

程序继续卸载直到完成，并显示出提示信息。

4.3运行

在桌面托盘，直接双击杀毒软件的图标，即可弹出主界面。

或者直接在桌面点击瑞星杀毒软件图标启动。

4.4病毒查杀

4.4.1 主程序界面

瑞星ESM 365客户端主程序界面如下图所示。

主程序界面包括：

- 查杀按钮：用于进行病毒查杀操作，包括【全盘查杀】、【快速查杀】和【自定义查杀】。
- 智能安全引擎：配备四个查杀引擎，分别为：基础引擎、决策引擎、云查杀引擎、基因引擎。
- 设置按钮：主窗体右上角，点击设置按钮后可配置客户端策略。
- 菜单栏：点击菜单栏后，可以查看病毒日志，查看病毒隔离区。

状态栏：显示了软件的当前版本和更新日期，当扫描或者查杀病毒时，显示文件数、病毒数和当前扫描文件路径。

4.4.2 快速查杀

点击【快速查杀】，启动快速查杀。快速查杀会扫描如内存、系统文件等关键区域。通常利用快速查杀就可以杀掉大多数病毒。

查杀时，可以选择查杀模式：自动、高速、办公。

扫描中，带毒文件名、文件路径、病毒名称、威胁类型和处理状态将显示在查毒结果栏内。

扫描结束后，扫描结果将自动保存到瑞星杀毒软件安装路径下的日志目录中，您可以通过历史记录来查看以往的扫描结果。

4.4.3 全盘查杀

点击【全盘查杀】，启动全盘查杀。全盘查杀会扫描电脑所有磁盘及其文件，全面清除各种病毒、木马、后门、蠕虫等。全盘查杀需要很长时间，建议在空闲时间或者晚上进行。

扫描中，带毒文件名、文件路径、病毒名称、威胁类型和处理状态将显示在查毒结果栏内。扫描结束后，扫描结果将自动保存到瑞星杀毒软件安装路径下的日志目录中，您可以通过历史记录来查看以往的扫描结果。

4.4.4 自定义查杀

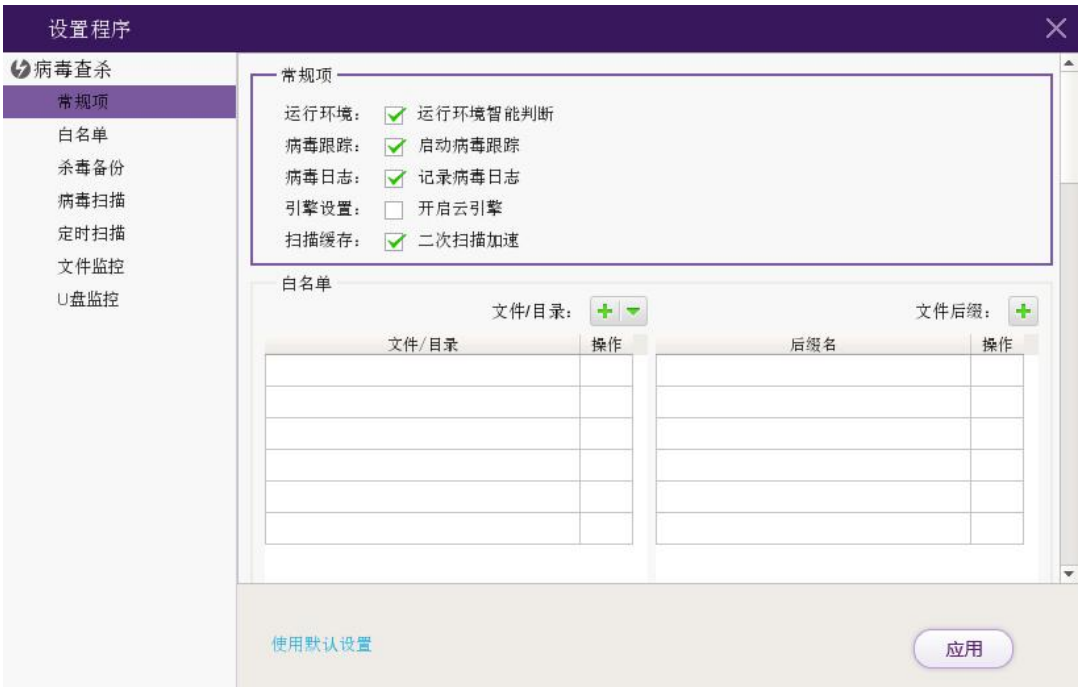
点击【自定义查杀】，选择需要扫描的路径，然后点击【开始查杀】，软件开始自定义扫描。此项操作适用于需要同时查杀多个指定位置文件和文件夹，操作起来更快捷，无需查杀全部文件。最后点击【开始查杀】，开始杀毒。如下图所示。

4.5策略设置

4.5.1 常规项

在程序的主界面，选择菜单【设置】/【病毒查杀】/【常规项】，打开常规项设置界面。

- 运行环境：勾选【运行环境智能判断】选项后，软件将自动设置好参数，适应系统，发挥最好的性能。
- 病毒跟踪：勾选【病毒跟踪】选项后，软件将启用病毒跟踪功能，对常见和流行性病毒进行实时跟踪。
- 病毒日志：勾选【病毒日志】选项后，软件将会对系统查杀和扫描的病毒信息进行记录，方便进行病毒分析和病毒防御。
- 云引擎设置：可以设置为公有云引起或者私有云引擎。
- 扫描缓存：勾选【二次扫描加速】选项后，软件将开启二次扫描加速功能，对一段时间内的扫描状态进行缓存和优化，使扫描更快、更流畅。



4.5.2 白名单

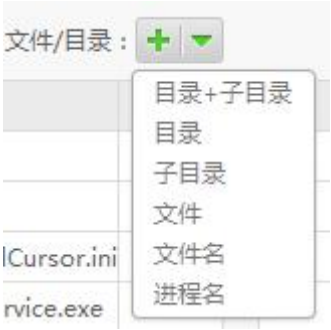
白名单用于添加那些不需要扫描和查杀的文件，添加白名单后，软件扫描和监控时将智能跳过这些文件。

在程序的主界面，选择菜单【设置】/【病毒查杀】/【白名单】打开白名单设置界面。

白名单添加方式分为两种：一种是以文件/目录方式，另一种是以文件后缀方式。如下图所示。

4.5.2.1 文件/目录

点击【病毒查杀】>【白名单】，然后在文件/目录栏点击图标“  ”，出现下拉菜单，如图所示。



在菜单中，可以通过四种方式设置文件和目录，分别是：

目录+子目录：扫描时，软件将所选的目录和它的子目录一起忽略。

目录：扫描时，软件将忽略掉所选目录中的文件，而其子目录中的文件依然会扫描到。

子目录：扫描时，软件只忽略所选目录的子目录及其文件。

文件：扫描时，软件忽略掉所选的文件。

文件名：扫描时，所有符合设定文件名的文件都将忽略。

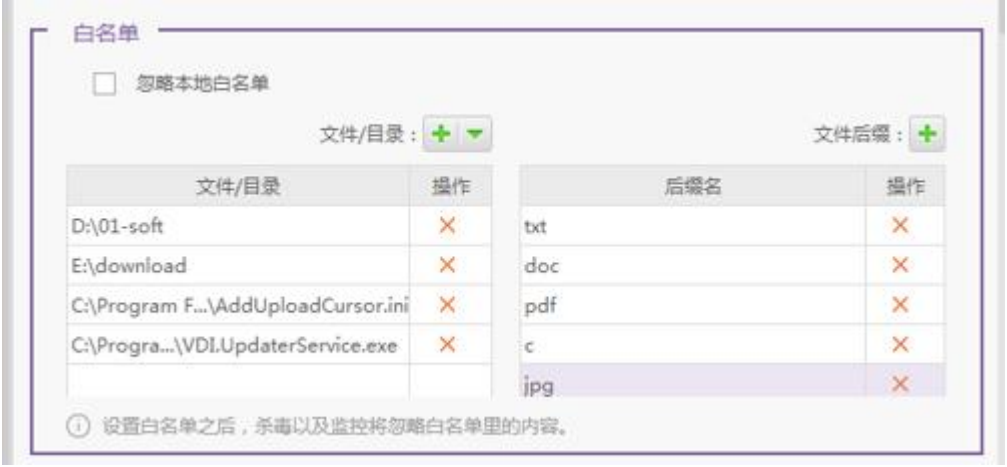
进程名：扫描时，符合设定进程名的将智能忽略。

如果需要将已经加入白名单的文件/目录删除，请点击表中“操作”一栏的删除【X】。

设置完成后，点击右下角【应用】，保存设置。

4.5.2.2 文件后缀

点击【病毒查杀】>【白名单】，然后在文件后缀一栏点击图标【+】，下方的表格中将添加一行，输入需要加入白名单文件的后缀名，如图所示。



如果要从白名单中删除，点击“操作”一栏中的删除【X】。

设置完成后，点击右下角【应用】，保存设置。

4.5.3 杀毒备份

杀毒备份对应于病毒隔离区，杀毒软件进行病毒查杀的时候，会把病毒和被病毒感染的文件移至隔离区。通过杀毒备份，设置不同情形下的病毒文件处理方式。既可以有效防止继续感染其他文件，又可以保留被病毒感染的文件。

点击【设置】>【病毒查杀】>【杀毒备份】，进入病毒备份设置，如下图所示。

杀毒备份设置项如下：

备份文件：勾选【杀毒时备份原文件】，即可将病毒文件备份到隔离区，供以后使用。

文件超长：查杀时，文件很大，可以设置询问、直接删除、不处理。

空间不足：当隔离区备份的文件过多，导致隔离区空间不够时，空间的处理方式可以自动覆盖老文件，或者空间自动增长。用户根据具体环境进行选择。

备份失败：当备份病毒文件失败时，可以设置询问我、删除文件和不处理的方式。用户根据具体环境进行选择。

所有设置项设置完成后，点击右下角【应用】，保存设置。

4.5.4 病毒扫描

病毒扫描可以设置扫描文件类型、查杀引擎的选择等。

点击【设置】>【病毒查杀】>【病毒扫描】，进入病毒扫描设置，如图所示。

文件类型：杀毒软件需要在查杀时扫描的文件类型，默认为所有文件，也可以选择程序和文档。

查杀引擎：杀毒软件带有 4 个查杀引擎，分别针对不同类型的病毒和安全威胁。勾选“仅查杀流行病毒”，会重点查杀最近比较活跃的病毒；勾选“启发式查杀”，可以有效的对可疑的文件查杀；勾选“启动压缩包查杀”，并设置好压缩包的容量，查杀时可以解开限定容量的压缩包进行查杀。

发现病毒：发现病毒的处理方式，可选自动或者手动。自动方式无需用户确认，自行清除病毒文件；手动处理方式，需要用户确认是保留还是删除病毒文件。不处理，只显示扫描结果，不做任何操作。

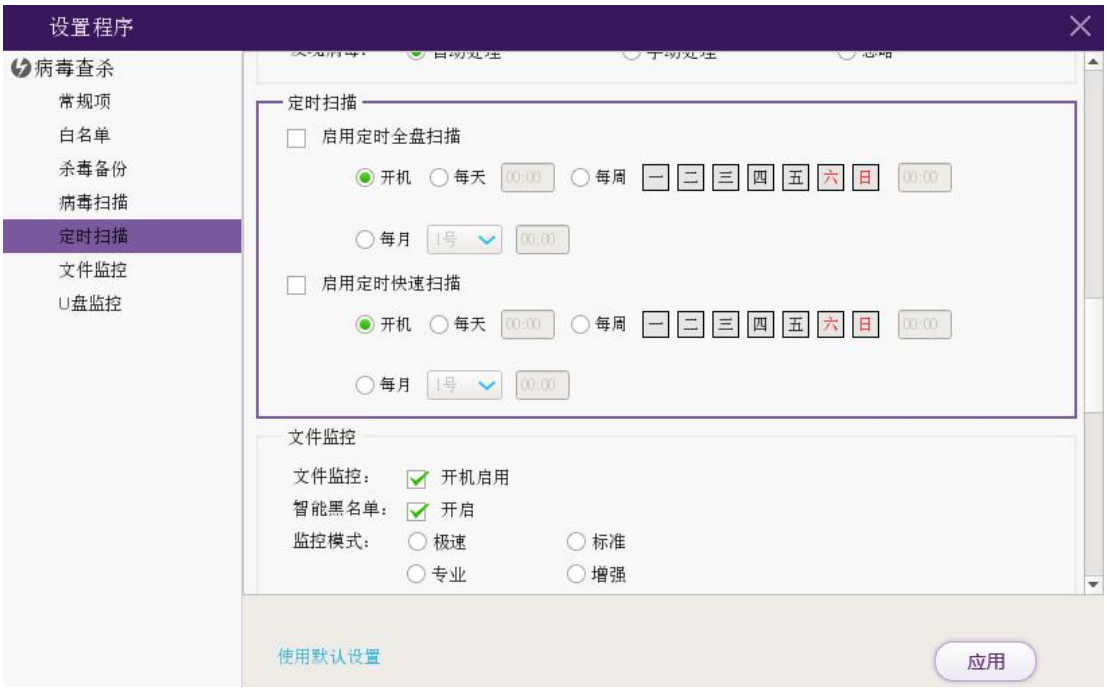
清除失败：当病毒清除失败时，设置为直接处理或者不处理。

所有设置项设置完成后，点击右下角【应用】，保存设置。

4.5.5 定时扫描

定时扫描可以设置特定日期和时间进行病毒扫描。

点击【设置】>【病毒查杀】>【定时扫描】，进入定时扫描设置，如图所示。



启用对全盘扫描：勾选后，启用请示全盘扫描功能。

设置定时模式，开机扫描、每天定时扫描、每周定时扫描、每月定期定时扫描。如图中所示为每周工作日 12:00 定时扫描。

启用定时快速扫描：勾选后，可以设置定时快速扫描，和定时全盘扫描的区别是，定时快速扫描速度更快，只扫描系统关键区域的文件和目录。

设置定时快速扫描的模式：开机扫描、每天定时扫描、每周定时扫描、每月定期定时扫描。如图中所示为每天 9:00 定时快速扫描。

所有设置项设置完成后，点击右下角【应用】，保存设置。

4.5.6 文件监控

文件监控能对终端的读写、文件、程序进行实时保护，一旦发现可疑文件和可疑操作立即拦截。

点击【设置】>【病毒查杀】>【文件监控】，进入文件监控设置，如图所示。

文件监控设置项如下：

文件监控：勾选【开机启用】，则文件监控功能随计算机启动，实时监控扫描病毒和木马。

智能黑名单：勾选【开启】，黑名单生效。

监控模式：文件监控模式，分为极速、标准、专业和增强。每一种模式适用于不同的场景和环境。

1.极速模式，可快速的监控常见文件和程序，监控使用的资源低，不会影响用户正常使用电脑；

2.标准模式，一般采用的模式，兼顾速度和监控效率，能够监控到大部分的威胁和病毒爆发；

3.专业模式，为用户特殊需求设计，能够针对性的监控文件，如对 word 等 office 文档的增强监控，可以有效的降低宏病毒的影响。可以自定义文档类型，诸如 CFG;DAT；BIN 等 Windows 常见文件的增强监控。能有效拦截恶意脚本恶意配置文件。

4.增强模式，为用户提供最全面的监控，对系统内所有文件和程序类型提供强力监控，缺点是占用系统资源相当高，可能会影响用户使用体验。

文件类型：可以选择【所有文件】或者【程序和文档】或者【指定文件类型】。

监控加速：勾选【信任程序分析】，监控加速功能生效。

查杀引擎：勾选【仅查杀流行病毒】，即对活跃病毒进行重点的查杀；勾选【启发式查杀】，即将所有的可疑文件都列入查杀范围；勾选【启动压缩包查杀】，即可以查杀压缩包内的文件，同时对压缩包的大小和曾经可以进行限定。

发现病毒：选择发现病毒时的处理方式，可选择【自动处理】，如需手动处理，则选择【手动处理】。

清除失败：当病毒清除失败时，可选直接处理或者不处理。

报告结果：勾选后开启功能，病毒清除成功后通知用户。

所有设置项设置完成后，点击右下角【应用】，保存设置。

4.5.7 U 盘监控

U 盘监控，对 U 盘进行防护，能有效的防止病毒从 U 盘感染计算机。

点击【设置】>【病毒查杀】>【U 盘监控】，进入 U 盘监控设置，如图所示。

插入 U 盘时：设置插入优盘时的操作，选择【询问是否查杀】或者【立即查杀】。

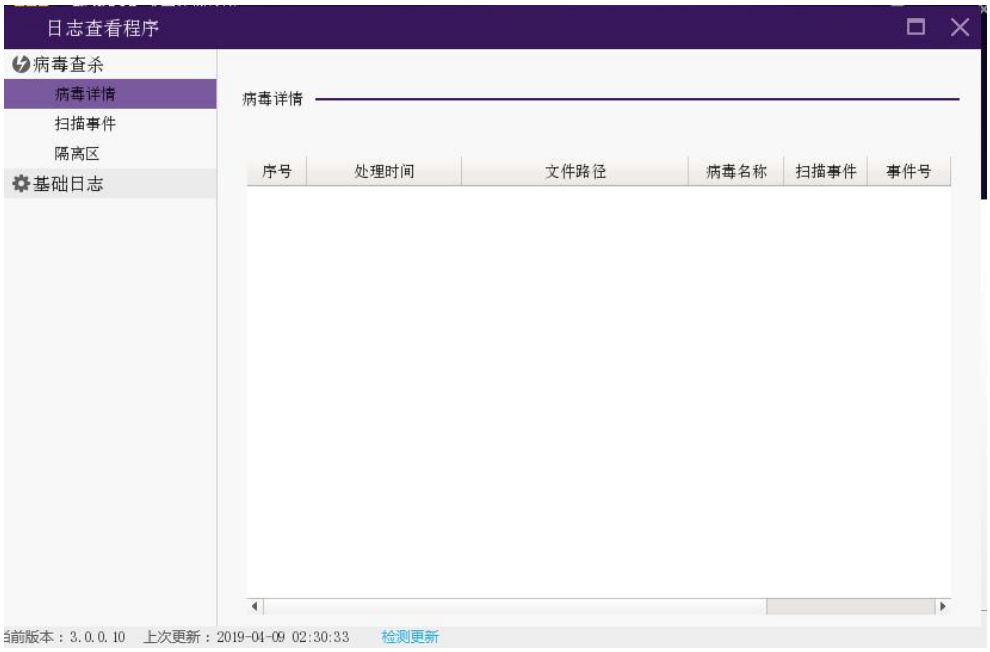
查杀深度：可以设置对 U 盘文件的查杀递归层次，数字设置越大，能查杀的目录层次越深，查杀的文件越多。

所有设置项设置完成后，点击右下角【应用】，保存设置。

4.6 日志管理

用户在客户端可以查看客户端本地的查杀情况，包括扫描日志、病毒日志。通过日志报告，用户可查看本机扫描病毒的记录，包括开始时间、结束时间、病毒数、清除数、文件数和扫描方式信息。

操作方法：点击【菜单】/【日志】，进入日志查询页面。

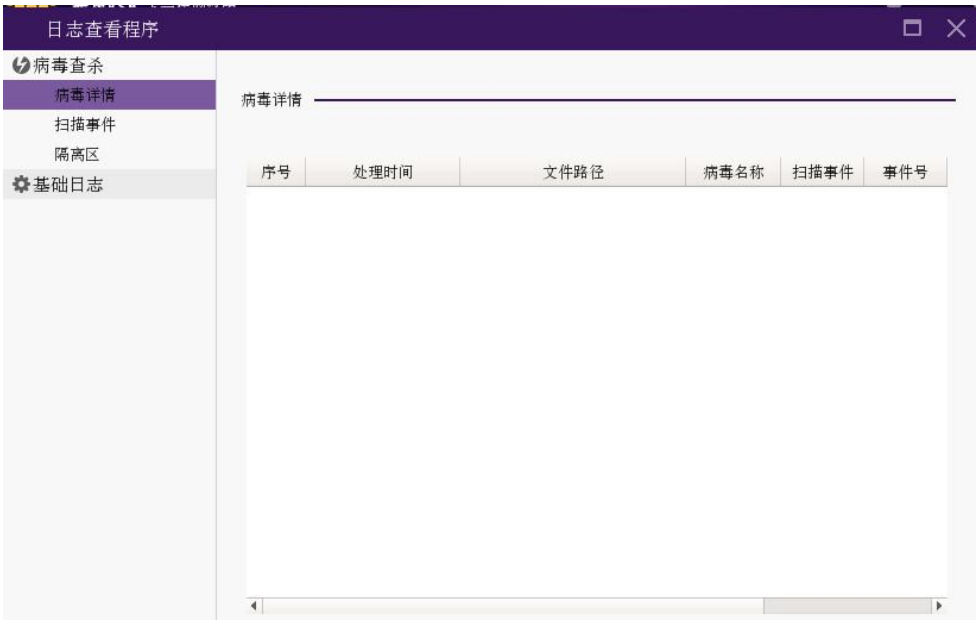


4.6.1 病毒查杀

病毒查杀日志记录了查杀操作、查杀病毒信息、隔离区信息等。

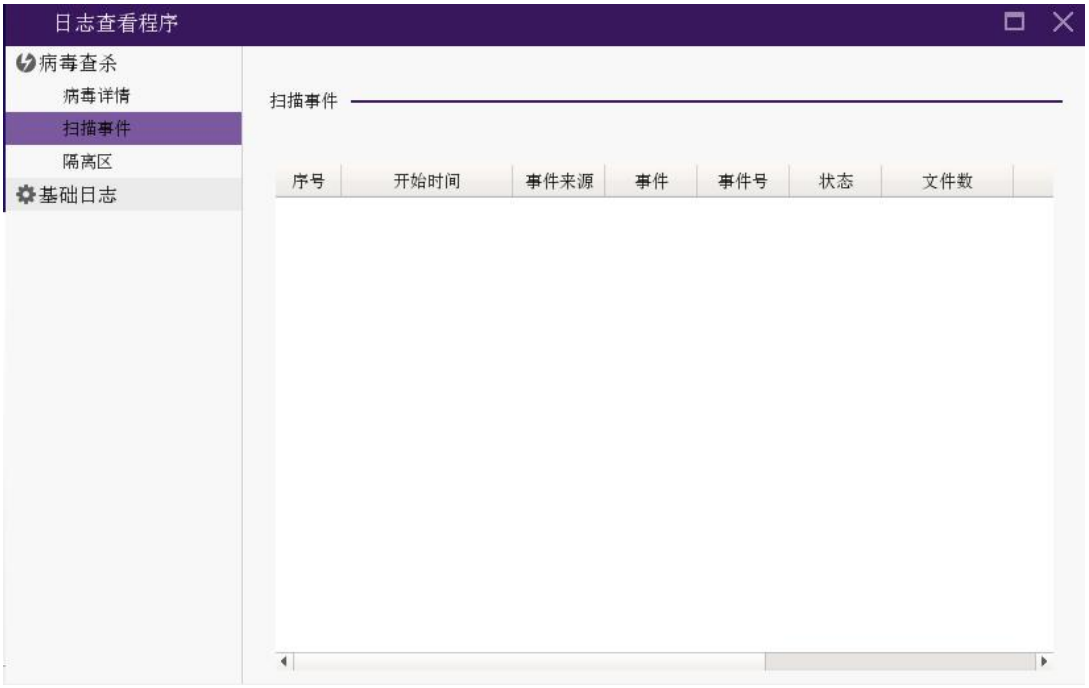
4.6.1.1 病毒详情

在病毒详情页面，用户可以查看到杀毒软件扫描或者监控到的所有病毒信息，包括扫描或监控到的时间、文件路径、病毒名称、威胁类型和状态等。可以按时间、来源和处理方式对扫描或监控到的病毒进行筛选。



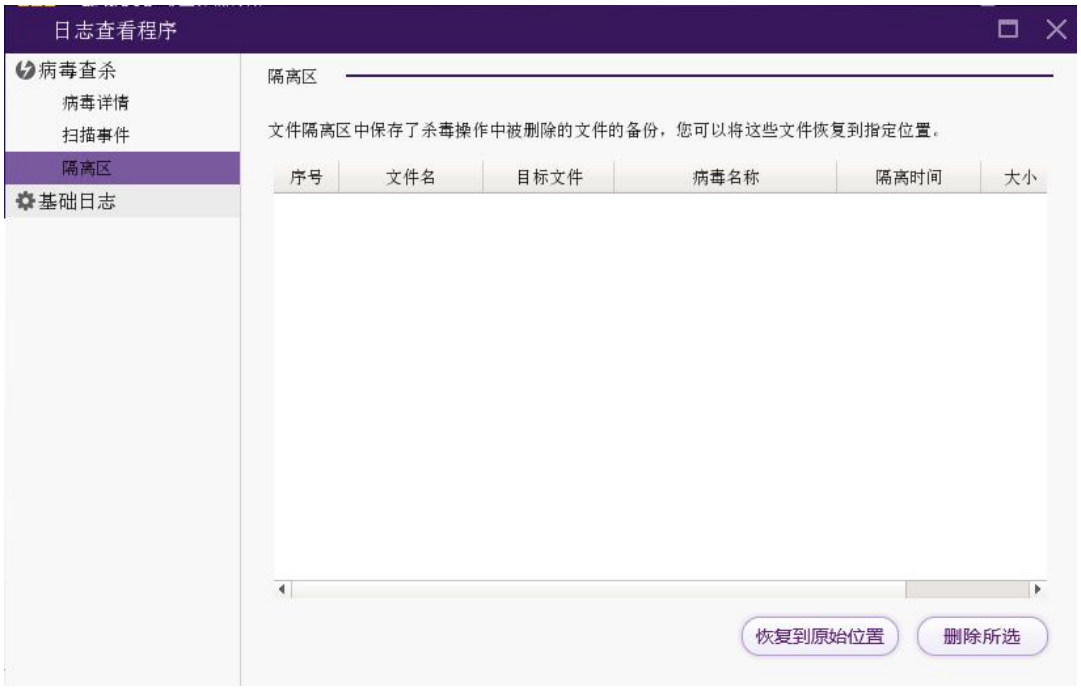
4.6.1.2 扫描事件

点击【扫描事件】，进入扫描事件页面，本页面记录了杀毒软件的扫描记录。



4.6.1.3 隔离区

点击【隔离区】，进入隔离区页面，文件隔离区中保存了杀毒操作中被删除的文件备份。



勾选隔离区的文件，下方的操作按钮变亮，可以将文件【恢复到原始位置】、【恢复到指定位置】、【删除所选】和【加入白名单】。恢复到原始位置，是将病毒文件恢复初始位置；恢复到指定位置，用户可以将他恢复任意位置；删除所选，选择要删除的病毒文件，进行删除，并且不可恢复。

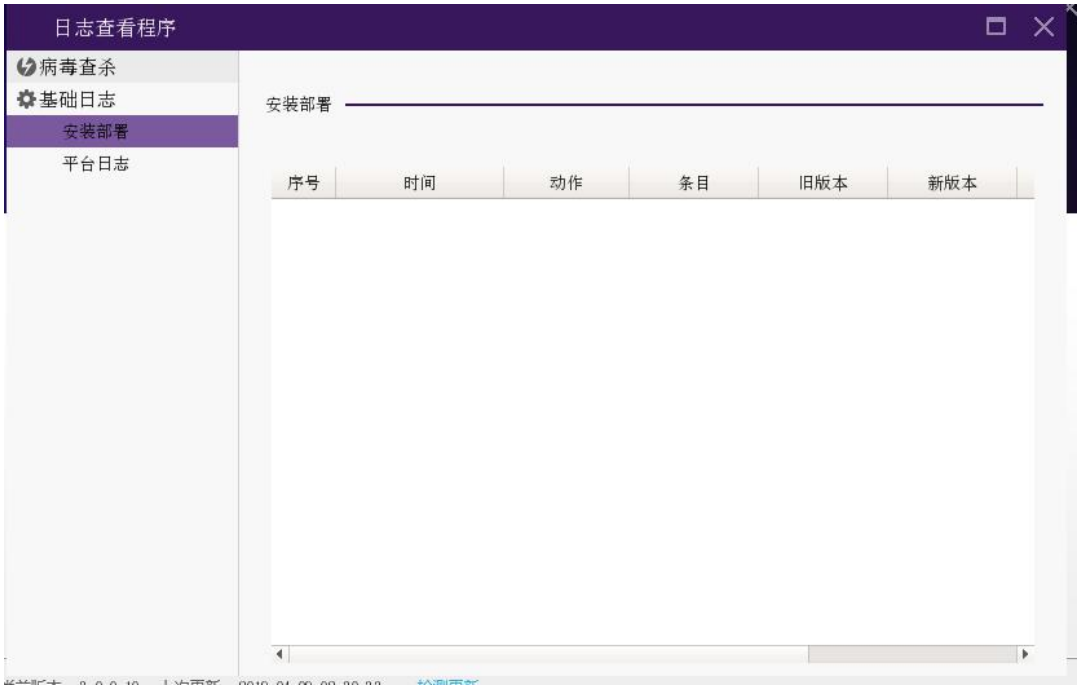
在隔离区页面详细的记录了病毒文件的文件名、目标文件、病毒名称、隔离时间和大小。在文件搜索框中可以对文件名进行搜索。

4.6.2 基础日志

点击【基础日志】，可以查看安装部署日志和平台日志。

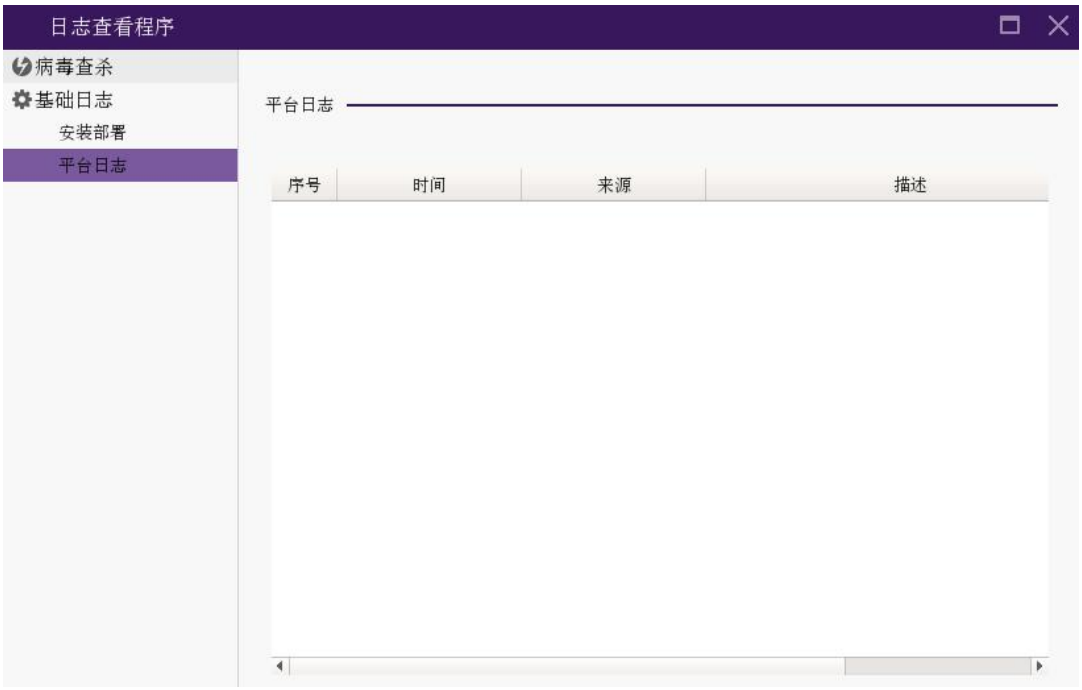
4.6.2.1 安装部署

通过安装部署日志，可以查询安装软件、插件的时间、动作、条目、旧版本、新版本和重启标识等。如，在动作中可以看到，安装是通过定时升级、手动还有远程修复等方式实现。



4.6.2.2 平台日志

平台日志则可以查询登录管理平台的相关日志信息。包括登录的时间、来源和描述。通过平台日志，能够及时发现异常登录。


日志查看程序
病毒查杀
基础日志
安装部署
平台日志
平台日志
序号
时间
来源
描述

5 Windows 客户端

瑞星 ESM 365 Windows 客户端适配 Windows 7 以上版本的系统。具备病毒查杀、上网防护、防火墙等功能。

5.1 安装

安装前，从安全管理员或者超级企业管理员处获得客户端下载链接。用浏览器访问获得的地址（例如：https://esm365.rising.cn/Install/index/XXX），点击【↓安装包下载】下载 Windows 客户端。如图所示。

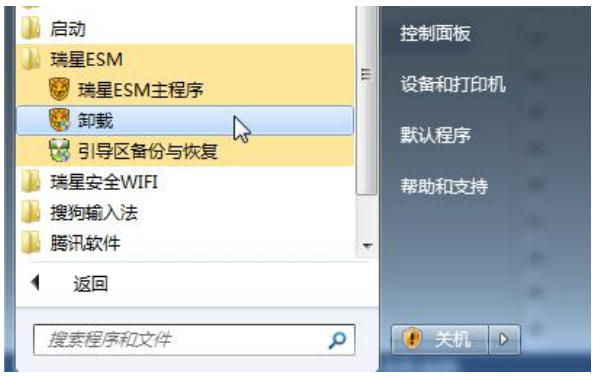
待安装包下载完成后，双击安装包启动安装，点击【开始】。

安装包将自动加载并开始安装。

安装完成，点击【开启安全之旅】，进入客户端软件主界面。

5.2 卸载

需要卸载软件时，请依次点击电脑的【开始】/【所有程序】/【瑞星 ESM】/【卸载】。如图所示。



在弹出的界面中点击【开始卸载】，如需删除隔离区文件，请勾选【删除“隔离区”文件】，如图所示。

5.3 系统托盘

鼠标右键点击系统托盘  图标，可进行【打开主程序】、【快速查杀】、【自我防护】、【设置】、【日志】、【升级】和【退出】操作。

打开主程序

点击【**打开主程序**】，包括以病毒查杀、网络防护为主的各种功能。还可以通过鼠标左键单击托盘图标，直接打开主界面。

快速查杀

点击【**快速查杀**】，启动快速查杀病毒功能，客户端随即开始快速查杀。

自我防护

点击【**自我防护**】开关，可开启或者关闭客户端的自我保护功能。

设置

点击【设置】，弹出设置中心，可快速进行客户端的设置。

日志

点击【日志】，弹出日志中心，可快查看客户端的日志。

升级

点击【升级】后，客户端开始自动升级。

退出

点击【退出】后，托盘与主界面退出。若再次启动可从 Windows 桌面的快捷方式，或者在 Windows 桌面依次选择【开始】/【程序】/【ESM 365】，进行启动。

5.4病毒查杀

客户端防病毒模块为用户提供了杀毒软件客户端主程序，是用户操作防病毒的入口。安装防病毒后，杀毒软件客户端主程序随系统自动启动。用户关闭杀毒主程序后，可通过桌面图标、开始菜单或者双击系统托盘图标 打开主程序。

病毒查杀界面包括快速查杀、全盘查杀和自定义三项子功能，右下角可以勾选【发现病毒自动处理】和【扫描完成自动关机】。

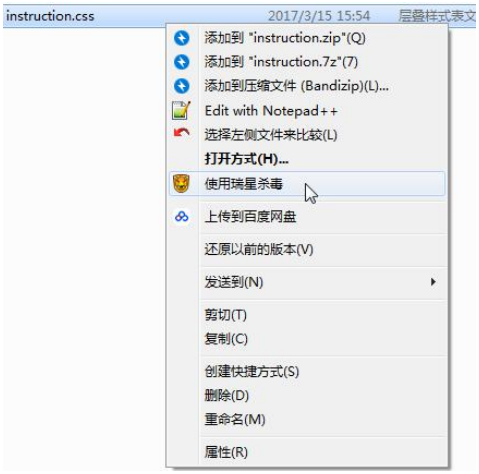
在扫描过程中，您可以随时点击【暂停】按钮来暂时停止查杀病毒，点击【继续】按钮则继续查杀，或点击【停止】按钮停止查杀病毒。

5.4.1 右键查杀

右键查杀实际上是自定义查杀的一种方式，因为操作快捷方便，使用频率更高。

如果需要对某一文件或者某一个文件夹进行杀毒，您可以将该文件或文件夹用鼠标拖入客户端界面内，软件将自动开始查杀。

还可以通过右键点击文件或者文件夹，选择【使用瑞星杀毒】，可快速查杀指定目标。如下图所示。



查杀时的效果图。

查杀结束后显示杀毒结果。

5.4.2 快速查杀

点击【快速查杀】，启动快速查杀。快速查杀会扫描您的电脑中各种蠕虫等病毒易于存在的系统位置，如内存、系统文件等关键区域，查杀速度快，效率高。通常利用快速查杀就可以杀掉大多数病毒，防止病毒发作。

5.4.3 全盘查杀

点击【全盘查杀】，启动全盘查杀。全盘查杀会扫描您电脑所有磁盘，全面清除各种未知木马、后门、蠕虫等病毒。

全盘查杀发现病毒展示如下图：

5.4.4 自定义查杀

点击【自定义查杀】，选择扫描位置后点击【开始查杀】，软件将开始扫描您指定的文件。此项操作适用于需要同时查杀多个指定位置文件和文件夹，操作起来更快捷，查杀的结果也容易获得。

点击【开始查杀】，启动自定义查杀后的效果图如下。

任意扫描完成后显示扫描结果信息。

5.5防护中心

ESM 365 为用户提供了全面的防护机制。防护中心分为监控类防护和专杀类防护。

在主界面右下角，点击【防护中心】按钮，进入防护中心。

各防护功能通过滑动开关进行控制，点击相应功能开关即可打开或关闭功能。当功能下的开关处于【已开启】时，表示该功能开启，功能图标呈蓝色；当处于【已关闭】时，表示该功能关闭，功能图标呈灰色。

点击右下角的【安全设置】，进入所有防护功能的设置界面，可以对文件监控、邮件监控等进行详细设置。

点击右下角的【防护日志】，进入安全防护功能的日志记录界面，查看防护中心产生的日志。

点击右上角的【X】，关闭防护中心界面。

5.5.1 监控类防护

监控类防护包括：文件监控、U 盘监控、系统加固、应用加固。如图所示。

文件监控：主要针对计算机本地存储的文件，对文件的活动和状态进行有效的监控，能及时拦截病毒木马。

当文件监控发现病毒时，会以弹窗的形式提醒。若文件监控设置【发现病毒处理】设置为自动清除，则提示“发现病毒并清除成功”，如图所示：

若【发现病毒处理】设置为【手动清除】，则弹出病毒警告，提示“发现病毒需要处理”，如图所示：

弹窗将显示病毒所在位置、病毒名称、相关进程以及出现问题的原因和处理建议。

在弹窗中选择【删除】，删除病毒文件；否则，选择【不处理】，不对病毒文件做任何处理。对不做处理的病毒，可以点击文件定位图标  ，定位病毒文件位置。

如果不需要再弹窗提示，请勾选“重启前不提示”复选框，那么在重启计算机之前，都不再弹窗提示。

U 盘监控：主要针对插入计算机的 U 盘进行扫描和监控，对有害文件进行及时的拦截和处理。

系统加固：对系统的重要文件进行加固防护，保护系统安全，对破坏系统文件类型病毒有很好的防护效果。

启用系统加固后，使用文件、注册表、进程、系统文件遭到删除或篡改时，客户端将进行拦截，并弹出提示，如图所示。

应用加固：对系统安装的应用进行加固，防止病毒或木马对系统上的应用进行破坏，或者是阻止木马盗取系统应用数据。

开启应用加固后，客户端软件将对浏览器/办公软件实时进行保护。有对浏览器/办公软件进行攻击和修改的行为，都将进行拦截并弹出提示，如图所示。

5.5.2 专杀类防护

专杀类防护主要包括：飞客虫蠕虫、雨云病毒、威客虫蠕虫免疫、DLL 劫持免疫。专杀类防护功能开启后，对上述病毒进行针对性防护。如图所示。

飞客虫蠕虫：飞客虫蠕虫(Hack Exploit Win32 MS08-067)是一个利用微软 MS08-067 漏洞发起攻击的蠕虫病毒。该病毒会对随机生成的 IP 地址发起攻击，攻击成功后会下载一个木马病毒，通过修改注册表键值来使安全软件功能失效。病毒会修改 hosts 文件，使用户无法正常访问安全厂商网站及其服务。

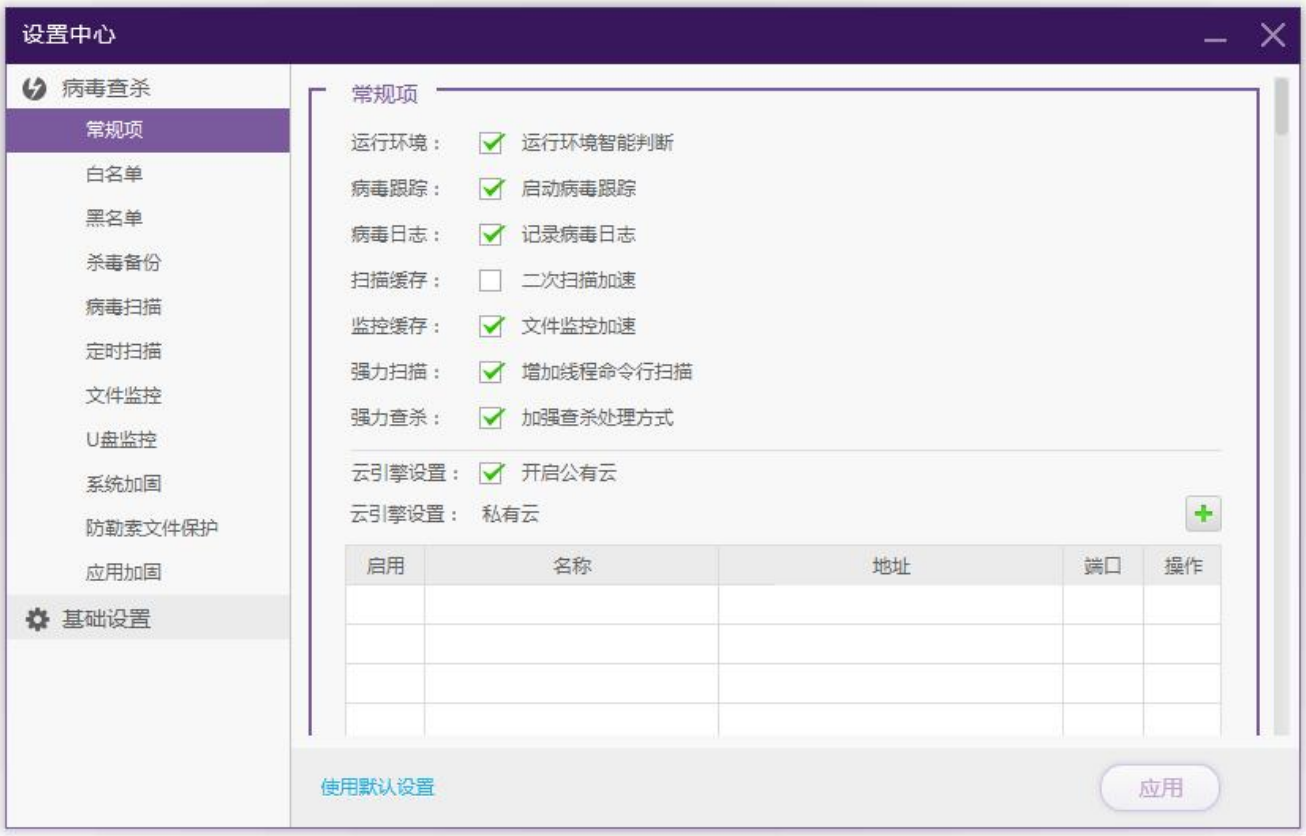
雨云病毒：雨云病毒为蠕虫病毒，中毒后的表现为任务管理器中有 wscript.exe 运行，在桌面上有名为 yuyun_ca 的图标，并且无法删除。通过共享方式进行传播，在局域网中很容易传播。

威客虫蠕虫免疫：威客虫蠕虫病毒中毒表现为无法启动系统，若启动系统后进行全盘扫描，则直接死机，该蠕虫病毒主要针对硬盘，中毒后只能格式化整块硬盘。

DLL 劫持免疫：DLL 劫持表现为，当一个可执行文件运行时，Windows 加载器将可执行模块映射到进程的地址空间中，加载器分析可执行模块的输入表，并设法找出任何需要的 DLL，并将它们映射到进程的地址空间中。

5.6设置中心

在客户端的主界面右上角点击设置图标“  ”，进入设置中心，如图所示。



设置中心分病毒查杀、基础设置。下面将详细说明各项目设置方法。所有的设置项都可以通过点击设置见面左下角的【使用默认设置】，恢复默认设置。

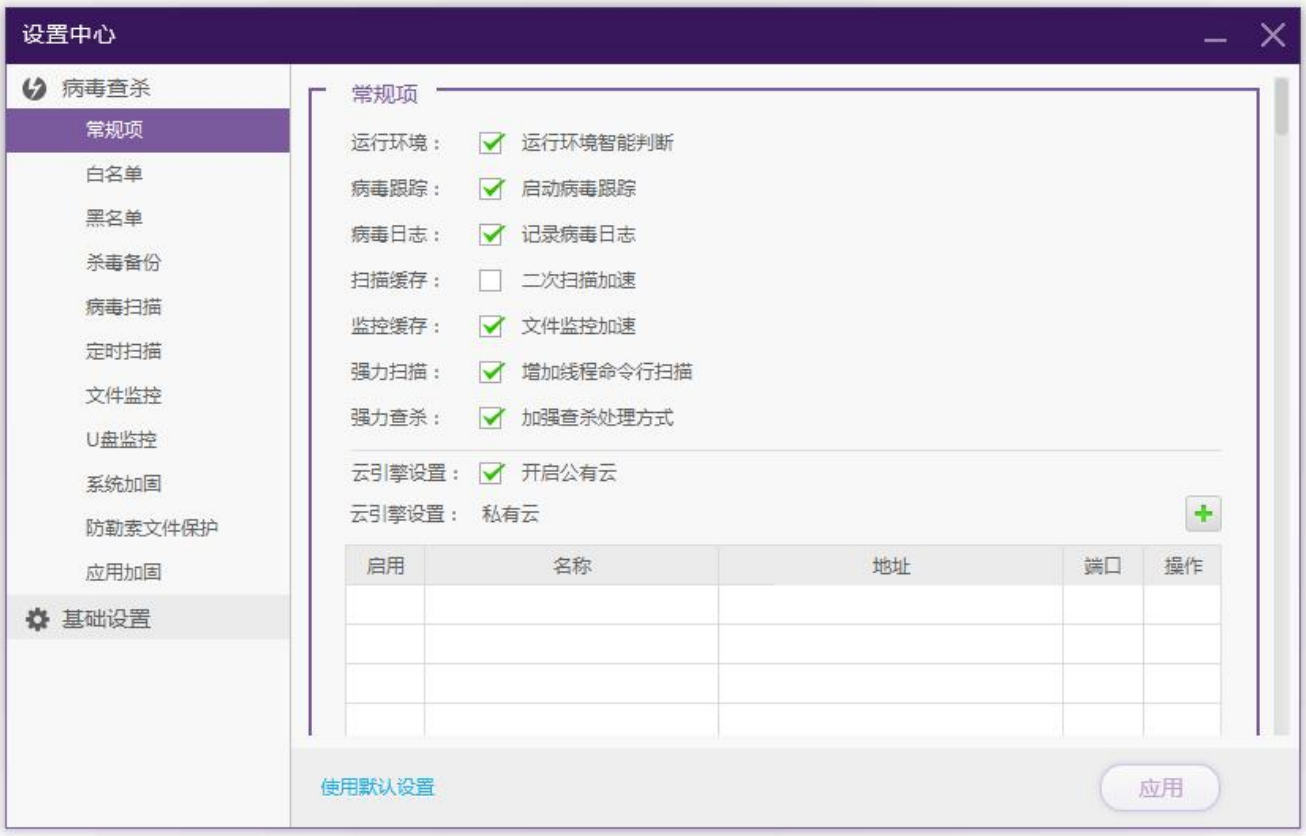
5.6.1 病毒查杀

病毒查杀设置可以对客户端的杀毒、扫描进行详细设置，主要有常规项、白名单、黑名单、杀毒备份、病毒扫描、定时扫描、文件监控、U 盘监控、系统加固、防勒索文件保护和应用加固等。

5.6.1.1 常规项

常规项设置可设置项为：运行环境、病毒跟踪、病毒日志、云引擎设置、扫描缓存、监控缓存等。

点击【病毒查杀】>【常规项】，进入常规项设置，如图所示。



运行环境：勾选【运行环境智能判断】选项后，软件将自动设置好参数，适应系统，发挥最好的性能。

病毒跟踪：勾选【病毒跟踪】选项后，软件将启用病毒跟踪功能，对常见和流行性病毒进行实时跟踪。

病毒日志：勾选【病毒日志】选项后，软件将会对系统查杀和扫描的病毒信息进行记录，方便进行病毒分析和病毒防御。

扫描缓存：勾选【二次扫描加速】选项后，软件将开启二次扫描加速功能，对一段时间内的扫描状态进行缓存和优化，使扫描更快、更流畅。

强力扫描：勾选【增加线程命令扫描】后，增强查杀引擎的扫描能力，新增线程，多个线程并发扫描。

强力查杀：勾选【加强查杀处理方式】后，使用增强型模式进行查杀，引擎和功能开启最强的模式，加快查杀速度和查杀深度。

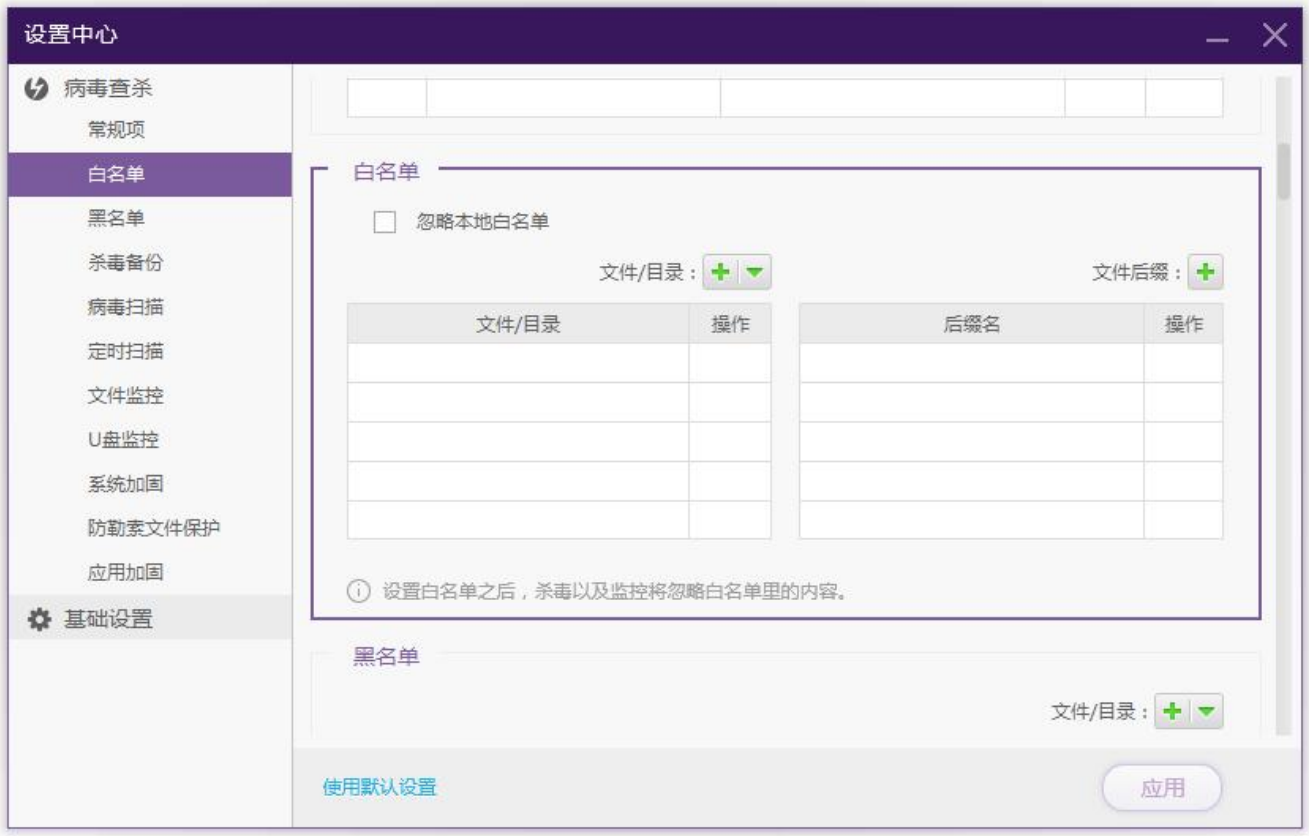
云引擎设置：可以设置为公有云引起或者私有云引擎。

勾选【开启公有云】选项后，软件将开启公有云查杀模式，使用瑞星自主研发的云引擎，提高查杀效率和速度。

启用私有云引擎步骤：点击“+”，在启用勾选，输入私有云服务器地址和端口。

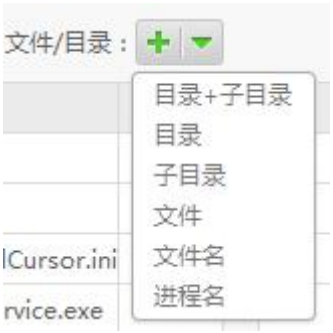
5.6.1.2 白名单

白名单用于添加那些不需要扫描和查杀的文件，添加白名单后，软件扫描和监控时将智能跳过这些文件。白名单添加方式分为两种：一种是以文件/目录方式，另一种是以文件后缀方式。如图所示。



5.6.1.2.1文件/目录

点击【病毒查杀】>【白名单】，然后在文件/目录栏点击图标“  ”，出现下拉菜单，如图所示。



在菜单中，可以通过四种方式设置文件和目录，分别是：

目录+子目录：扫描时，软件将所选的目录和它的子目录一起忽略。

目录：扫描时，软件将忽略掉所选目录中的文件，而其子目录中的文件依然会扫描到。

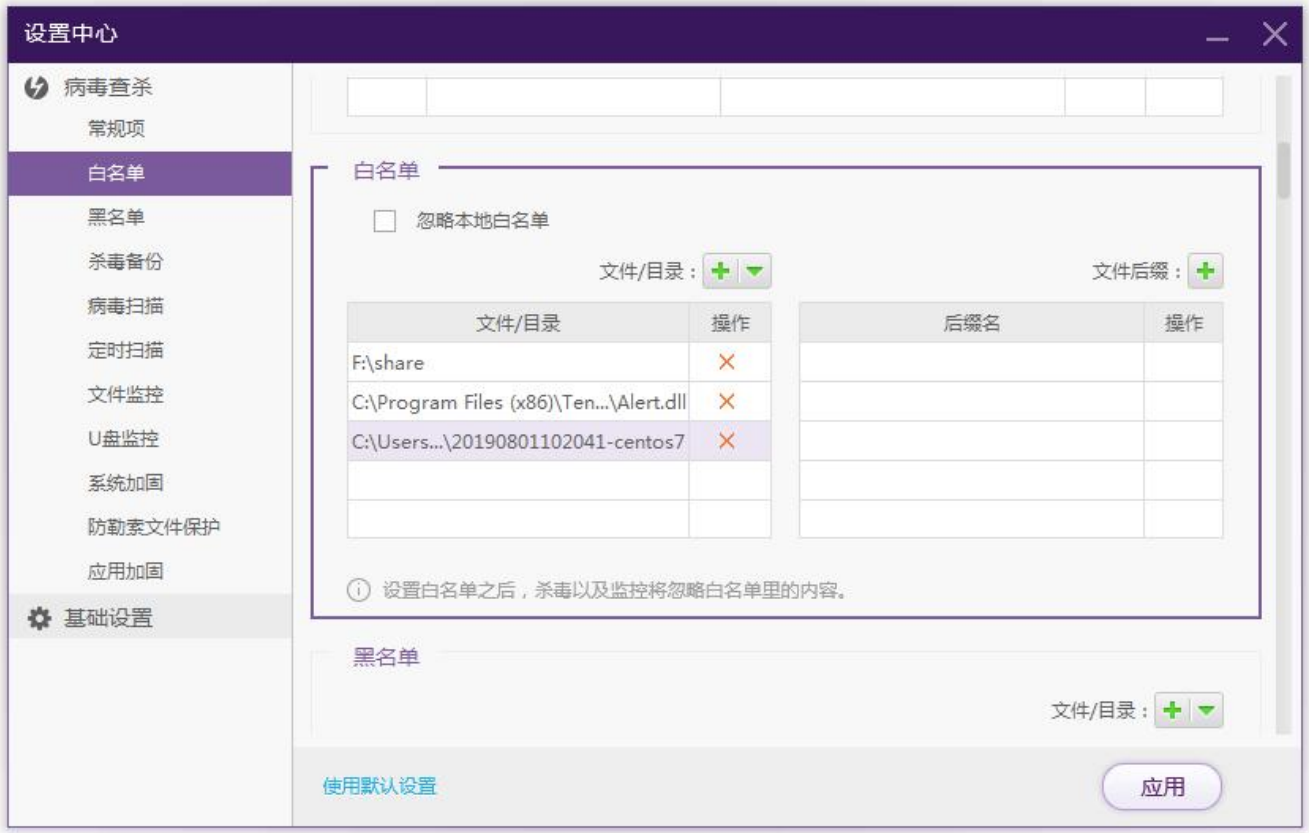
子目录：扫描时，软件只忽略所选目录的子目录及其文件。

文件：扫描时，软件忽略掉所选的文件。

文件名：扫描时，所有符合设定文件名的文件都将忽略。

进程名：扫描时，符合设定进程名的将智能忽略。

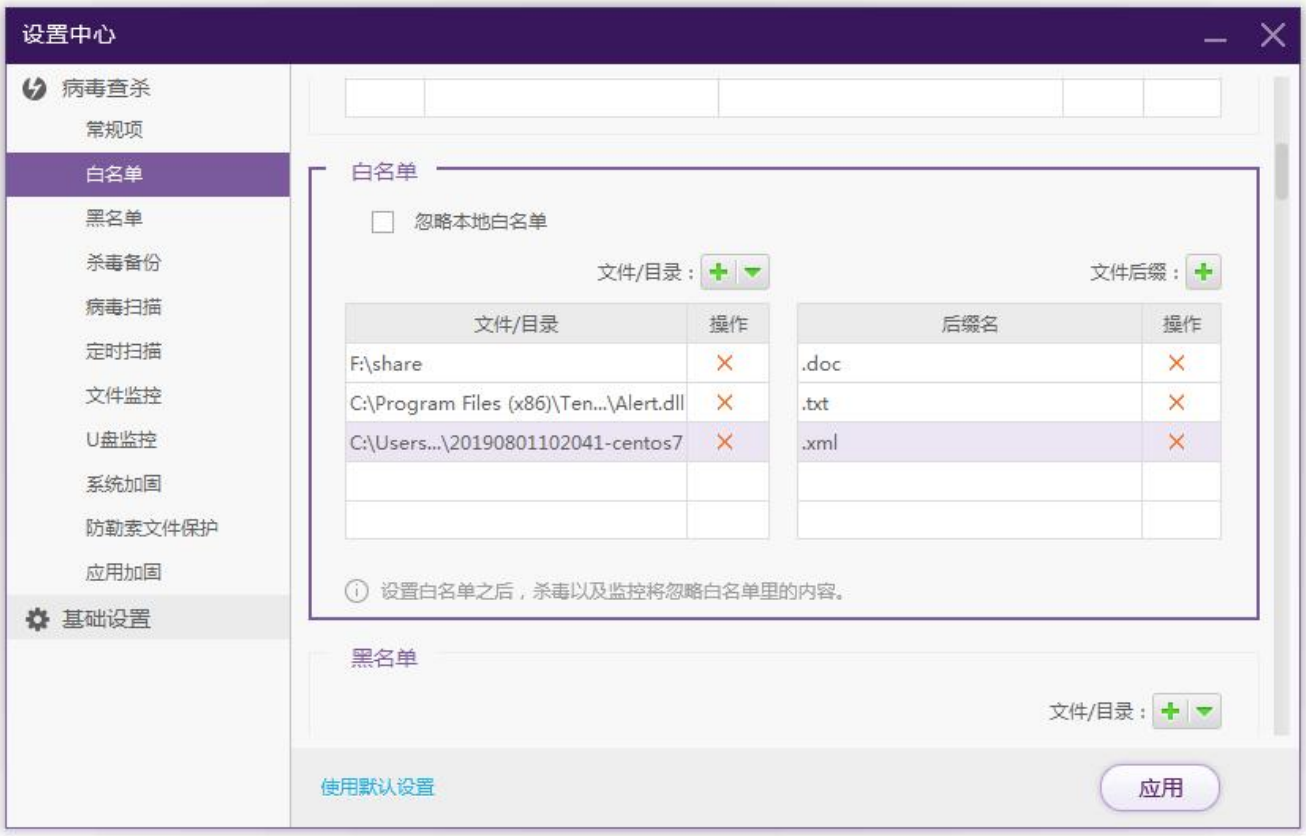
如果需要将已经加入白名单的文件/目录删除，请点击表中“操作”一栏的删除【X】。如图所示分别为添加的目录、子目录、文件和进程。



设置完成后，点击右下角【应用】，保存设置。

5.6.1.2.2文件后缀

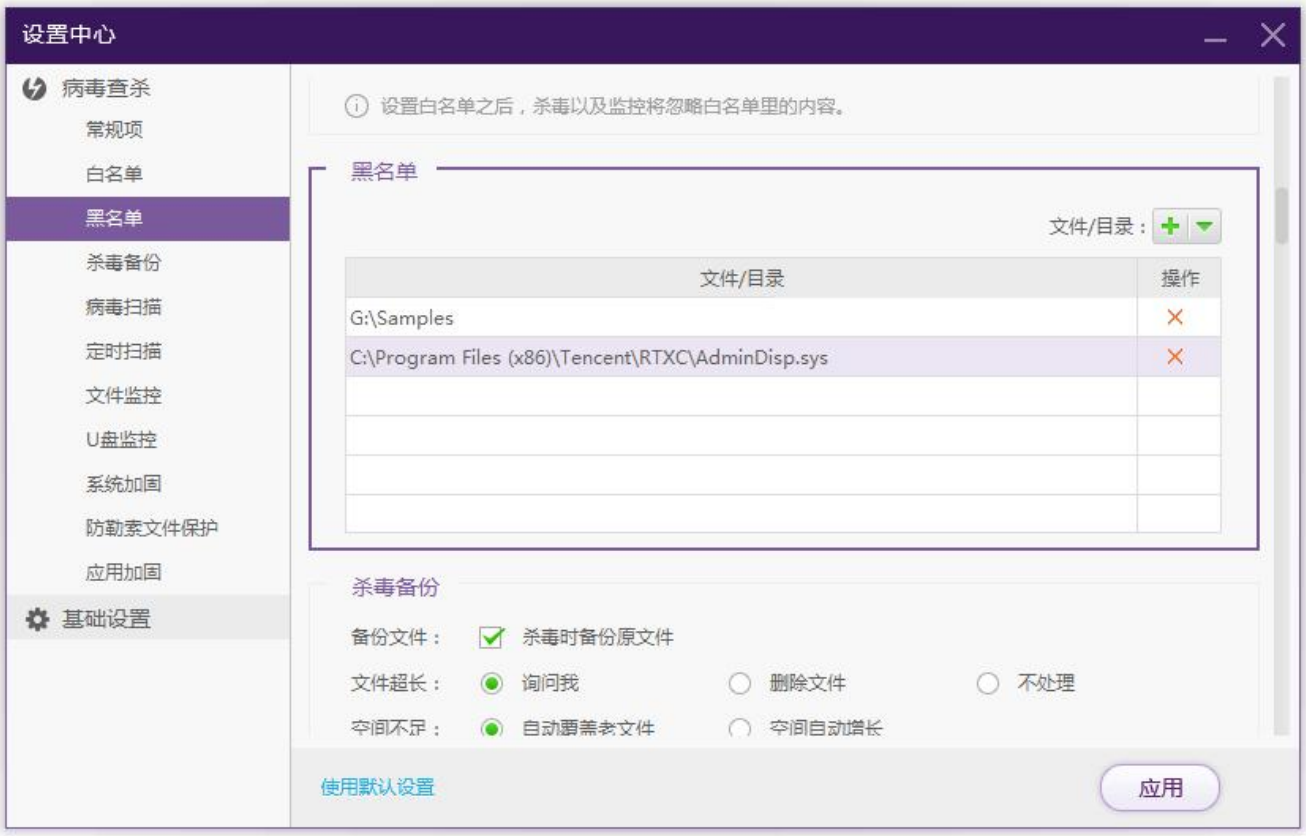
点击【病毒查杀】>【白名单】，然后在文件后缀一栏点击图标【+】，下方的表格中将添加一行，输入需要加入白名单文件的后缀名，如图所示。



如果要从白名单中删除，点击“操作”一栏中的删除【X】。设置完成后，点击右下角【应用】，保存设置。

5.6.1.3 黑名单

点击【病毒查杀】>【黑名单】，然后在文件/目录一栏点击图标【+】，弹出选择窗口，选择需要加入黑名单的文件或者目录，如图所示。



在菜单中，可以通过四种方式设置文件和目录，分别是：

目录+子目录：设置后，软件每次扫描都会扫描该目录及其子目录。

目录：扫描时，软件都会扫描所选目录中的文件，而忽略其子目录中。

子目录：扫描时，软件只扫描所选目录的子目录。

文件：扫描时，软件每次都扫描所选的文件。

文件名：扫描时，所有符合设定文件名的文件都将扫描。

进程名：扫描时，符合设定进程名的将被扫描。

如果需要将已经加入黑名单的文件/目录删除，请点击表中“操作”一栏的删除【X】。

设置完成后，点击右下角【应用】，保存设置。

5.6.1.4 杀毒备份

杀毒备份对应于病毒隔离区，杀毒软件进行病毒查杀的时候，会把病毒和被病毒感染的文件移至隔离区。通过杀毒备份，设置不同情形下的病毒文件处理方式。既可以有效防止继续感染其他文件，又可以保留被病毒感染的文件。

点击【病毒查杀】>【杀毒备份】，进入病毒备份设置，如图所示。

杀毒备份设置项如下：

备份文件：勾选【杀毒时备份原文件】，即可将病毒文件备份到隔离区，供以后使用。

文件超长：查杀时，文件很大，可以设置询问、直接删除、不处理。

空间不足：当隔离区备份的文件过多，导致隔离区空间不够时，空间的处理方式可以自动覆盖老文件，或者空间自动增长。用户根据具体环境进行选择。

备份失败：当备份病毒文件失败时，可以设置询问我、删除文件和不处理的方式。用户根据具体环境进行选择。

所有设置项设置完成后，点击右下角【应用】，保存设置。

5.6.1.5 病毒扫描

病毒扫描可以设置扫描文件类型、查杀引擎的选择等。

点击【病毒查杀】>【病毒扫描】，进入病毒扫描设置，如图所示。

文件类型：杀毒软件需要在查杀时扫描的文件类型，默认为所有文件，也可以选择程序和文档。

查杀引擎：杀毒软件带有 4 个查杀引擎，分别针对不同类型的病毒和安全威胁。勾选“仅查杀流行病毒”，会重点查杀最近比较活跃的病毒；勾选“启发式查杀”，可以有效的对可疑的文件查杀；勾选“启动压缩包查杀”，并设置好压缩包的容量，查杀时可以解开限定容量的压缩包进行查杀。

发现病毒：发现病毒的处理方式，可选自动或者手动。自动方式无需用户确认，自行清除病毒文件；手动处理方式，需要用户确认是保留还是删除病毒文件。不处理，只显示扫描结果，不做任何操作。

清除失败：当病毒清除失败时，设置为直接处理或者不处理。

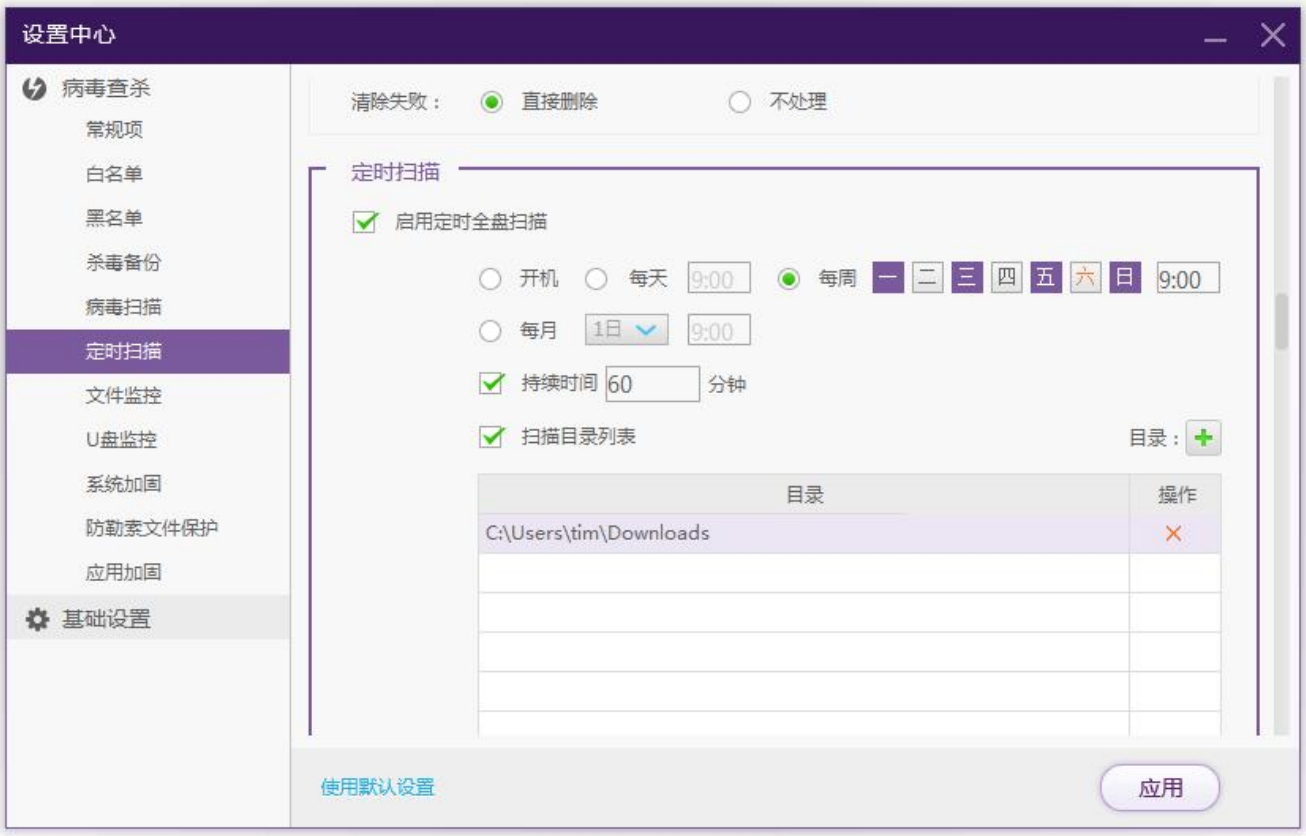
所有设置项设置完成后，点击右下角【应用】，保存设置。

5.6.1.6 定时扫描

定时扫描可以设置特定日期和时间进行病毒扫描。定时扫描可设置全盘定时扫描和快速定时扫描。

a．定时全盘扫描

点击【病毒查杀】>【定时扫描】，进入全盘定时扫描设置，如图所示。



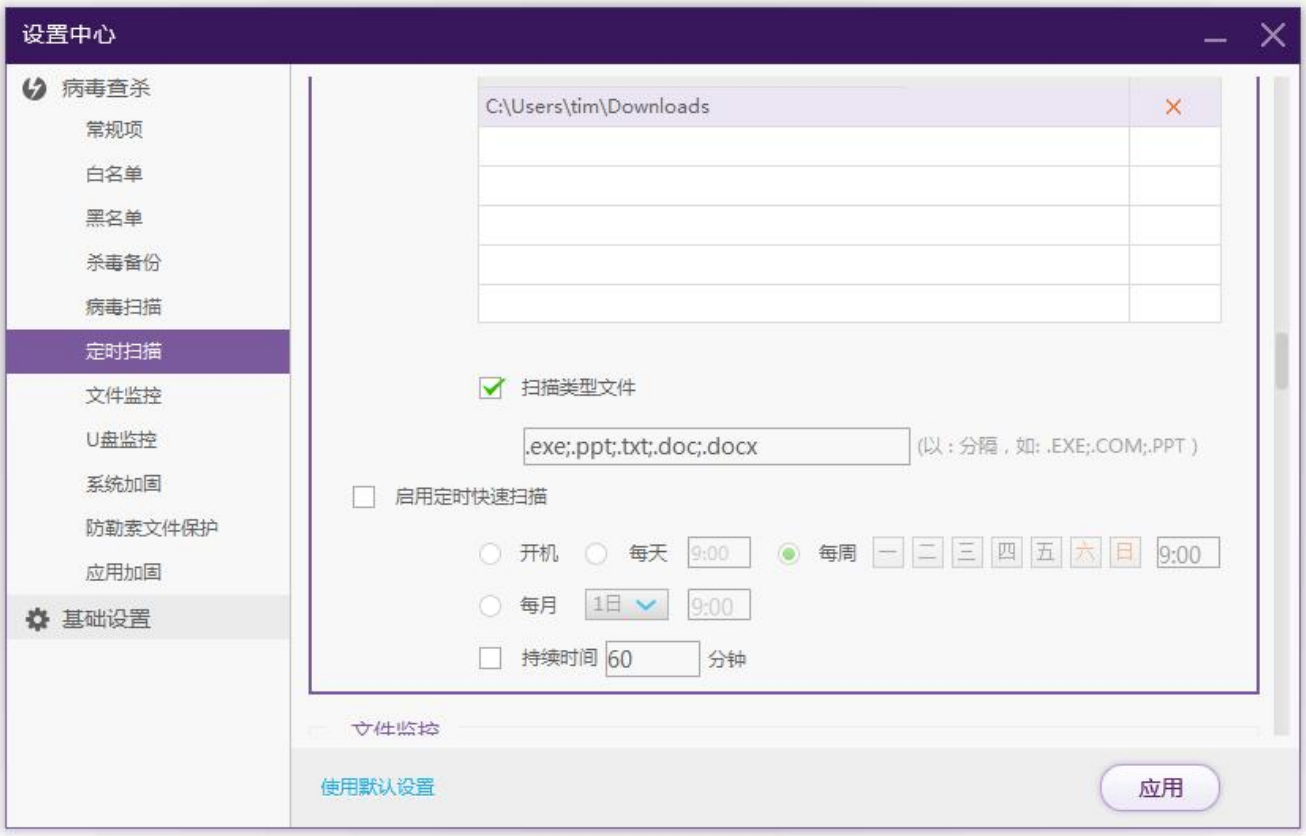
启用对全盘扫描：勾选后，启用请示全盘扫描功能。

设置定时模式，开机扫描、每天定时扫描、每周定时扫描、每月定期定时扫描。如图中所示为每周一，三，五，日 9:00 定时扫描。

持续时间：持续到设置的时间结束扫描，如设置为 60 分钟，则超过 60 分钟自动停止扫描。

扫描目录列表：勾选后，才能设置扫描指定目录列表，点击【+】添加需要定时扫描的目录。

扫描类型文件：勾选后，可以设置定时扫描的文件类型，如.EXE;.COM 等。

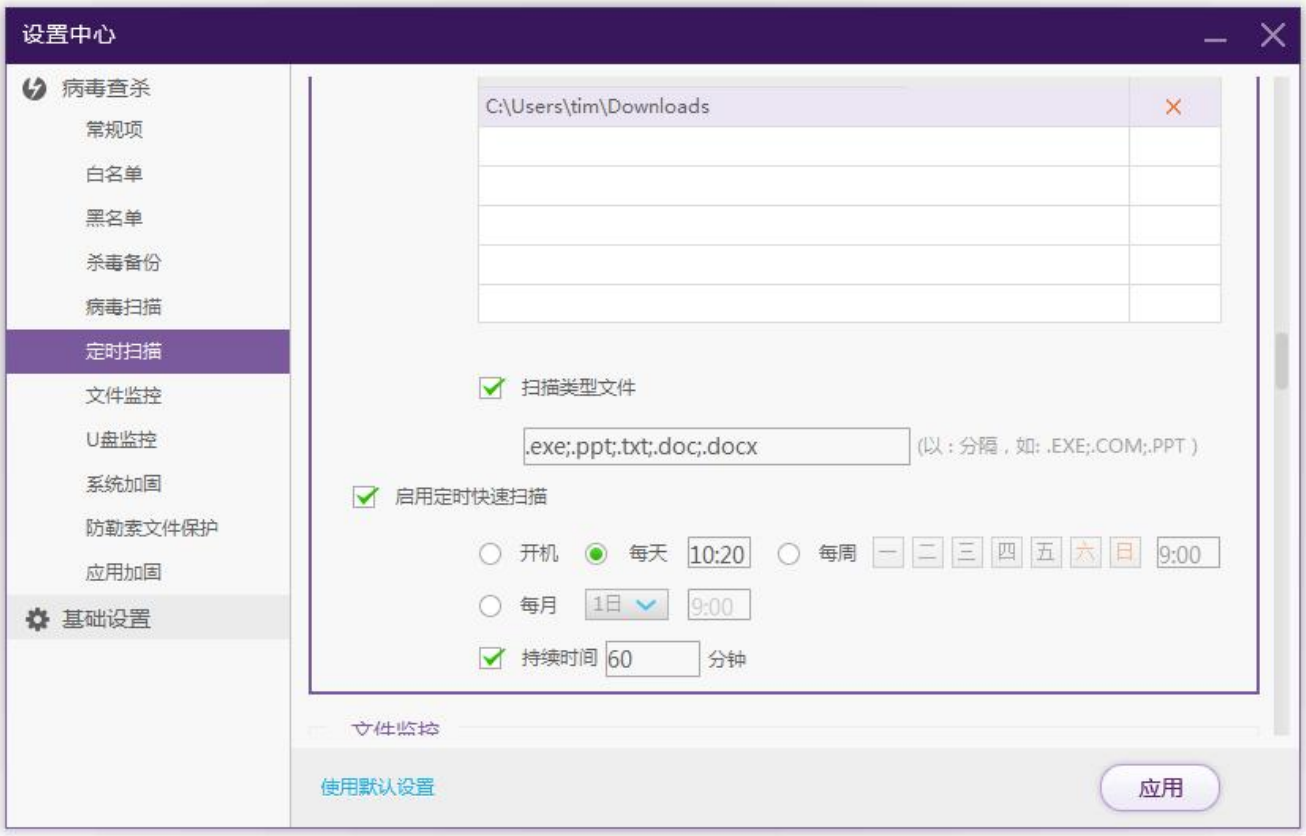


b．定时快速扫描

启用定时快速扫描：勾选后，可以设置定时快速扫描，和定时全盘扫描的区别是，定时快速扫描速度更快，只扫描系统关键区域的文件和目录。

设置定时快速扫描的模式：开机扫描、每天定时扫描、每周定时扫描、每月定期定时扫描。如图中所示为每天 10:20 定时快速扫描。

持续时间：持续到设置的时间结束扫描，如设置为 60 分钟，则超过 60 分钟自动停止扫描。



所有设置项设置完成后，点击右下角【应用】，保存设置。

5.6.1.7 文件监控

文件监控能对终端的读写、文件、程序进行实时保护，一旦发现可疑文件和可疑操作立即拦截。

点击【病毒查杀】>【文件监控】，进入文件监控设置，如图所示。

文件监控设置项如下：

文件监控：勾选【开机启用】，则文件监控功能随客户端开机启动，实时监控扫描病毒和木马。

智能黑名单：勾选【开启】，黑名单生效。

监控设置：勾选【开启内核监控】，内核监控功能生效。

监控模式：文件监控模式，分为极速、标准、专业和增强。每一种模式适用于不同的场景和环境。

⑤ 极速模式，可快速的监控常见文件和程序，监控使用的资源低，不会影响用户正常使用电脑；

⑥ 标准模式，一般采用的模式，兼顾速度和监控效率，能够监控到大部分的威胁和病毒爆发；

⑦ 专业模式，为用户特殊需求设计，能够针对性的监控文件，如对 word 等 office 文档的增强监控，可以有效的降低宏病毒的影响。可以自定义文档类型，诸如 CFG;DAT；BIN 等 Windows 常见文件的增强监控。能有效拦截恶意脚本恶意配置文件。

⑧ 增强模式，为用户提供最全面的监控，对系统内所有文件和程序类型提供强力监控，缺点是占用系统资源相当高，可能会影响用户使用体验。

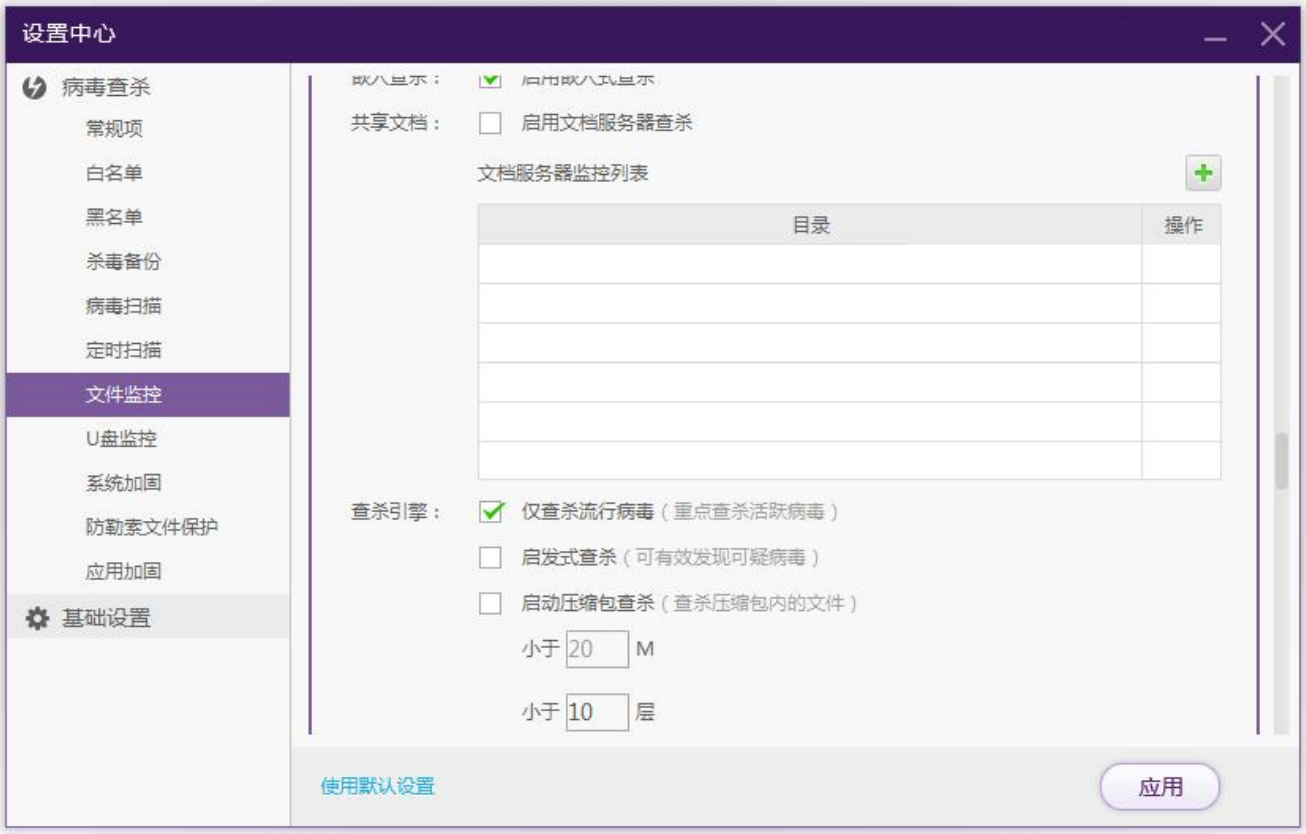
文件类型：可以选择【所有文件】或者【程序和文档】或者【指定文件类型】。

监控加速：勾选【信任程序分析】，监控加速功能生效。

驱动缓存：勾选【不使用驱动缓存】后，策略变动时重置驱动缓存。经常性变动策略时，勾选此项，可以加快策略的生效速度。使用驱动缓存能够加快查杀的速度，不使用驱动缓存，每次查杀都会重新扫描已经

扫描过的文件。

嵌入查杀：勾选【启用嵌入式查杀】，嵌入式查杀功能生效。



共享文档：勾选【启用文档服务器查杀】，能专门查杀共享文档，防止通过共享文档传播病毒。点击【+】，添加需要监控的文档服务地址或者目录。

查杀引擎：勾选【仅查杀流行病毒】，即对活跃病毒进行重点的查杀；勾选【启发式查杀】，即将所有的可疑文件都列入查杀范围；勾选【启动压缩包查杀】，即可以查杀压缩包内的文件，同时对压缩包的大小和曾经可以进行限定。

发现病毒：选择发现病毒时的处理方式，可选择【自动处理】，如需手动处理，则选择【手动处理】。

清除失败：当病毒清除失败时，可选直接处理或者不处理。

报告结果：勾选后开启功能，病毒清除成功后通知用户。

行为规则：勾选【启用】后，开启内置的规则。也可以自行定义规则。点击【+】，可以查看行为规则的具体内容，进行修改，删除等操作。

下方的【触发规则时通知用户】，在规则触发时，会在客户端弹窗提示。【记录拦截日志】会记录拦截日志。如图为触发规则时的弹窗。

所有设置项设置完成后，点击右下角【应用】，保存设置。

5.6.1.8 U 盘监控

U 盘监控，对 U 盘进行防护，能有效的防止病毒从 U 盘感染计算机。

点击【病毒查杀】>【U 盘监控】，进入 U 盘监控设置，如图所示。

插入 U 盘时：设置插入优盘时的操作，选择【询问是否查杀】或者【立即查杀】。

查杀深度：可以设置对 U 盘文件的查杀递归层次，数字设置越大，能查杀的目录层次越深，查杀的文件越多。

所有设置项设置完成后，点击右下角【应用】，保存设置。

5.6.1.9 系统加固

应用主动防御技术，对系统的重要文件、文件关联、系统注册和服务进行加固防护，保护系统安全，可以阻止篡改系统注册表和替换文件关联等行为。

点击【病毒查杀】>【系统加固】，进入系统加固设置，如图所示。

发现威胁：【自动处理】，发现威胁后，软件自行处理；【通知我】，发现威胁及时通知用户选择处理方式。

拦截日志：勾选【记录拦截日志】，则在日志中心产生日志记录，去掉勾选则不生成日志。

监控灵敏度：分为【低】、【中】、【高】，灵敏度越高，需要消耗更多的系统资源，推荐选择【中】。

审计模式：勾选【开启】后，审计模式生效，对所有触犯规则的动作都做放行处理。

其他：勾选【放过带数字签名的程序】，对系统中已经获得安全数字签名认证的程序一律放行。

行为规则：勾选启用规则后，才能启用系统加固-行为规则，说明：开启了系统加固此处规则才能生效!

点击【+】进入系统加固行为规则设置。

触发规则时通知用户：勾选后，能够收到触发行为规则的通知。

记录拦截日志：勾选后，记录触发行为规则的拦截记录，在规则列表中，可以通过下拉进度条进行翻阅。

规则列表中，可以点击【删除】删除对应的规则。通过勾选规则前的复选框，选中规则生效，未选中的规则则无效。

点击右侧的【添加】按钮，可以添加新的规则。如图所示。

已经存在的规则，可以通过鼠标点击输入，直接进行修改。

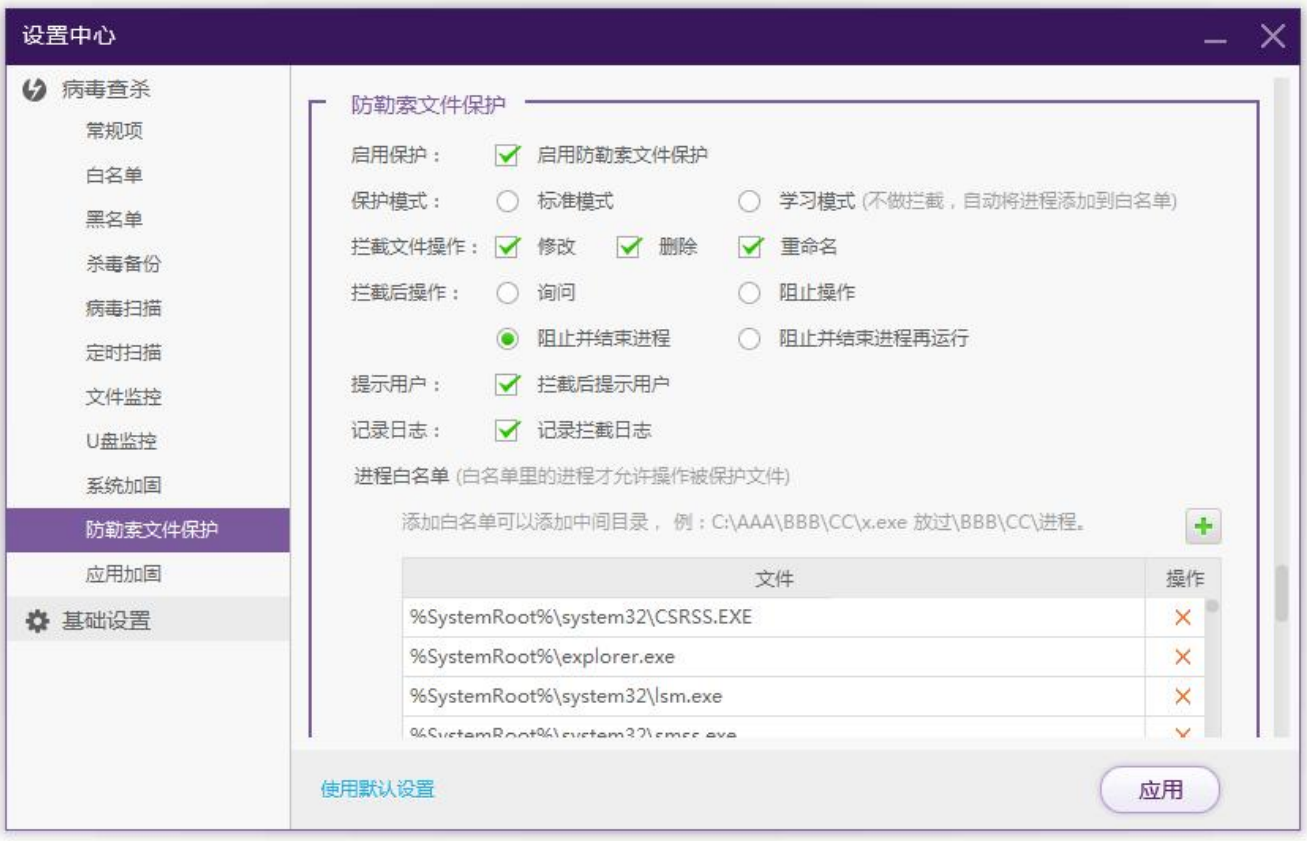
说明：该规则是高级定制功能，请不要随意修改。如有需要请联系管理员定制化修改！

所有设置项设置完成后，点击右下角【应用】，保存设置。

5.6.1.10 防勒索文件保护

防勒索文件保护用于防加密类勒索病毒感染文档、文件，能有效的防御诸如永恒之蓝的病毒。开启功能后，防勒索功能才能工作。开启步骤如下：

点击【病毒查杀】>【防勒索文件保护】，进入防勒索文件保护设置，如图所示。



启用保护：勾选【启用勒索文件保护】，启用功能。

保护模式：分标准模式和学习模式。标准模式：启用标准模式后，软件将拦截勒索病毒及勒索行为；学习模式：当用户自主选择某些行为不是勒索病毒行为时，将自动添加进程到白名单，以后将不再拦截该进程，使用时间越长，学习模式越智能。

拦截文件操作：至拦截到有文件中勒索病毒后，可对文件进行的操作，包括修改、删除和重命名。用户根据实际需求勾选。

拦截后操作：默认是询问用户，也可以设置为阻止操作、阻止并结束进程和阻止并结束进程再运行中的一种。

提示用户：勾选【拦截后提示用户】，当有勒索病毒被拦截时，弹出通知客户端用户。

记录日志：勾选【记录拦截日志】后，将开始记录所有的拦截日记，便于后期分析。建议勾选。

进程白名单：为了更为有效的保护文档，可以设置白名单模式。只有在白名单中的进程才能够操作被保

护的文件。点击【+】，添加白名单进程，填写进程路径，点击【应用】。

列表中已经内置了许多白名单进程，这些都是常用的软件进程，不要随意删除，否则会导致正常软件无法操作保护文档。

除了可以设置白名单进程，我们还需要设置受保护的文件。

文件的保护模式有两种，一种是包含目标文件，另一种是排除目标文件。跟进实际需求，选择。然后点击【+】添加需要保护（排除）的文件和目录。

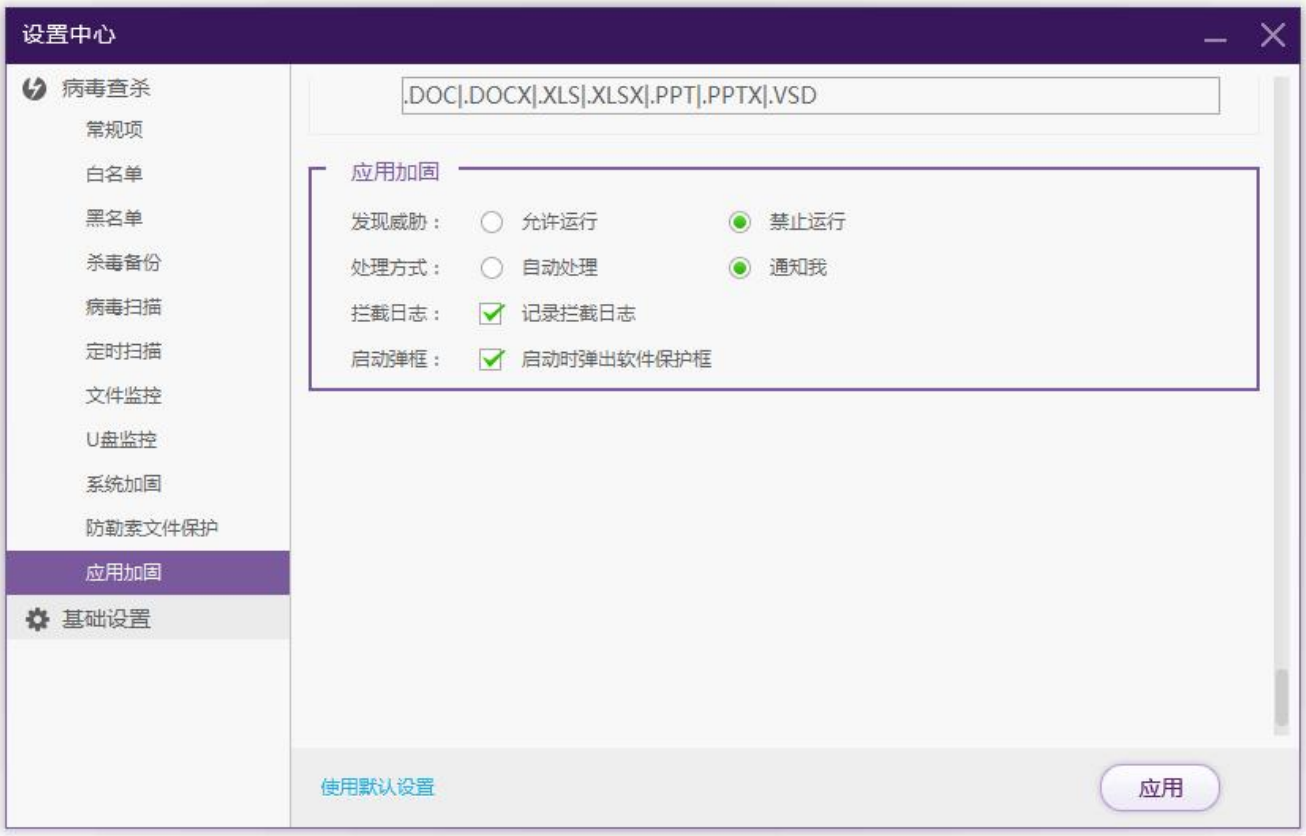
在下方的文件后缀中，可以设置多种文件后缀，所有包含（排除）后缀的文件都会被列入保护。只有白名单进程才能操作。

设置完成后，点击【应用】。

5.6.1.11 应用加固

当对系统安装的应用进行加固，防止病毒或木马对系统上的应用进行破坏，或者是阻止木马盗取系统应用数据。

点击【病毒查杀】>【应用加固】，进入应用加固设置，如图所示。



可设置项包括：

发现威胁：选择【允许运行】，是继续让威胁应用运行，选择【禁止运行】，让威胁应用立即停止运行。

处理方式：发现威胁后通知用户的方式，要么选【自动处理】，即不通知；要么选【通知我】，即以弹窗的形式提醒用户威胁。

拦截日志：勾选【记录拦截日志】后，在日志中心将产生应用加固的日志信息。否则没有应用加固拦截日志。

启动弹框：勾选【启动时弹出软件保护框】，在计算机启动时弹出软件对计算机的保护信息。

所有设置项设置完成后，点击右下角【应用】，保存设置。

5.6.2 基础设置

基础设置主要是账户和托盘以及软件更新方面的设置。

5.6.2.1 管理员身份

【管理员身份】，这里可以修改管理员密码，一般由系统管理员在操作客户端时，需要修改密码时用到。普通用户略过。注意其中的提示：此密码为管理员唯一身份标识，特殊操作时所用，密码锁定后不可修改。

点击【设置一个】，开始设置管理员密码。

5.6.2.2 托盘设置

【托盘设置】，勾选【隐藏任务栏托盘图标】之后，在任务栏将不显示客户端的图标。

5.6.2.3 软件更新

升级模式：设置软件更新的模式，可选模式包括手动升级、每天、每周，其中可设置每天的更新时间或者是每周的某天更新，还可以设置为间隔一定时间更新，如每隔 12 小时更新一次。

延时启动：为软件更新设置延时，可选择项分别为禁用、自动和延时，延时时间可以自行设置。

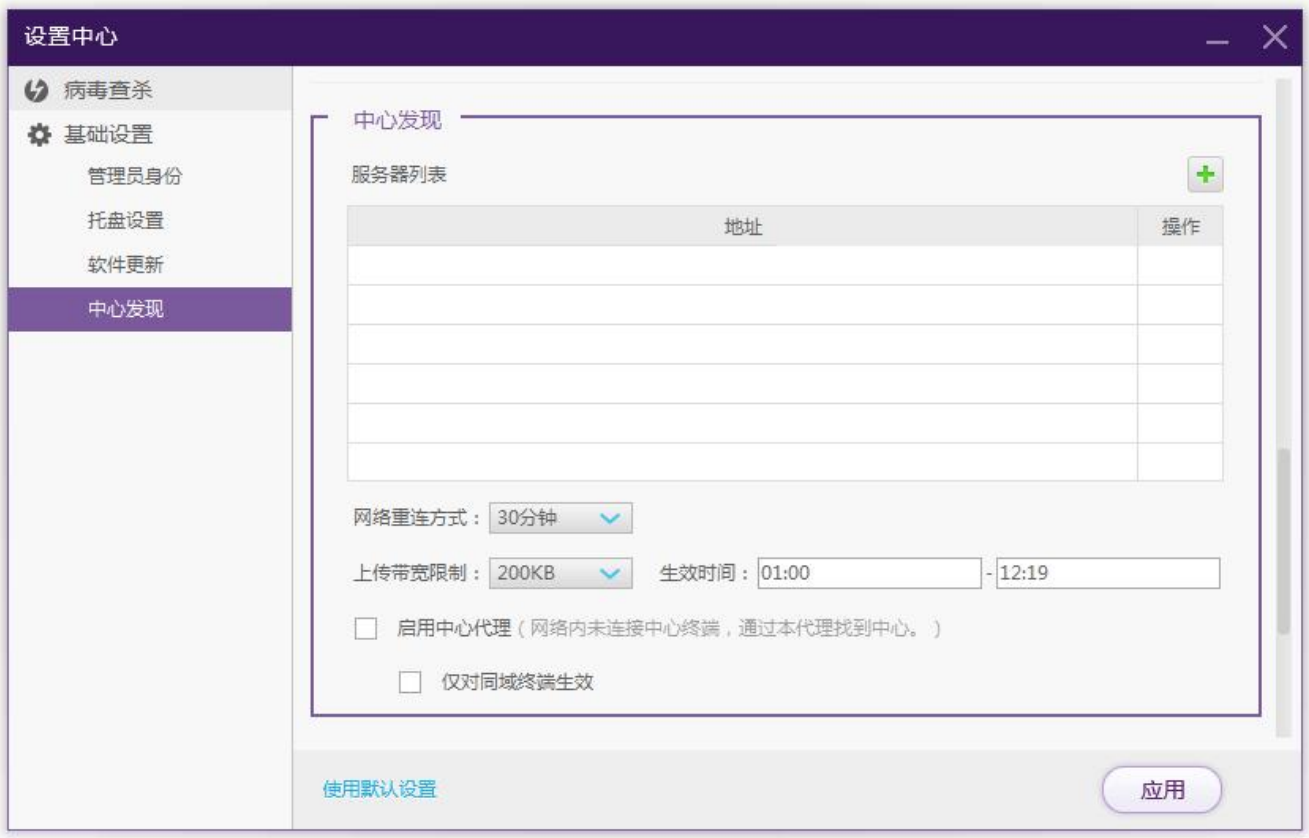
升级内容：升级所有组件、仅升级病毒库、实时检查病毒库新版本；

代理设置：和普通代理类设置类似，填写地址、端口、账号、密码；

升级源：升级源用于设置升级中心的地址，可以勾选瑞星官网的升级源，或者是自定义第三方升级源。点击【增加其他升级中心】，然后在列表中输入其他升级中心的地址。删除时请点击操作中的【X】删除。设置完毕点击【应用】。

5.6.2.4 中心发现

中心发现新增了中心的多 IP 模式，可以添加多个中心服务器的 IP 地址，提高中心的可用性。在某个中心无法连接时，客户端将尝试列表中的 IP，直到找到一个能连接的 IP 为止。中心 IP 地址由管理员在中心设置。



网络重连方式：客户端可以设置中心重连的时间间隔，可以选实时连接，或者 5 分钟。如图所示。

上传带宽限制：设置客户端上传数据的带宽限制，还可以定制该限制的生效时间。这样可以避免上传数据时影响客户端用户的体验。

启用中心代理：网络内心的终端（未连接中心）可以将本终端作为代理连接到中心，前提是本终端能连

接到中心。

仅对同域生效：勾选后，只能作为本域内的代理客户端。域外的客户端不能将该终端作为代理。去掉勾选后，域外用户也可将本终端作为代理。

5.7 日志中心

杀毒日志功能可以让用户查看病毒详情、扫描事件、系统加固和应用加固的详细信息以及处理结果等。

在主界面点击  进入杀毒日志界面。

5.7.1 病毒查杀

病毒查杀日志记录了病毒详情、扫描时间、系统加固日志、应用加固日志、隔离区日志。

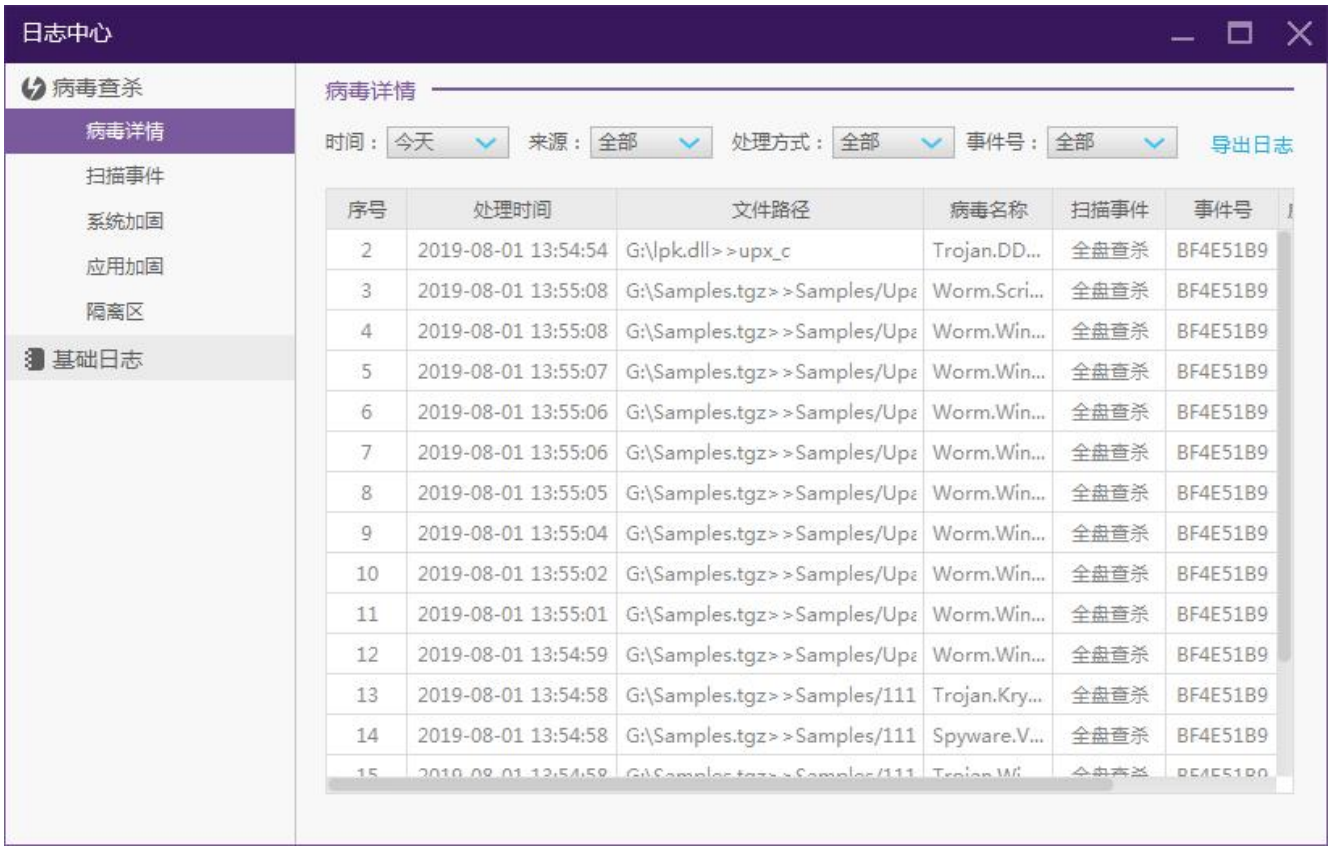
5.7.1.1 病毒详情

在病毒详情页面，用户可以查看到杀毒软件扫描或者监控到的所有病毒信息，包括扫描或监控到的时间、

文件路径、病毒名称、威胁类型和状态等。

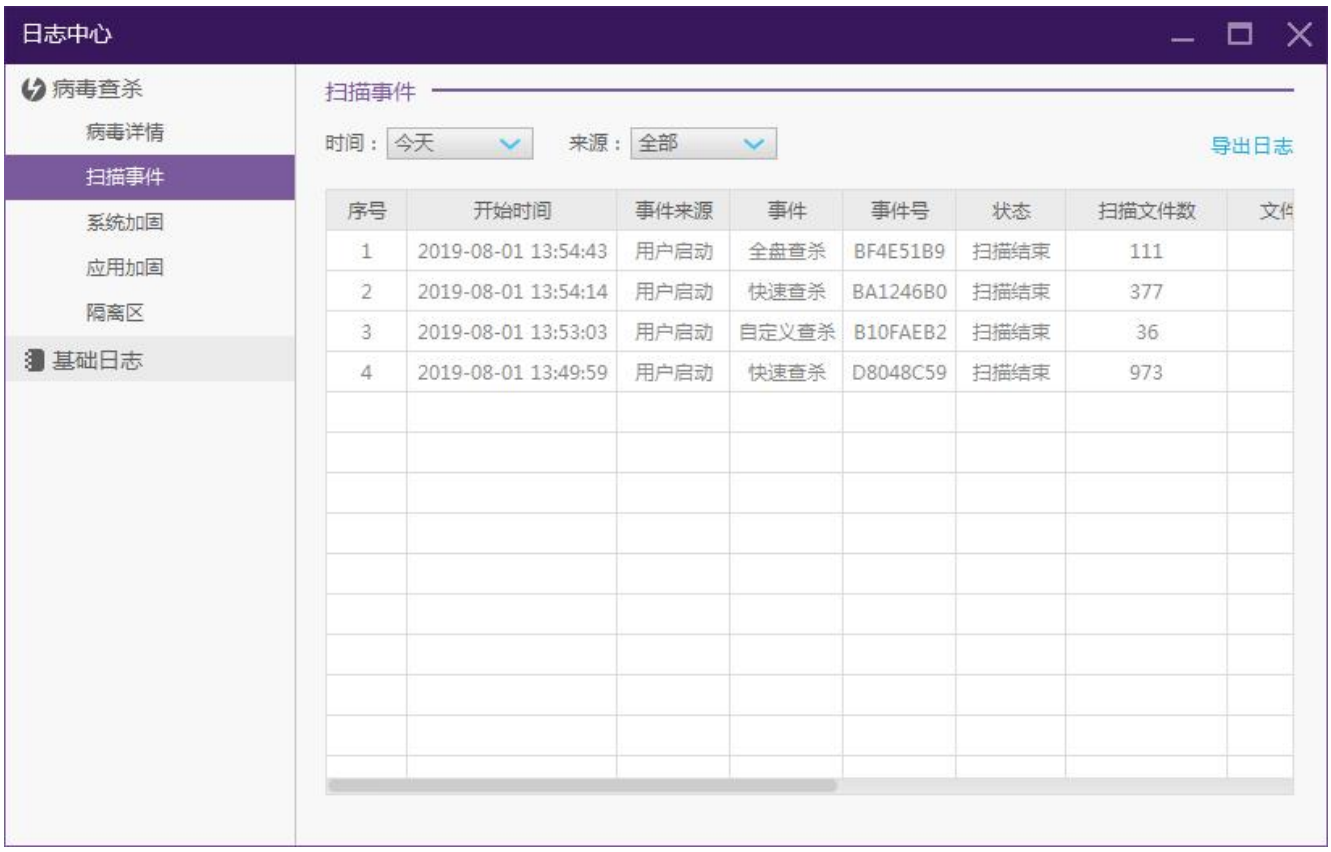
可以按时间、来源和处理方式对扫描或监控到的病毒进行筛选。按时间筛选分为全部、今天、最近三天、最近一周和最近一个月。按来源筛选分为全部、快速查杀、全盘查杀、自定义查杀、文件监控。按处理方式筛选分为全部、暂未处理、忽略、删除、清除、信任和备份失败。

可以点击页面右上角的【导出日志】将日志记录导出为 csv 文件。



5.7.1.2 扫描事件

点击【扫描事件】，进入扫描事件页面，本页面记录了杀毒软件的扫描记录。

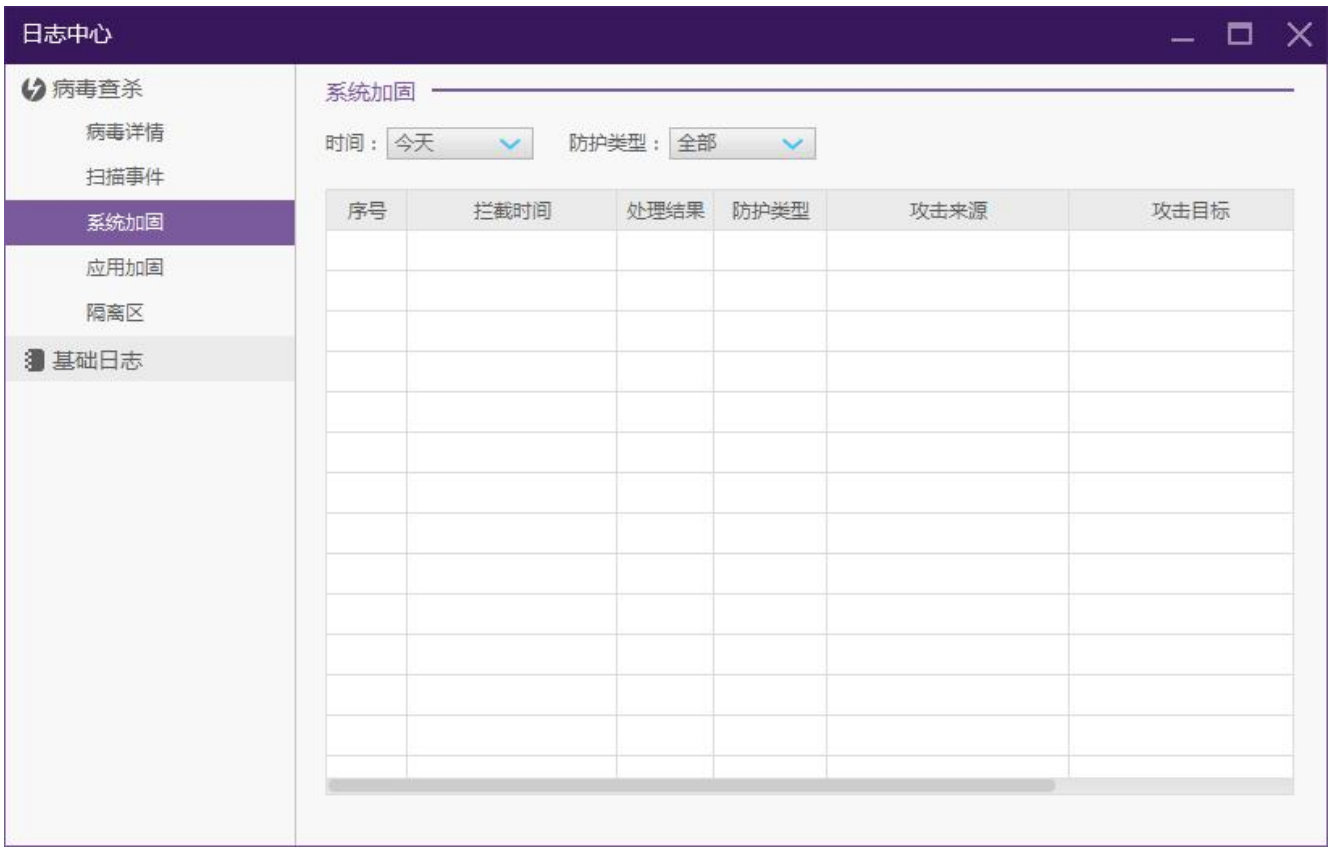


在扫描事件页面详细的记录了包括开始时间、事件来源、扫描事件、扫描状态、扫描对象、发现威胁和已处理等。可以按时间和来源对记录进行筛选。按时间筛选分为全部、今天、最近三天、最近一周和最近一个月。按发现源筛选分为全部、快速查杀、全盘查杀、自定义查杀。

可以点击页面右上角的【导出日志】将日志记录导出为 csv 文件。

5.7.1.3 系统加固

点击【系统加固】，进入系统加固页面，本页面记录了系统防护的相关事件

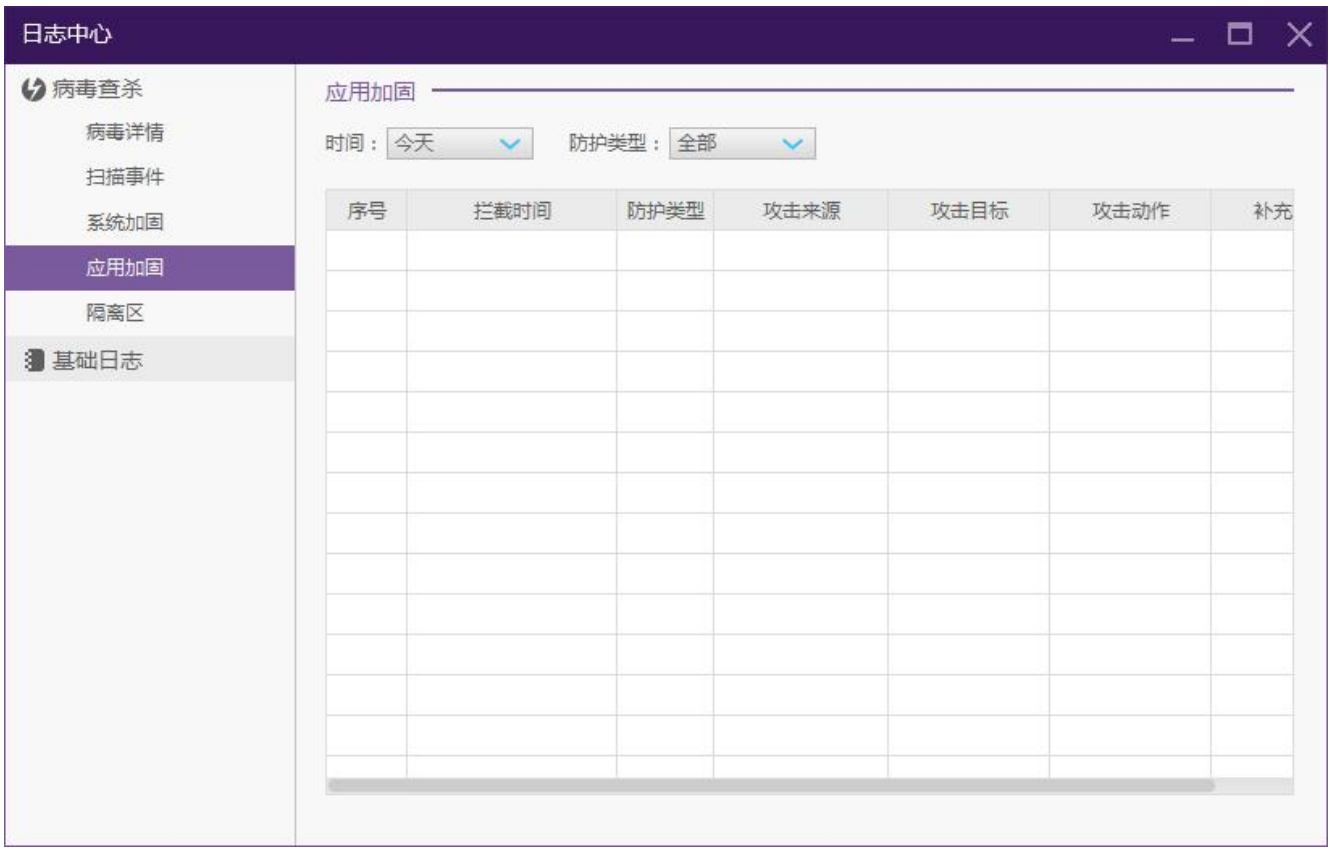


在系统加固页面详细的记录了包括时间、处理结果、事件、来源和目标等。可以按时间和防护类型进行筛选。按时间筛选分为全部、今天、最近三天、最近一周和最近一个月。按防护类型筛选分为全部、文件防护、注册表防护、进程防护和系统防护。

可以点击页面右上角的【导出日志】将日志记录导出为 csv 文件。

5.7.1.4 应用加固

点击【应用加固】，进入应用加固页面，本页面记录了常用应用程序防护的相关事件



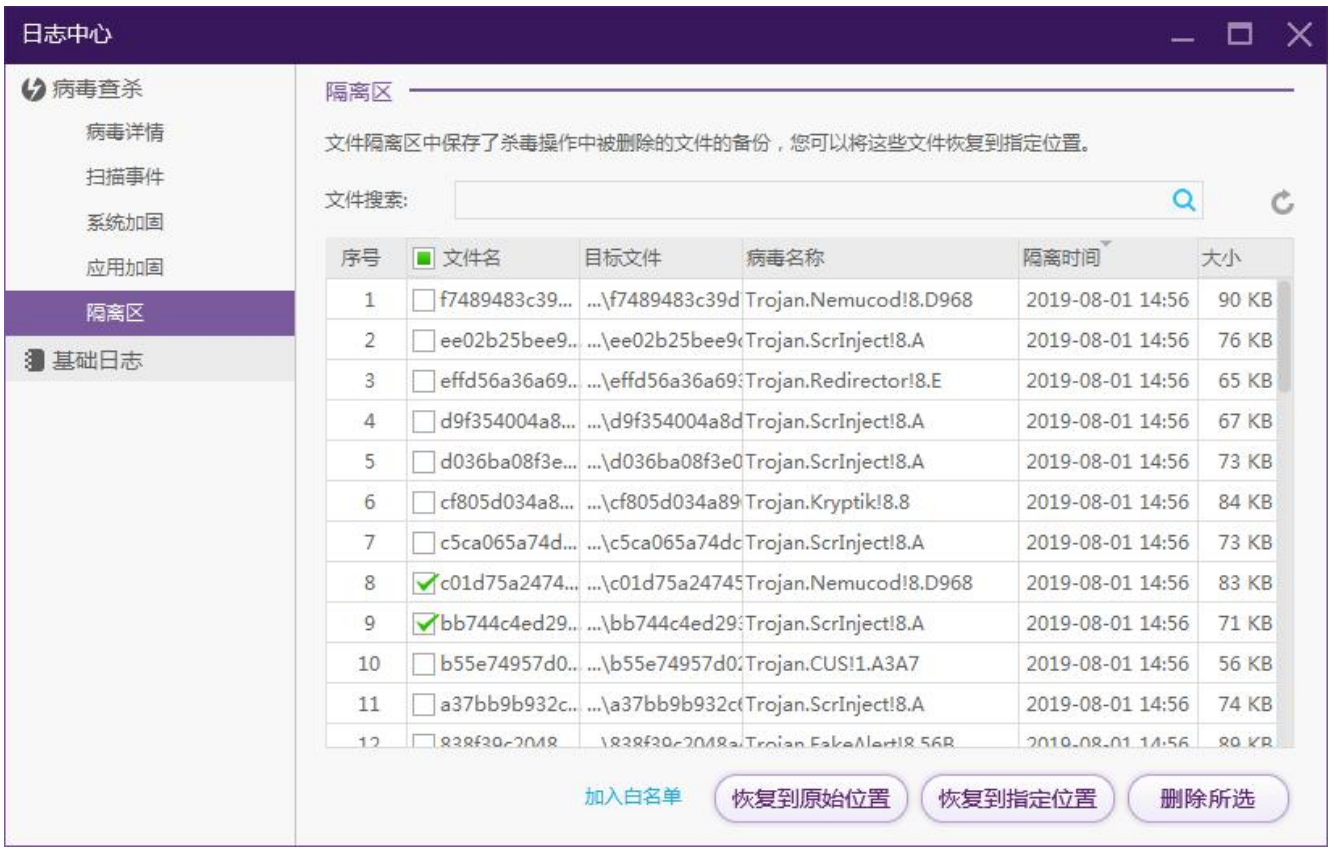
在应用加固页面详细的记录了包括时间、程序类型、来源、操作、目标和补充信息等。可以按时间和应用类型进行筛选。按时间筛选分为全部、今天、最近三天、最近一周和最近一个月。按应用类型筛选分为全部、浏览器和办公软件。

可以点击页面右上角的【导出日志】将日志记录导出为 csv 文件。

5.7.1.5 隔离区

点击【隔离区】，进入隔离区页面，文件隔离区中保存了杀毒操作中被删除的文件备份。

勾选隔离区的文件，下方的操作按钮变亮，可以将文件【恢复到原始位置】、【恢复到指定位置】、【删除所选】和【加入白名单】。恢复到原始位置，是将病毒文件恢复初始位置；恢复到指定位置，用户可以将他恢复任意位置；删除所选，选择要删除的病毒文件，进行删除，并且不可恢复。



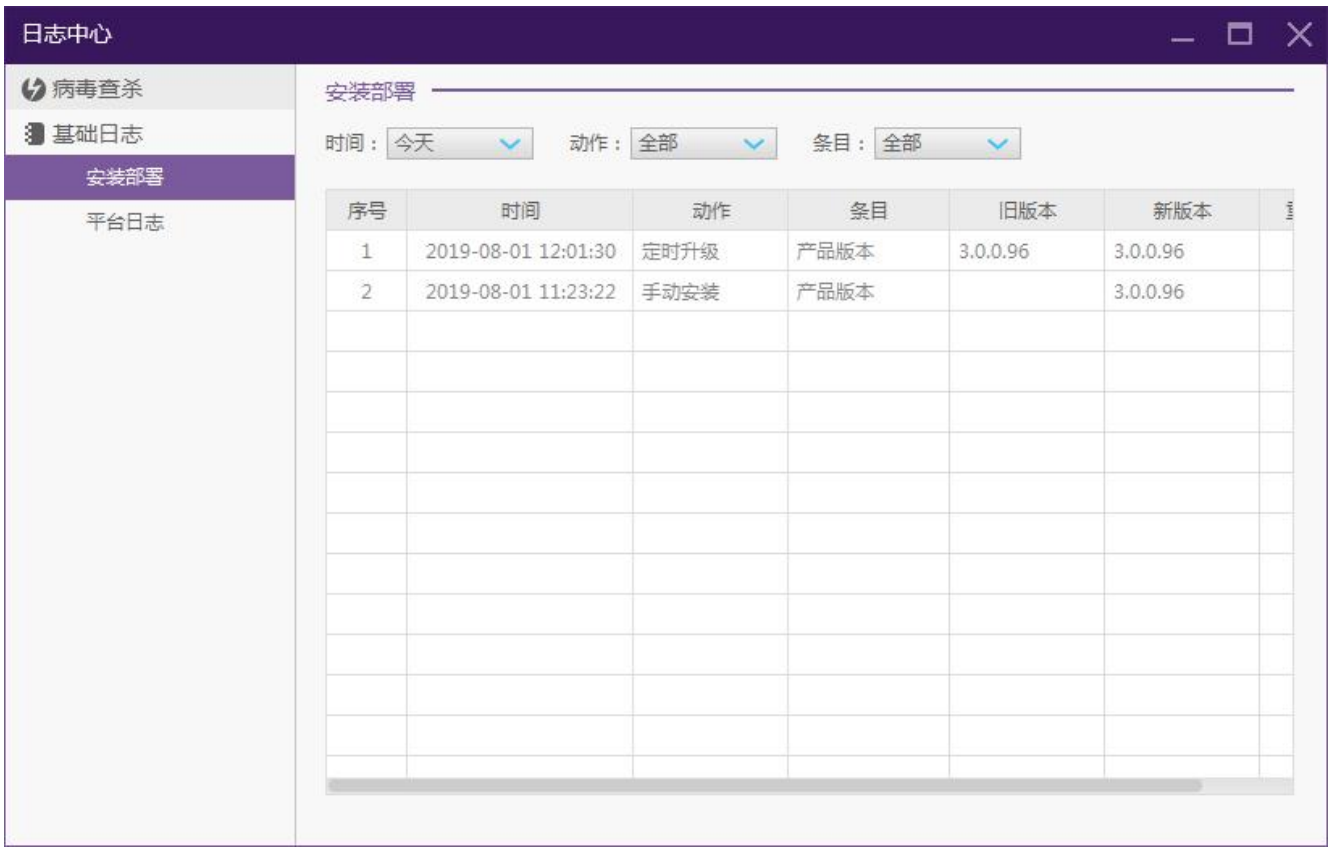
在隔离区页面详细的记录了病毒文件的文件名、目标文件、病毒名称、隔离时间和大小。在文件搜索框中可以对文件名进行搜索。

5.7.2 基础日志

点击【基础日志】，可以查看安装部署的日志，还可以查看平台日志。

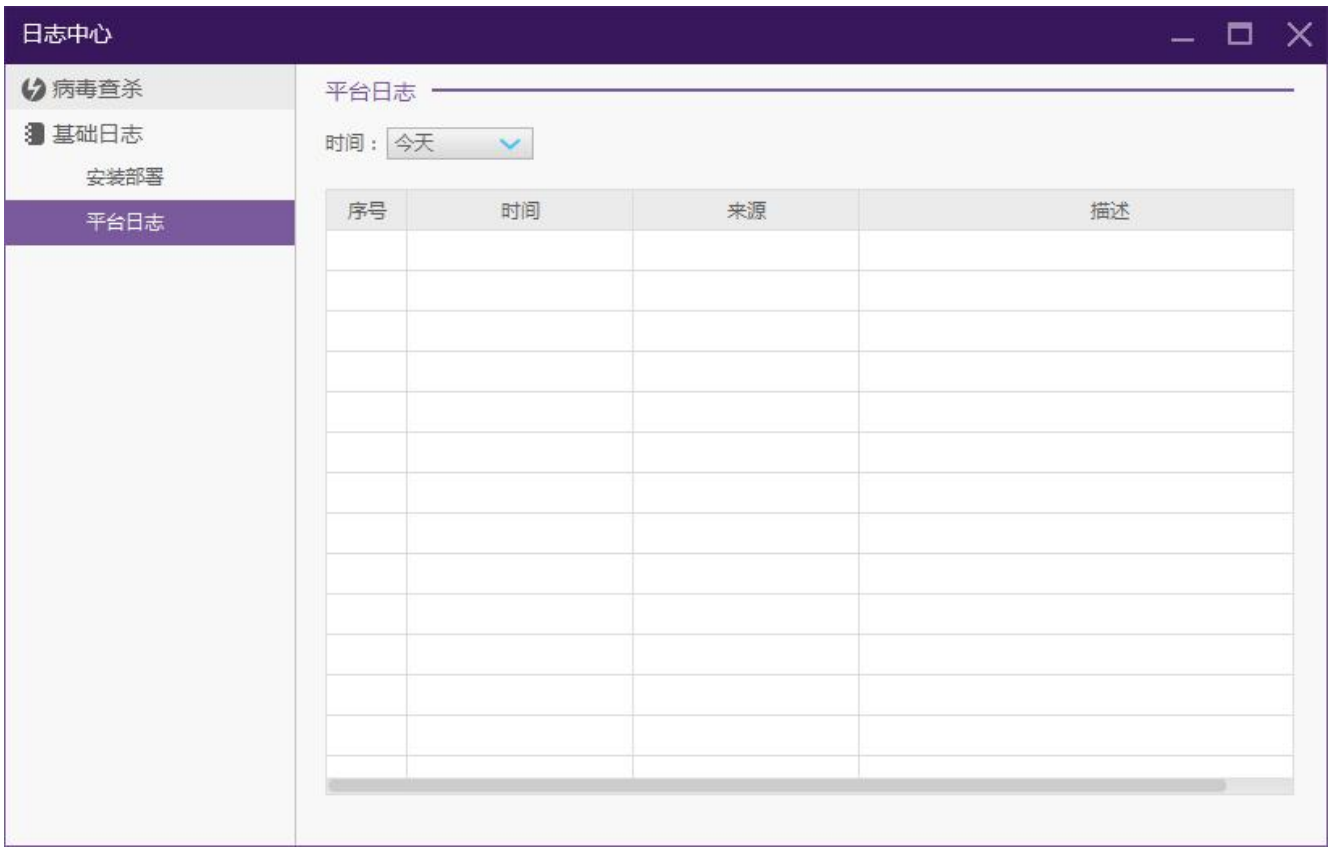
5.7.2.1 安装部署

通过安装部署日志，可以查询安装软件、插件的时间、动作、条目、旧版本、新版本和重启标识等。如，在动作中可以看到，安装是通过定时升级、手动还有远程修复等方式实现。



5.7.2.2 平台日志

平台日志则可以查询登录管理平台的相关日志信息。包括登录的时间、来源和描述。通过平台日志，能够及时发现异常登录。



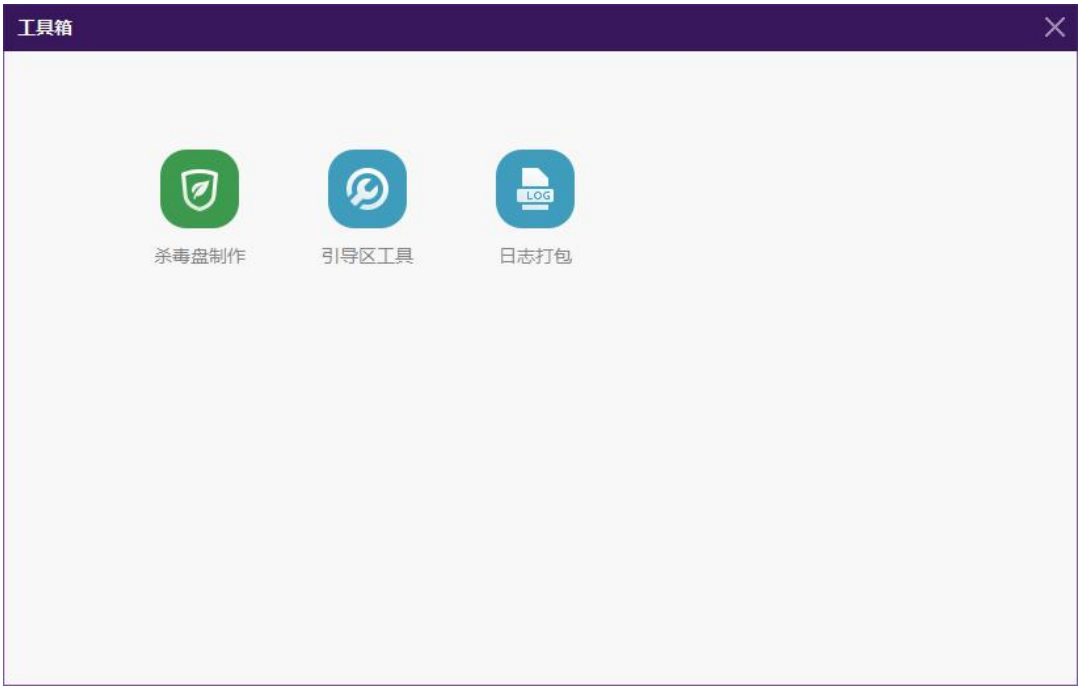
平台日志记录了登录中心的时间和描述，能及时了解登录中心的账户情况。

5.8工具

瑞星 ESM 365 的客户端工具提供了日志打包和 U 盘工具，用于故障应急提取日志。

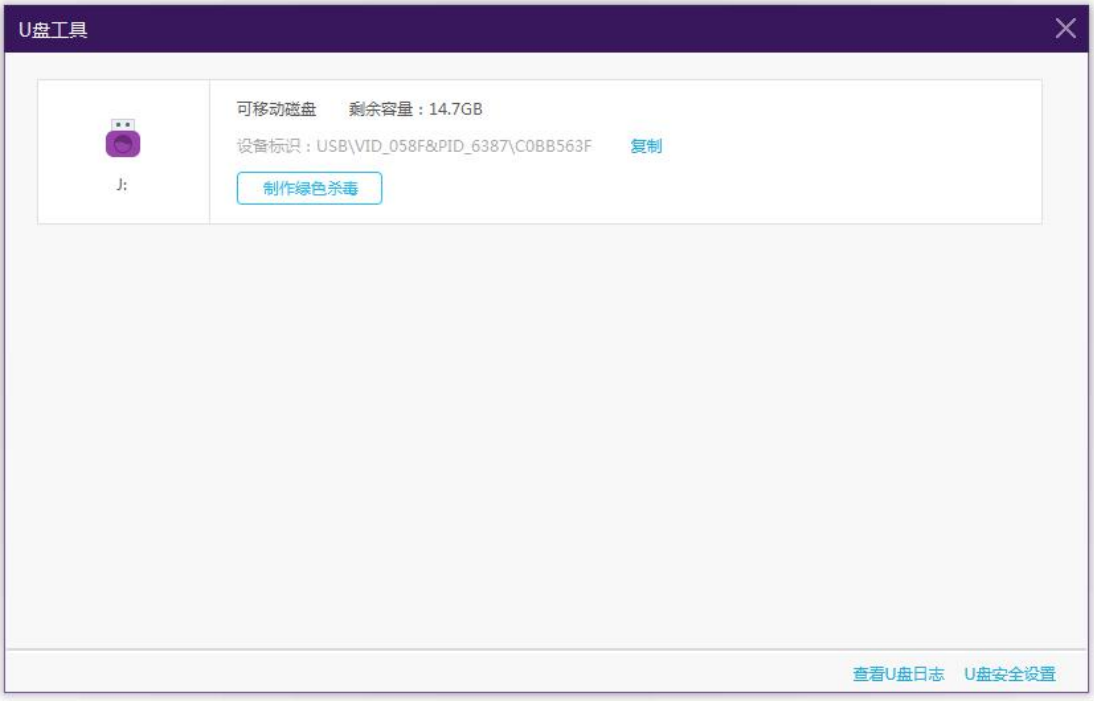
点击如图红框所示按钮，进入工具区域。

进入工具箱界面后如图所示。



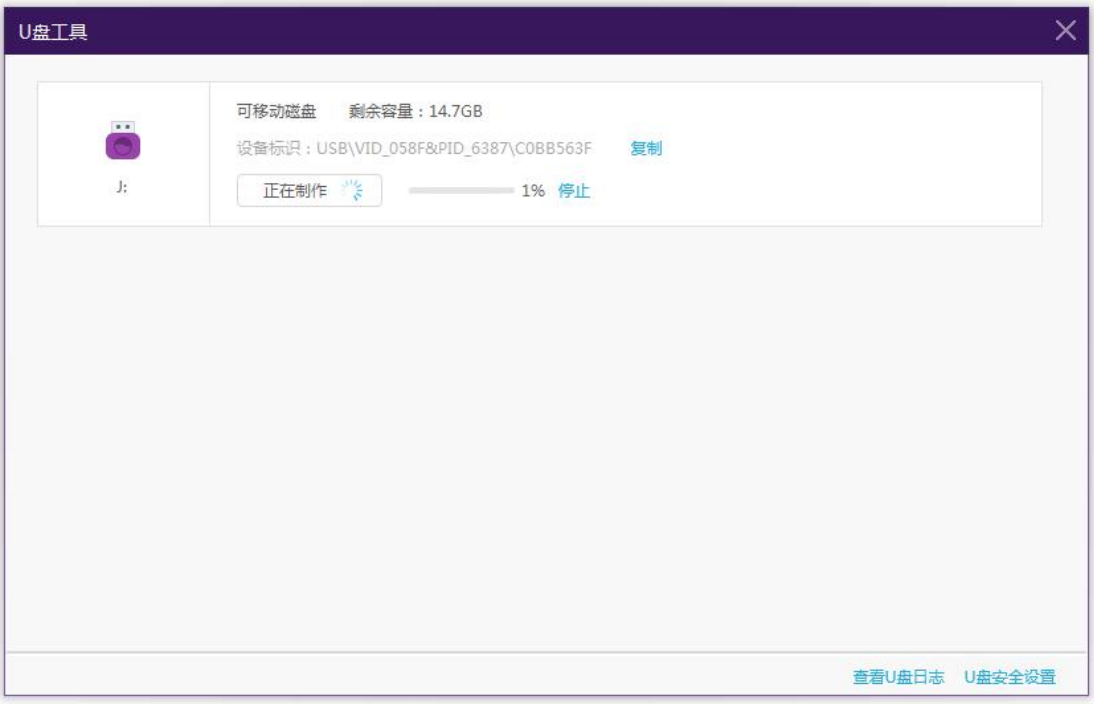
5.8.1 杀毒盘制作

首先将 U 盘插入客户端的 USB 接口，然后在工具界面点击【杀毒盘制作】，进入界面。

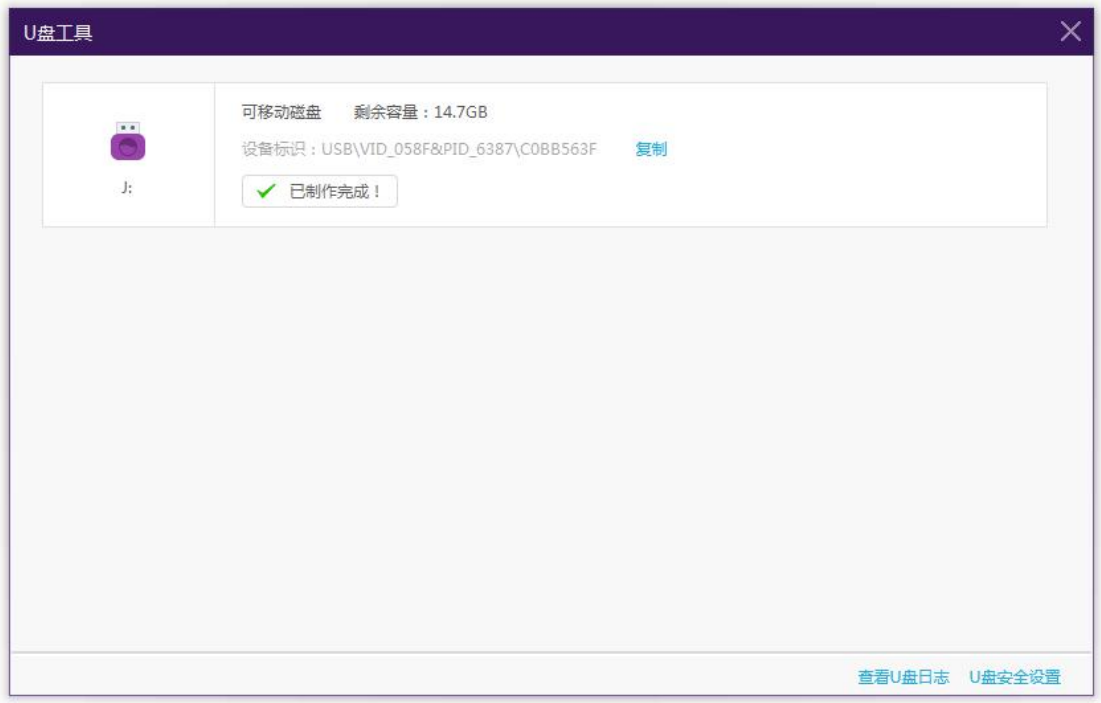


制作绿色杀毒

在 U 盘工具界面点击【制作绿色杀毒】，软件将自动开始制作绿色杀毒软件。



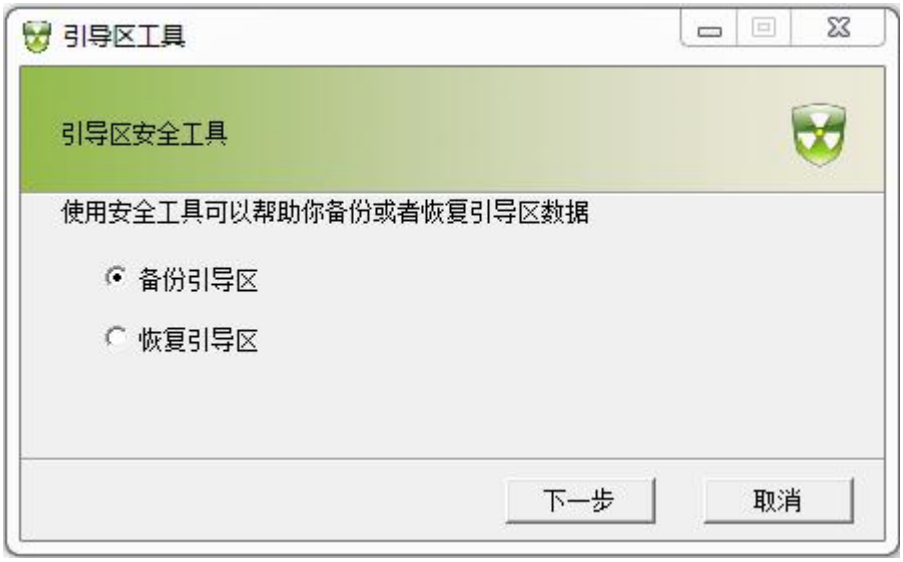
制作完成后界面如图所示。



绿色杀毒软件制作成功后，可以在未联网的情况下，拷贝到任何一台未安装杀毒软件的电脑上，即可在该电脑上使用瑞星杀毒软件。

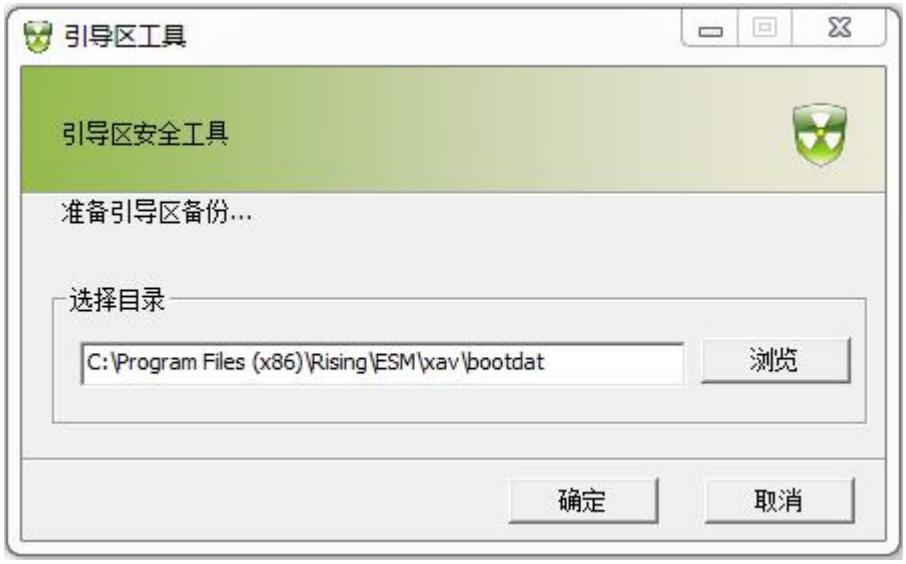
5.8.2 引导区工具

引导区工具可以帮助用户备份或者恢复引导区数据的功能。在工具界面点击【引导区工具】，进入引导区工具。



备份引导区

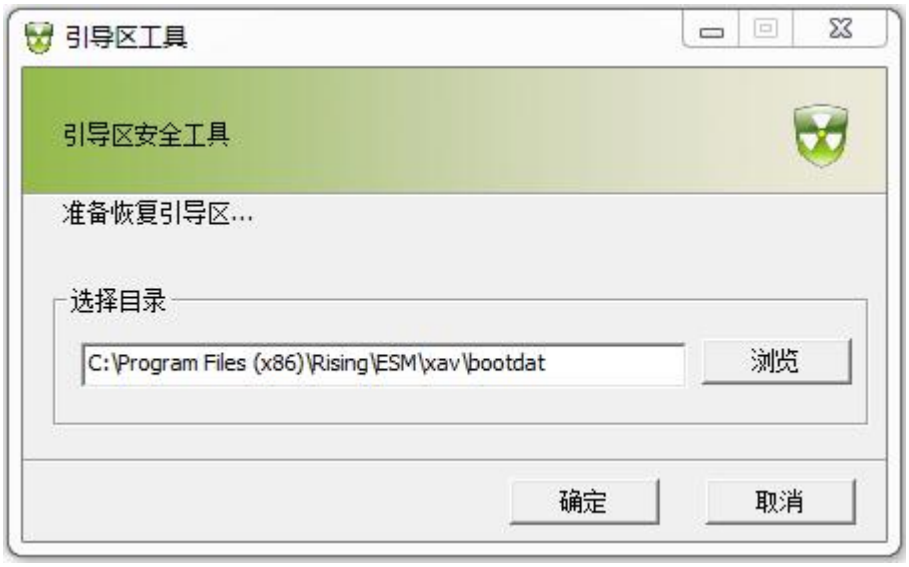
选择“备份引导区后”，点击【下一步】，可以选择引导区备份的路径。



路径选择完成后，点击【确定】即可完成备份，备份成功后，页面会弹出备份成功的提示信息。点击【取消】即可取消当前备份操作。

恢复引导区

当系统引导区损坏时，可以对引导区进行恢复操作。选择“恢复引导区”，点击【下一步】，再选择好之前备份文件的路径。



路径选择完成后，点击【确定】即可完成恢复，恢复成功后，页面会弹出恢复成功的提示信息。点击【取消】即可取消当前恢复操作。

5.8.3 日志打包

日志打包工具为用户软件的日志提供打包保存功能。

在工具界面点击【日志打包】，进入日志打包界面。也可以通过点击系统开始菜单的【ESM 365】程序组中的【日志打包工具】快捷方式启动工具。界面如图所示。

选择需要打包的日志，输入文件的名称，选择打包后的日志保存路径，点击【开始】，进行打包。打包后的日志保存于选择的路径中。到路径中提取日志包，以便于问题研究分析软件日志，便于排查软件问题。

5.9隔离区

隔离中心保存了杀毒操作中被删除的文件的备份，用户可以将这些文件恢复到指定的位置。

在主界面点击隔离区，进入隔离中心界面，如图所示。


瑞星ESM 365版
瑞星杀毒正在保护您的电脑!
日志中心
隔离区
检查更新
在线修复
智能客服
关于
全盘查杀
快速查杀
自定义查杀
智能安全引擎
基础引擎
决策引擎(RDM)
云查杀引擎
基因引擎
防护中心 (5/8)
当前版本：3.0 build：0.96
上次更新：2019-08-01 12:01:30
检查更新
发现病毒自动处理
扫描完成自动关机