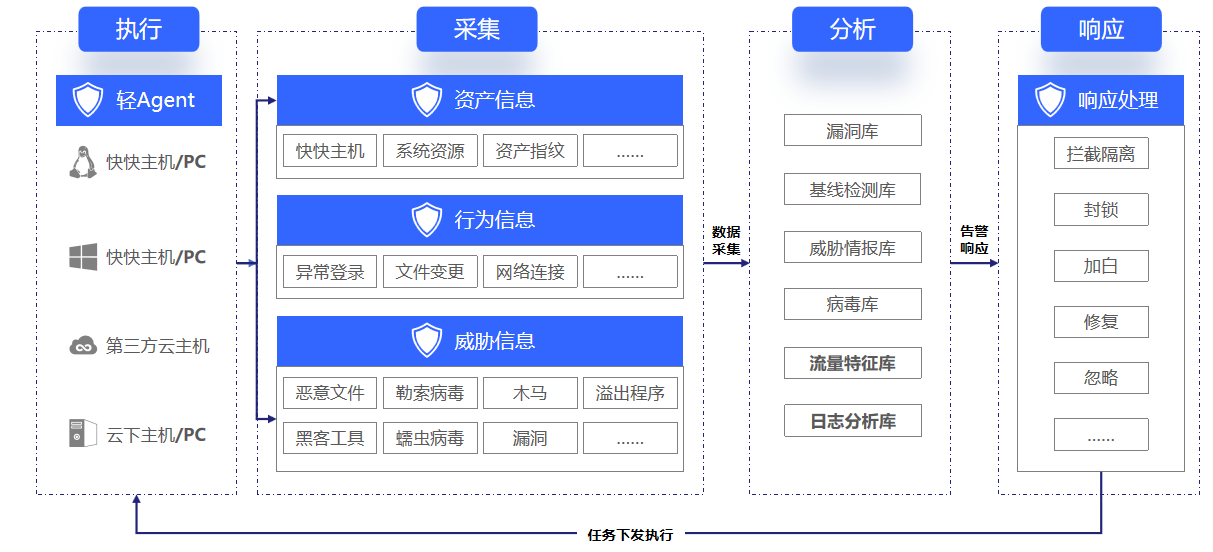
**快卫士用户使用手册（SaaS）**

**产品介绍**

**什么是快卫士**

快卫士是快快网络提供的一套终端安全解决方案，它集实时监测、智能分析、风险预警于一体，通过防勒索、漏洞扫描修复、防病毒、防篡改、合规检查等安全能力，帮助用户实现威胁检测与响应的自动化安全运营闭环，保护云上云下主机和办公PC安全，并满足监管合规要求。



**产品优势**

|  |  |
| --- | --- |
| 产品优势 | 具体说明 |
| 一键开启，轻量化运营 | 分钟级别的命令式安装，云上即开即用，规模扩大无需考虑软件的扩容和安全问题。 |
| 首个多重终端登录认证 | 2017年就在业内首个开创终端拥有者的身份二次认证功能，该技术获得专利创新认证。 |
| 统一化的终端安全管理 | 终端上的监控、资产信息、安全事件均可以在云端的控制台完成“白屏化操作”。 |
| 提供多种安全处理手段 | 病毒隔离查杀、漏洞一键修复、云端备份、安全规则出入流量限制、IP封禁等。 |
| 产品性能开销低 | 在终端正常负载下，Agent的CPU、内存占用率<10%（按2c2g规格来测算）；  在终端负载过高时 ，Agent会主动降级运行，严格限制对系统资源的占用；  内网部署下，客户控制台可以安装在虚拟化或真实物理环境中，只需满足该平台在纳管终端数规格下所需要的资源配置即可，无需特定独占服务器。 |
| 高性价比 | 主机防护、PC防护、等保合规产品服务。 |

**功能特性**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 功能模块 | 功能项 | 功能项说明 | 免费版 | 专业版 | 高级版 | 旗舰版 |
| 应用场景 |  |  | 满足个人单台终端资产基本资源消耗检测、登录异常等问题发现能力 | 满足个人少量终端资产的基础控制管理、漏洞问题发现、入侵检测、病毒查杀能力 | 满足企业用户多台终端资产统一运维管理，支持漏洞修复、系统安全配置检查、病毒查杀、入侵防护功能，满足企业等保合规检查要求 | 满足终端资产安全闭环的同时新增支持防护CC恶意攻击，网页防篡改及一对一安全专家全天候服务 |
| 终端资产管理 | 二次认证 | 业内首个开创资产拥有者身份二次认证功能 | **√** | **√** | **√** | **√** |
| 远程桌面保护 | 设定指定计算机、IP地址、指定区域、指定时间远程登录指定终端 | **√**(支持设置1个条件) | **√** | **√** | **√** |
| 远程桌面保护日志 | 记录远程登录终端日志信息 | **√**(支持查看近7天日志) | **√** | **√** | **√** |
| CPU监控 | 对终端平均CPU情况实时监测 | **√** | **√** | **√** | **√** |
| 内存监控 | 对终端内存使用量情况的实时监测 | **√** | **√** | **√** | **√** |
| 硬盘监控 | 对终端默认硬盘的使用情况实时监测 | **√** | **√** | **√** | **√** |
| 上传下载流量监控 | 对终端上传流量、下载流量的使用率实时监测 | **√** | **√** | **√** | **√** |
| 修改终端远程端口号 | 通过控制台对终端远程端口进行设置 | **√** | **√** | **√** | **√** |
| 终端软硬重启 | 通过控制台对终端进行软硬重启操作 | **√** | **√** | **√** | **√** |
| Agent问题排查 | 对Agent的异常状态进行问题检测 | **√** | **√** | **√** | **√** |
| 组织架构管理 | 通过组织架构对企业终端进行管理 | **√** | **√** | **√** | **√** |
| 修改终端远程密码 | 通过控制台对终端远程密码进行修改操作 | **√** | **√** | **√** | **√** |
| 终端资产管理 | 资产指纹 | 对终端中监听端口、运行进程、账户信息、软件管理进行信息收集展示 | **√** | **√** | **√** | **√** |
| 策略中心 | 终端防护保护 | 终端Agent基础设置 | **√** | **√** | **√** | **√** |
| 终端自适应管理 | 终端消耗的CPU、内存进行自定义阈值设置 | **×** | **×** | **√** | **√** |
| 病毒查杀 | 对系统自动进行病毒检测的策略设置 | **×** | **√** | **√** | **√** |
| 防勒索策略 | 对需要防护的终端目录进行防勒索策略的设置，预防未知的勒索病毒 | **×** | **×** | **√** | **√** |
| 对防护目录下的文件进行云端备份，方便终端数据异常时的恢复操作 | **×** | **×** | **√** | **√** |
| 资源监控策略 | 提供对应服务器系统监控阈值（CPU、系统盘容量、内存、网络流量）、异常位置登录告警等阈值设置 | **√** | **√** | **√** | **√** |
| 恶意进程自动防御 | 对系统检测出的恶意进程自动隔离查杀处理 | **×** | **√** | **√** | **√** |
| 防暴力破解 | 可自定义对暴力破解策略阈值设置 | **×** | **√** | **√** | **√** |
| 防端口扫描 | 可自定义对端口扫描策略阈值设置 | **×** | **×** | **√** | **√** |
| 防CC攻击 | 可自定义对CC攻击策略阈值设置 | **×** | **×** | **×** | **√** |
| 网页防篡改策略 | 对有重要文件的终端进行防护策略设置 | **×** | **×** | **×** | **√** |
| Webshell防护策略 | 对设置的防护目录下文件进行实时监测排查Webshell后门进行告警并提供处理方式 | **×** | **×** | **√** | **√** |
|  | 二次认证 | 业内首个开创资产拥有者身份二次认证功能 | **√** | **√** | **√** | **√** |
|  | 合规基线 | 自定义设置系统扫描基线策略 | **×** | **×** | **√** | **√** |
|  | 安全加固 | 虚拟防火墙在云端划分安全区域，通过配置安全规则，控制终端的入流量和出流量 | **×** | **√** | **√** | **√** |
|  | IP白名单 | 支持将信任IP列入白名单，系统不再进行IP异常判断 | **×** | **√** | **√** | **√** |
|  | 进程白名单 | 支持将信任进程列入白名单，系统不再进行IP异常判断 | **×** | **√** | **√** | **√** |
|  | 文件白名单 | 支持将信任文件列入白名单，系统不再进行IP异常判断 | **×** | **×** | **√** | **√** |
|  | 隔离箱 | 对于系统误判/人工判定的异常进程归入隔离箱，可在此进行恢复 | **×** | **√** | **√** | **√** |
|  | 漏洞管理 | 支持自定义进行漏洞等级、范围的扫描设置 | **×** | **×** | **√** | **√** |
|  | 策略恢复 | 对控制台常用功能的配置策略提供下载保存功能 | **×** | **×** | **√** | **√** |
| 威胁检测 | 病毒查杀 | 可有效清理服务器上的各类恶意威胁 | **×** | **√** | **√** | **√** |
|  | 漏洞查补 | 通过与漏洞库进行比对，检测并管理系统和软件存在的漏洞，对当前系统中存在的紧急漏洞进行提醒修复 | **√**（仅支持扫描） | **√**（仅支持扫描） | **√** | **√** |
|  | 合规基线 | 支持基线检测，包括登录弱口令检测、登录安全配置检测、密码复杂性检测、配置检测、用户权限配置文件、检测空密码账户检测等等 | **×** | **×** | **√** | **√** |
|  | 网页防篡改 | 检测当前系统存在非正常网络篡改行为进行拦截并告警，防止网站被植入黑链、色情等信息 | **×** | **×** | **×** | **√** |
| 告警与响应中心 | 安全告警 | 检测当前系统存在异常进行告警提示处理 | **√**（仅部分告警） | **√**（仅部分告警） | **√** | **√** |
| 日志报表 | 安全报告 | 周期性对终端安全防护情况进行汇总，并提供展示和保存功能 | **×** | **×** | **√** | **√** |
| 操作日志 | 对在控制台的任何操作进行记录 | **√** | **√** | **√** | **√** |
| 日志分析 | 提供准确实时的日志查询和日志分析能力 | **×** | **×** | **×** | **√** |
| 用户中心 | 用户账号 | 支持管理员对用户账号的增管及角色权限分配 | **√** | **√** | **√** | **√** |
| 组织架构 | 支持无限层级的组织架构设置 | **√** | **√** | **√** | **√** |
| 角色权限 | 支持对角色权限的管理，支持分配用户多重角色 | **√** | **√** | **√** | **√** |
| 系统管理 | 终端部署 | 对Agent安装步骤说明，包括安装注意事项、单台终端安装及批量安装，同时支持在线卸载 | **√** | **√** | **√** | **√** |
| 账号安全 | 支持对登录产品控制台账号进行安全设置 | **√** | **√** | **√** | **√** |
| 通知设置 | 支持对周期性及实时告警的类型、频率、时间、通道的设置。告警通道覆盖短信、微信、邮件、飞书机器人、钉钉机器人 | **√**（仅支持有限的短信、微信、邮件） | **√** | **√** | **√** |

**接入快卫士**

**Agent概述**

安装快卫士Agent后，您的终端资产才能受到快卫士的保护。

**安装Agent**

参考安装手册：[安装手册](https://cex1rtlpay.feishu.cn/wiki/X5UtwhX6kioJiak7OOoc7TK4nob?from=from_copylink)

**卸载Agent**

如果某台终端无需快卫士提供的安全防护，您可以卸载该终端上的快卫士Agent。本文介绍如何卸载快卫士Agent。

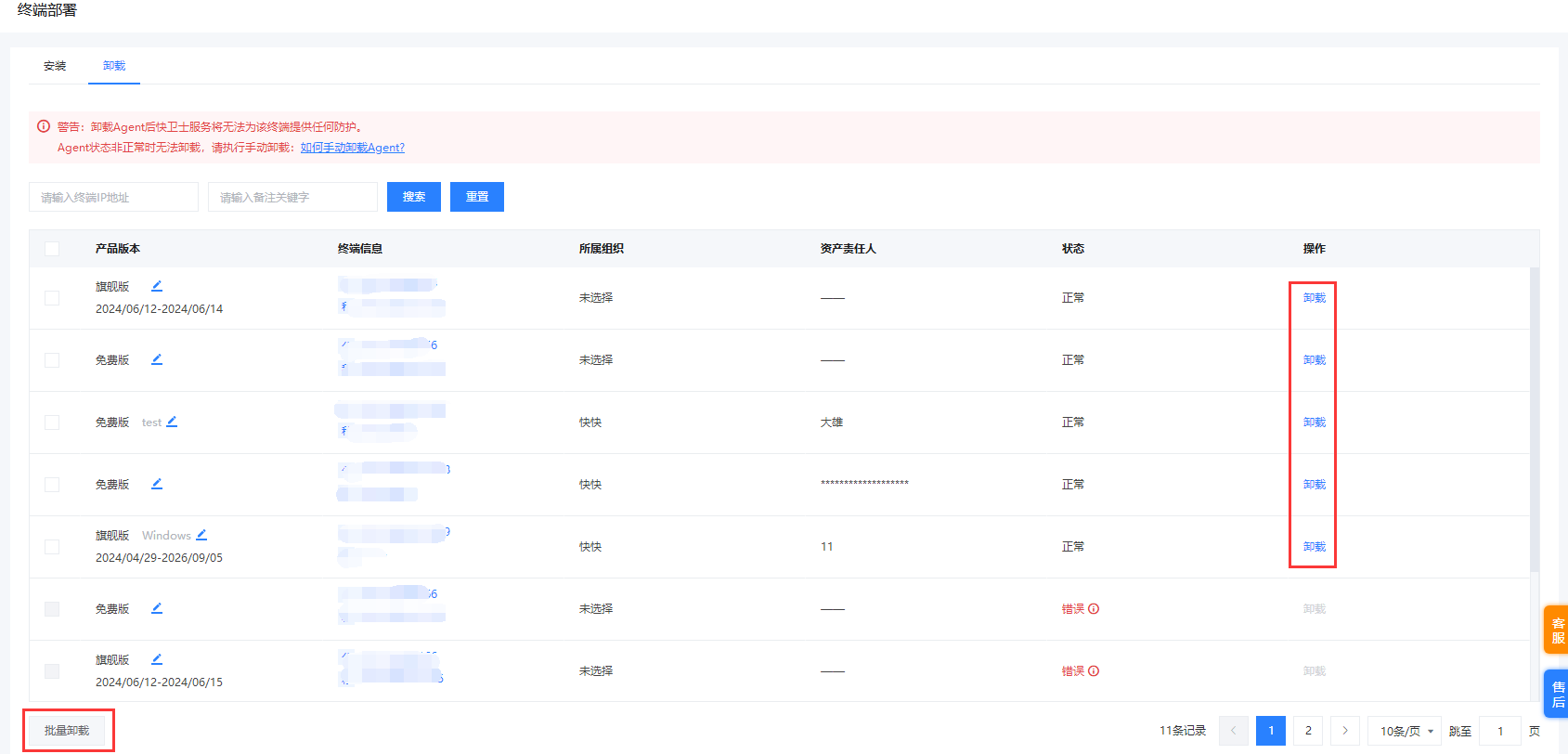
**卸载须知**

快卫士是快快网络科技有限公司官方提供的终端安全软件，卸载终端上的快卫士Agent会产生影响如下：

* 快卫士不再为该终端提供安全告警服务
* 快卫士不再为该终端提供非法入侵防护
* 快卫士不再为该终端提供监控系统资源服务
* 快卫士不再为该终端提供漏洞、基线检测防护
* 快卫士不再为该终端提供资产指纹服务
* 快卫士不再为该终端提供防火墙防护
* 快卫士不再为该终端提供病毒查杀、防勒索功能
* 快卫士不再为该终端提供防CC攻击功能
* 快卫士不再为该终端提供网页防篡改保护

**云端卸载方式**

1. 登录**快卫士控制台**，在上方导航栏，选择**系统管理**。
2. 在左侧导航栏，选择**终端部署-》卸载**。

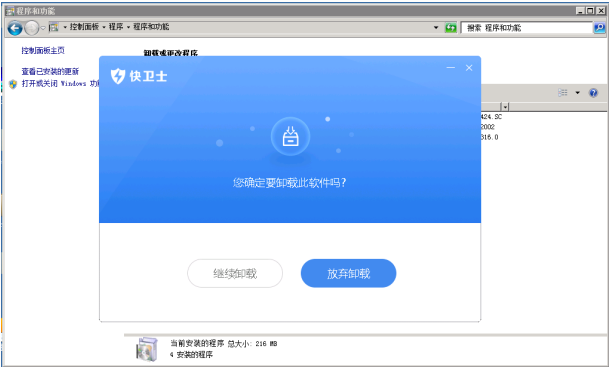


|  |
| --- |
| 当Agent状态未为非正常时，无法进行云端卸载。需登录终端执行手动卸载。 |

**手动按卸载Agent**

* **Windows系统服务器手动卸载Agent方式**

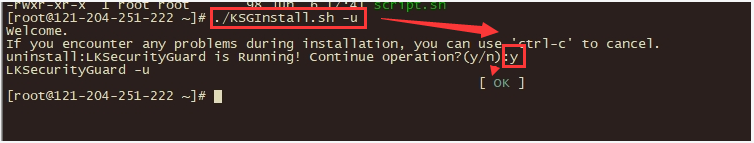
1. 直接在控制面板上，找到程序和功能，在界面上，找到快卫士进行双击，根据界面提示进行卸载。如图：



1. 双击快卫士Agent安装包进行卸载。

* **Linux系统服务器手动卸载Agent方式**

1. 复制该命令卸载快卫士Agent：./KSGInstall.sh -u



**Agent状态异常排查**

Agent状态主要分为以下五种，若Agent的运行状态为“错误”时，可能是Agent与服务器间通讯异常。请参见本文进行排查。

* 正常：Agent运行正常
* 错误：Agent与快卫士云端端通讯异常
* 停止：Agent被停止防护
* 静默：Agent检测终端资源消耗异常而自动降级防护
* 未安装：终端未安装快卫士Agent
* 卸载：快快终端卸载了快卫士

**可能的原因**

* 使用错误的安装命令
* 网络故障：Agent和快卫士云端通信出现异常，例如网络连接中断
* Agent进程异常
* 用户手动停止快卫士Agent防护，系统异常

**处理方法**

|  |  |
| --- | --- |
| 快快-Linux | **1、**若安装后，控制台显示机器还是未安装，刷新无效后。  1）请登录终端执行下列命令：grep -a "Connect to Server" LKSecurityGuard.log确认是否正常连接云端服务器。若有当前时间的错误日志，则说明存在连接失败情况，将情况反馈我司技术处理。  **2、**登录服务器执行以下命令：egrep -i -r 'killed process' /var/log确认系统是否强制退出快卫士。若存在此情况，则反馈我司技术处理。  **3、**到根目录查看是否有core.xxx文件，有则反馈给技术支持并把快卫士的版本号（版本号查询方法：LKSecurityGuard -v）一同告知。  **4、**以上情况均正常，仍旧无法启动快卫士，则打包快卫士日志目录（/var/ksg/log）提供我司技术查看。 |
| 非快快-Linux | **1、**若安装后，控制台无法显示相关产品信息。  1）请登录终端执行下列命令：grep -a "Input key value is error" LKSecurityGuard.log确认Key值是否正确。  **2、**登录终端执行以下命令：egrep -i -r 'killed process' /var/log确认系统是否强制退出快卫士。若存在此情况，则反馈我司技术处理。  **3、**到根目录查看是否有core.xxx文件，有则反馈给技术支持并把快卫士的版本号（版本号查询方法：LKSecurityGuard -v）一同告知。  **4**、以上情况均正常，仍旧无法启动快卫士，则打包快卫士日志目录（/var/ksg/log）提供我司技术查看。 |
| Windows | **1、**确认是否防火墙出站规则是否禁用了9501，9503、9601/9603端口；  **2、**确认快卫士服务进程KSecurityGuard.exe是否正常运行；  **3、**至快卫士目录下将log日志提交我司技术排查，默认安装路径：C:\Program Files (x86)\快快网络\快卫士\Log。 |

**工作台**

**终端管理**

**终端资产管理**

快卫士支持采集并记录终端信息以及终端上的端口、软件、进程、账户、资源监控、防入侵设置、漏洞基线检测等信息，帮助您全面了解终端运行状态，便于统一管理。

**终端分组**

您可以根据您企业实际组织架构情况，进行对终端的分组管理，当前组织架构不限层级限制。组织架构的统一设置，可参考本文[用户中心-》组织架构](https://cex1rtlpay.feishu.cn/wiki/CGKJwhLABi8sBlkR9F1coO6ZnRb#doxcnzZz5QIkdsybODdI6phLuJd)章节。



**查看终端信息**

快卫士的终端资产管理页面提供了所有终端的相关信息。

**操作步骤**

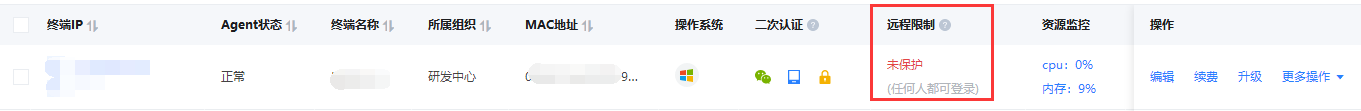
1. 登录快卫士控制台。在上方导航栏，选择**终端管理**。
2. 在左侧导航栏，选择**终端资产管理**，查看终端资产信息。

如果您想查看某个终端的信息，您可以使用终端列表上方提供的搜索功能，通过搜索**产品版本、Agent状态、远程限制、终端类型、服务商类型、IP地址或关键字**来搜索该终端。



**修改终端保护状态**

快卫士的终端管理页面提供的所有终端的登录入口保护状态信息。



远程登录保护设置包括计算机名认证、IP地址[WAF]认证、区域认证、登录时间认证。

|  |
| --- |
| 1. Linux系统无法设置计算机名认证。 2. 免费版的快卫士，远程桌面保护条件仅支持1个设置数。远程登录日志仅支持查看近7天记录。 |

* 计算机名认证

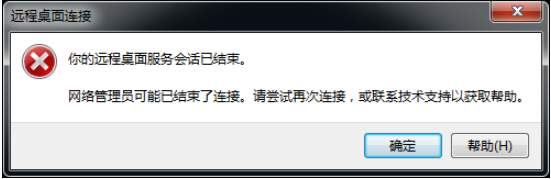
当您设置**计算机名认证**时，则只能通过设置的符合要求的计算机名才能认证成功访问对应终端。



* 单选**计算机名认证**，填写您需要认证的计算机名，多个计算机名则换行隔开。
* 单击**保存**按钮。
* 若您需要将配置覆盖至其它终端，则点击添加至其它终端进行覆盖。

注：付费版多条设置数无法覆盖免费版产品。

* 用非配置的计算机名远程访问安装Agent的终端电脑，出现以下的提示：

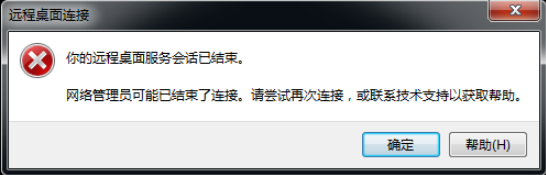


* IP地址[WAF]认证

当您设置**IP地址[WAF]认证**时，则只能通过设置的符合要求的IP地址才能认证成功访问对应终端。



* 单选**IP地址[WAF]认证**，填写您需要认证的IP地址，多个IP地址则换行隔开。
* 单击**保存**按钮。
* 若您需要将配置覆盖至其它终端，则点击添加至其它终端。
* 用非配置的IP远程访问安装Agent的终端电脑，出现以下的提示：

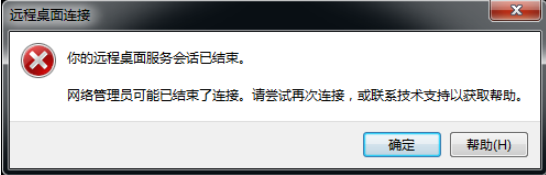


* 区域认证

当您设置**区域认证**，需选择需要认证的省市。未认证前默认全部区域可登录，认证后仅限于当前认证区域可登录。



* 单选**区域认证**，填写您需要认证的省市，可多选
* 单击**保存**按钮
* 若您需要将配置覆盖至其它终端，则点击添加至其它终端
* 用非配置的区域远程访问安装Agent的终端电脑，出现以下的提示：

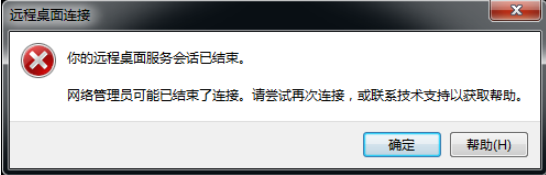


* 时间认证

单选**登录时间认证**，设置需要认证开始和结束时间。认证后超过登录范围的时间就算输入正确密码也无法成功登录。登录时间设置支持跨天设置，例如可设置晚上23:00—凌晨3:00的时间范围。



1. 单选**登录时间认证**，填写您需要认证的时间，开始时间需要小于结束时间
2. 单击**保存**按钮
3. 若您需要将配置覆盖至其它终端，则点击添加至其它终端按钮。
4. 用非配置的时间外的时间远程访问安装Agent的终端电脑，出现以下的提示：



**查看单个资产详情**

快卫士的终端资产管理页面提供了所有终端信息，包括详细信息、二次认证、系统资源监控、远程桌面保护、Windows系统漏洞/Linux软件漏洞、基线检测等。

**操作步骤**

1. 登录**快卫士控制台**，在上方导航栏，选择**终端管理**。
2. 在左侧导航栏选择**终端资产管理**
3. 选择查看的资产，点击**资产IP**，查看该资产内信息。

* 详细信息：该资产的实例ID、所属组织、资产等级、公网IP、私网IP、操作系统、内核版本、Agent状态、终端名称、MAC地址、资产责任人、责任人电话、资产编号、资产位置、终端类型、资源类型、终端来源、备注等。
* 资产指纹：查看资产指纹的统计信息。单击对应统计数值可抽屉页签查看指纹详细信息。
* 服务商类型：可对当前终端设置厂商归属，便于区分管理。
* 修改密码：可对该终端修改远程登录密码，增加终端安全。
* 二次认证：查看绑定的微信、手机、二次密码及备用密码信息，可针对单台终端进行验证开启或关闭，同时可设置远程登录验证的频率。
* 系统资源监控：实时监控当前终端CPU、内存、硬盘、流量使用量。
* 漏洞：查看目标终端下漏洞检测结果。
* 基线检测：查看目标服务器下基线检测结果。

**终端续费、升级**

快卫士专业版、高级版、旗舰版服务到期前，您需要及时续费以免影响正常的安全服务。快卫士支持手动续费和按月自动续费。

**到期说明**

快卫士高级版服务器到期前7天，到期前3天和到期当天，系统会以短信、微信和邮件的方式通知您续费。如果在服务到期前您没有及时续费，那么在服务到期日的次日，您将无法继续使用快卫士专业版、高级版、旗舰版的功能。

**快卫士版本手动续费**

参照以下步骤，手动为您的快卫士终端续费：

1. 登录**快卫士控制台**，在上方导航栏，选择**终端管理。**
2. 在左侧导航栏，选择**终端资产管理**。
3. 在**终端资产管理**列表中，单击**续费**。



1. 确认订单配置，并选择**购买时长**。
2. 进行订单确认后，点击**确认支付**。
3. 完成订单支付。

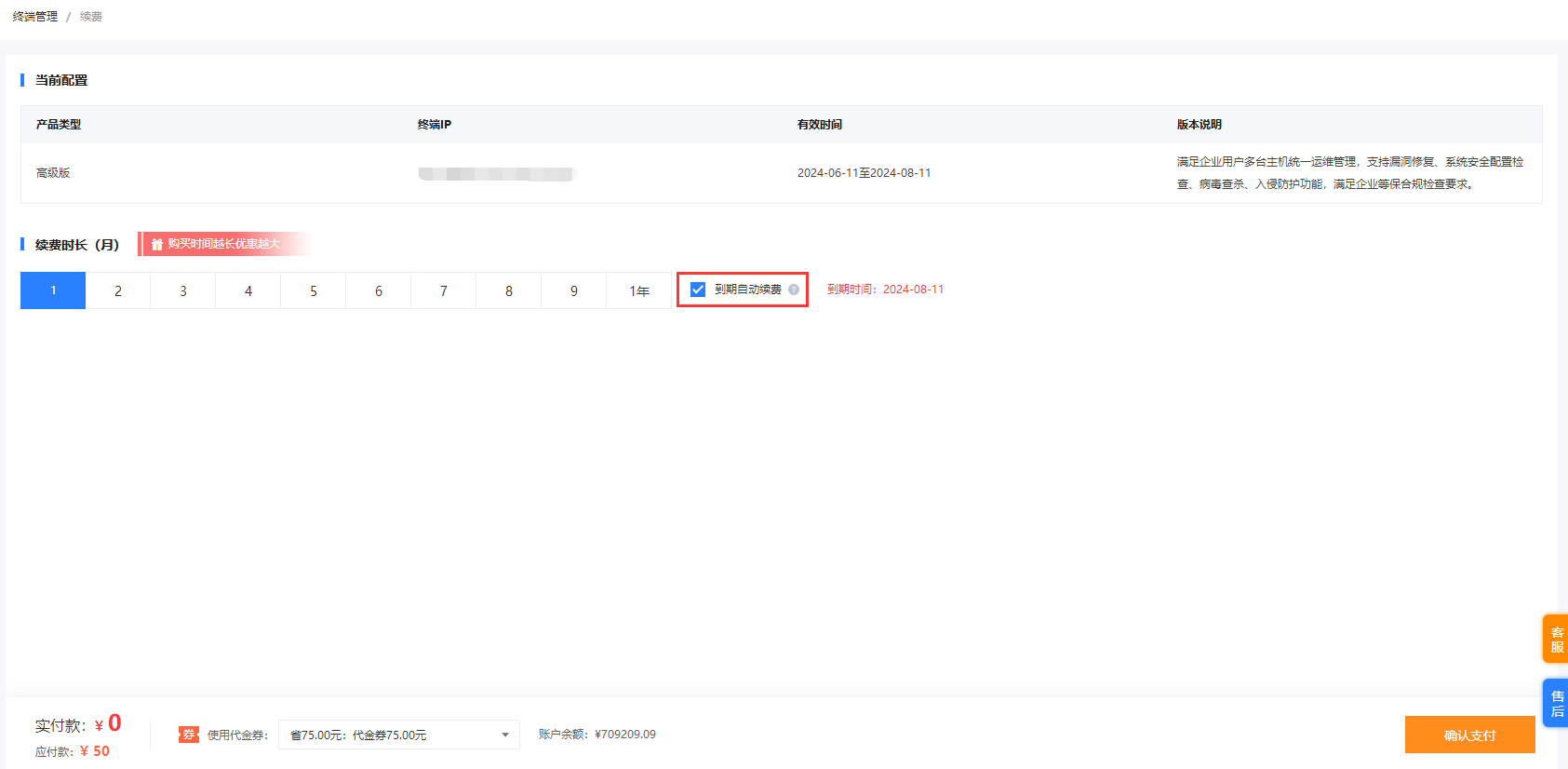
**快卫士版本按月自动续费**

如果您需要长期使用快卫士服务，可以开通按月自动续费功能。开通按月自动续费功能后，系统将在资源到期前执行自动续费操作，无需您手动操作续费。推荐您开通按月自动续费，避免因实例到期自动释放后安全防护失效，导致业务面临被黑客入侵的风险。以下是自动续费规则的说明：

* 自动续费将于服务到期前3天开始扣款，请保证账号余额充足，如果您的实例将于明天到期，请进行手工续费操作。
* 设置自动续费后将默认按照最近续费月份进行续费。

您可以参考一下步骤为快卫士服务开启按月自动续费。

1. 登录**快卫士控制台**，在上方导航栏，选择**终端管理。**
2. 在左侧导航栏，选择**终端资产管理**。
3. 在**终端资产管理**列表中，单击**续费**。
4. 确认订单配置，并选择**购买时长**。
5. 勾选**到期自动续费**选项。



1. 进行订单确认后，点击**确认支付**。
2. 完成订单支付。

**快卫士版本升级**

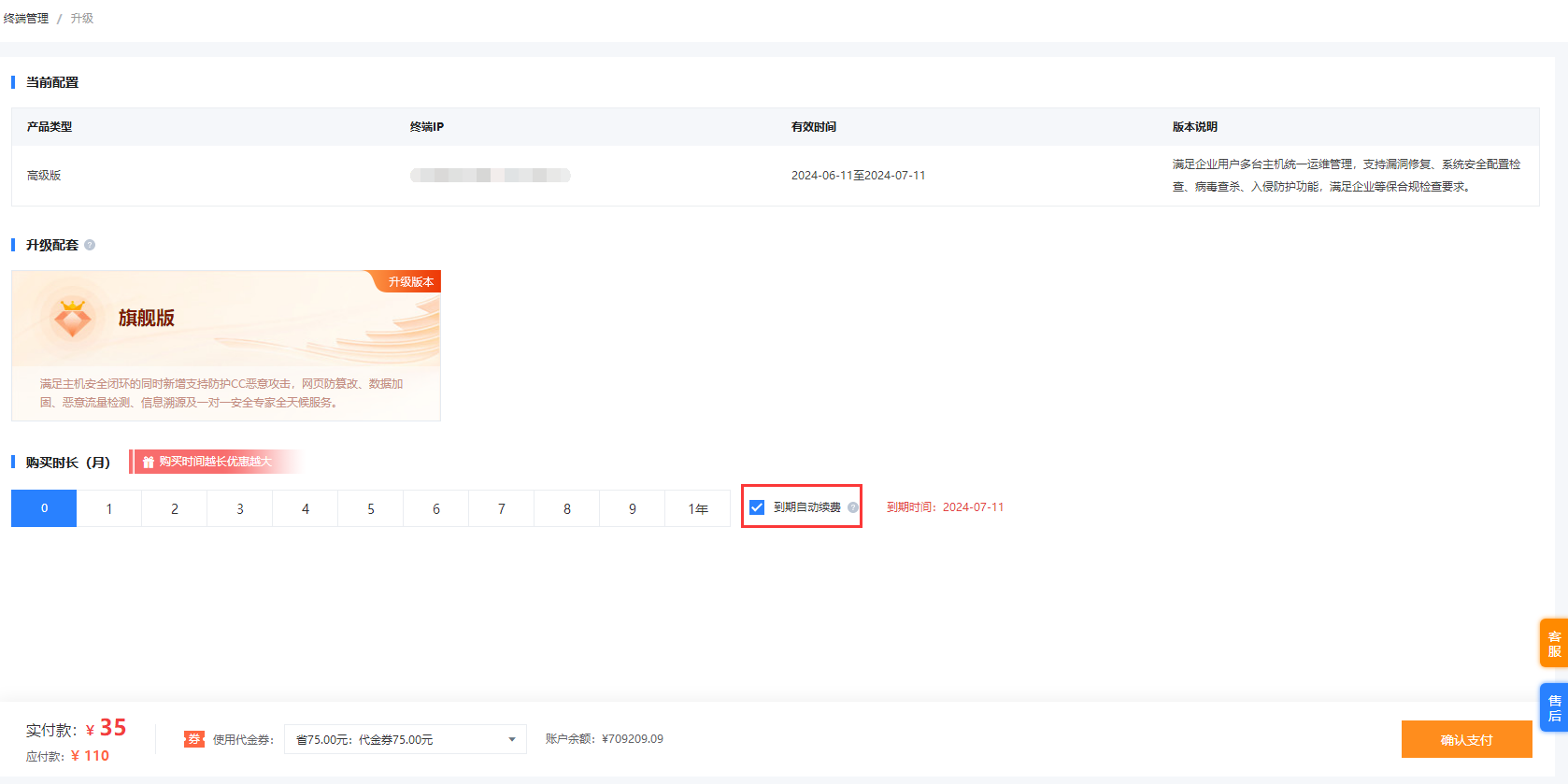
快卫士的升级默认为当前版本在到期前通过补差价方式进行升级。

参照以下步骤，手动为您的快卫士终端升级。

1. 登录**快卫士控制台**，在上方导航栏，选择**终端管理。**
2. 在左侧导航栏，选择**终端资产管理**。
3. 在**终端资产管理**列表中，单击**升级**。



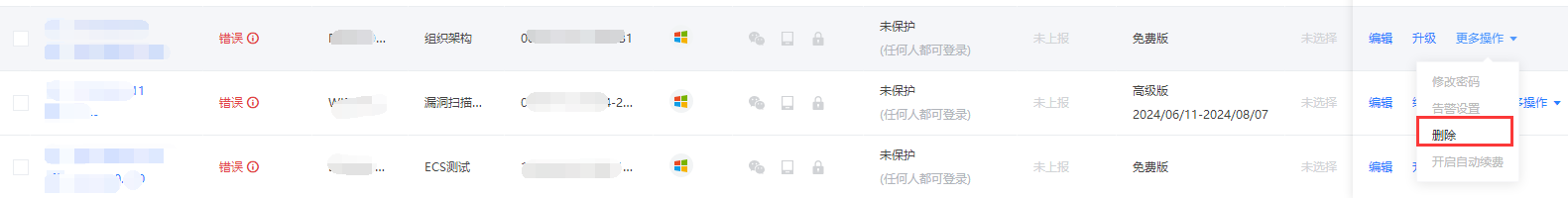
1. 选择您需要的升级版本，单击**立即购买**。建议您同时勾选自动续费选项，为您的终端持续安全防护。



1. 完成支付。

**删除列表中非快快服务器**

如果您的非快快终端已经Agent状态已经非正常（即处于错误、卸载状态），您确认无需快卫士继续防护这台终端，您也可以直接执行删除操作。



**配置迁移**

**场景使用**

1. Agent未通过正常流程卸载，直接进行的系统重装导致控制台出现了两条相同IP的记录。
2. 产品版本灵活配置，支持产品版本从一台终端迁移至另一台终端。
3. 原终端IP弃用，需要将原终端的配置信息迁移至新IP继续使用。

参照以下步骤，实现终端配置迁移操作：

**操作步骤**

1. 登录快卫士控制台-》终端资产管理-》找到需要配置迁移的终端-》更多操作-》配置迁移。



|  |
| --- |
| 配置迁移支持迁移三种方式：产品版本+安全配置策略、仅产品版本、仅安全配置策略。  配置迁移支持相同产品版本间、高阶产品迁移到低阶版本的操作场景。  高阶版本迁移低阶版本，无法选择“仅安全配置策略”选项。  高阶版本迁移低阶版本，选择“仅产品版本”，迁移完成后，原高阶的安全策略被锁定，无法再次迁移。 |

1. 配置迁移终端选择
2. 迁移的内容选择：产品版本+安全配置策略、仅产品版本、仅安全策略



|  |
| --- |
| 安全策略包括：远程登录保护策略、策略中心内所有策略信息  产品版本包括：产品版本信息（版本、有效时间）、是否自动续费设置 |

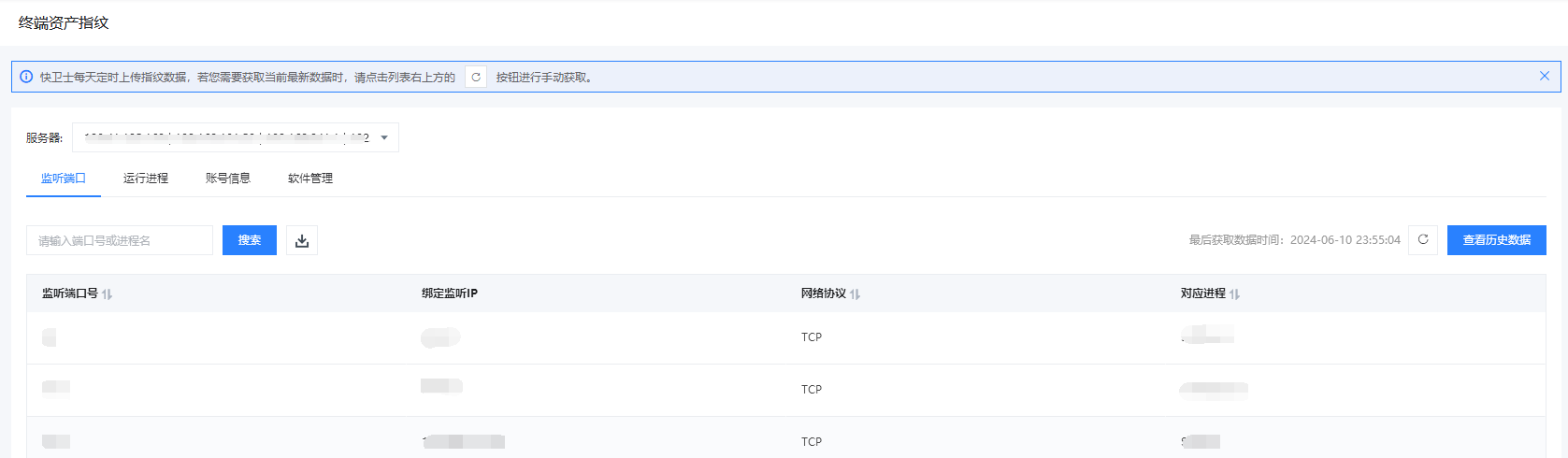
1. 记录留存选择（默认不保留）

|  |
| --- |
| 快快终端：需要通过删除服务器可删除记录信息。  非快快终端：选择不保留记录，则即时删除该条数据。 |

**终端资产指纹**

资产指纹可以为您提供对应终端下指纹（端口、进程、账号、软件）等资产统计信息。

您可手动触发终端资产指纹数据的更新，获取目标终端资产指纹的最新数据。



您可点击查看历史数据来确认目标服务器记录的历史指纹信息。

|  |
| --- |
| 资产指纹查看历史数据功能为快卫士的增值服务，仅**高级版和旗舰版**用户可开通和使用该服务。免费版、专业版用户需先升级到高级版或旗舰版才可使用查看历史数据功能。 |

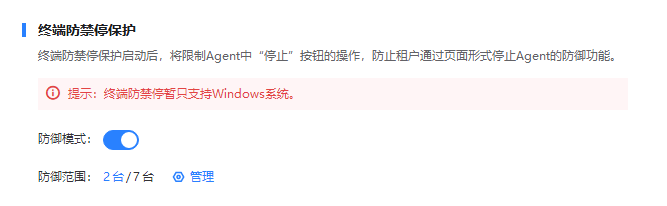
**策略中心**

**基础策略**

**终端防禁停保护**

该功能防止未经授权，在终端资产上对Agent操作停止安全防护。功能默认关闭。租户根据实际场景开启。开启后支持功能覆盖范围的选择。

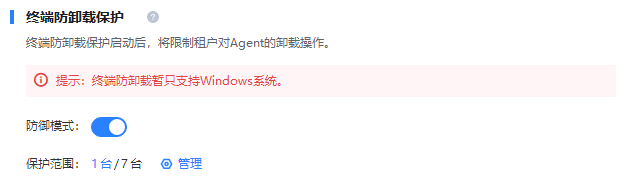
|  |
| --- |
| 该功能仅支持Windows系统。 |



**终端防卸载保护**

该功能防止未经授权对Agent进程进行退出、卸载的操作。

|  |
| --- |
| 该功能仅支持Windows系统。 |



**终端自适应管理**

该功能可根据终端业务运行需要，支持对CPU、内存的安全阈值自定义设置。作用于在实现安全防护的同时不影响终端上业务的正常运行。

|  |
| --- |
| 1.免费版、专业版默认基础防护，即对终端CPU和内存实时检测，超出系统设置的安全阈值后Agent将保留基础防护，不再启动定时扫描任务。  2.**高级版、旗舰版**可对防护策略阈值进行自定义设置。  3.默认一台终端仅支持一条防护策略。 |



**病毒查杀策略**

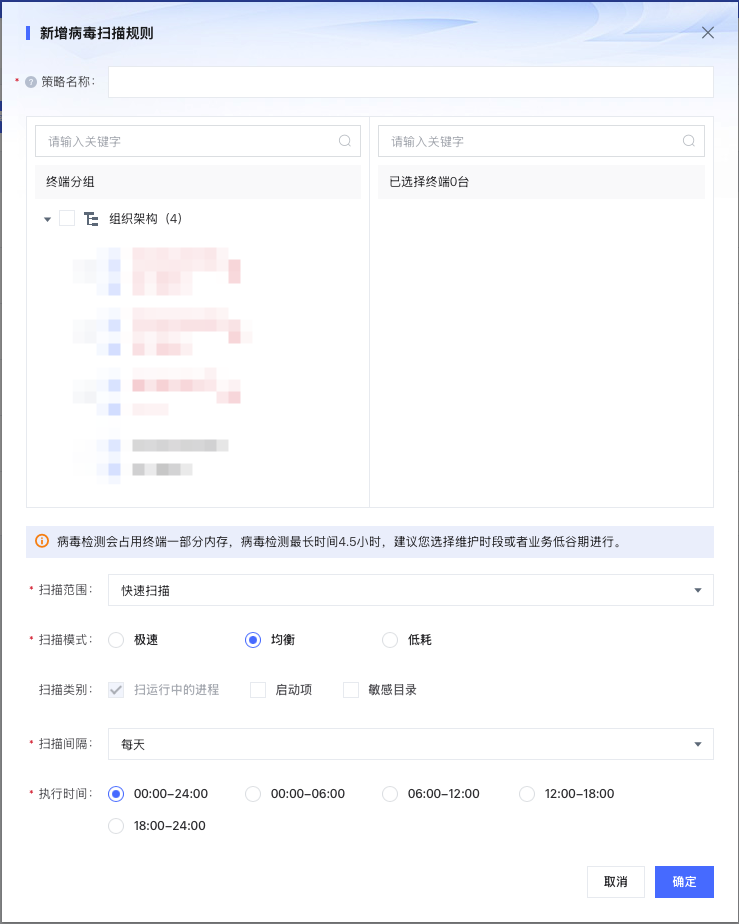
快卫士针对病毒扫描检测，提供了自定义定时扫描设置任务。您无法及时对终端进行病毒扫描检测时，即可通过该功能定时执行。

选择扫描执行时间段后，系统将在时间段任一时间进行病毒策略执行。

|  |
| --- |
| 1.仅快卫士**专业版、高级版、旗舰版**支持该功能，免费版不支持。  2.默认每台终端仅支持一条病毒扫描策略。  3.病毒扫描会占用终端一部分内存，扫描时长根据终端文件量而定，最长扫描时间4.5小时，建议您选择终端的维护时段或者业务低谷期进行。 |

**设置病毒查杀策略**

1. 登录快卫士产品控制台。
2. 点击上方导航，选择**策略中心。**
3. 在左侧导航栏，选择**病毒查杀策略-》新增病毒扫描规则。**



**实时防护**

**防勒索策略**

防勒索病毒已成为网络安全最大的威胁之一。快卫士针对勒索病毒，提供了通用的反勒索解决方案，该方案帮您解决终端被勒索病毒入侵的后顾之忧。

|  |
| --- |
| 防勒索功能为快卫士的增值服务，仅**高级版和旗舰版**用户可开通和使用该服务。免费版用户需先升级到高级版才可使用防勒索功能。 |

**勒索病毒防护原理**

* 实时防御已知勒索病毒

快卫士实现了对大量已知勒索病毒的实时防御，在终端被病毒感染的第一时间拦截勒索病毒，避免发生文件被病毒加密而进行勒索的情况。

* 诱捕、拦截新型未知勒索病毒

通过放置诱饵的方式，快卫士实时捕捉可能存在的勒索病毒行为。针对新型未知的勒索病毒，一旦识别到有异常加密行为发生，会立即拦截，同时通知您进行排查清理。

* 支持恢复被病毒感染文件

快卫士在对勒索病毒进行防御的同时，还支持文件云端备份服务，能定期对指定文件进行备份，支持按时间或文件版本恢复服务器数据。在发生极端情况导致文件被加密时，能够通过文件恢复的方式找回数据，确保终端数据的安全。

**数据备份说明**

快卫士根据用户设置的防护目录，自动启动不同数量的备份任务。若防护目录下的数据量大，备份耗时将增加，备份会消耗一定量的CPU和内存资源。为避免对您的业务造成影响，建议您选择业务量较小的时段进行数据备份。

当备份的数据量较大时，Windows数据备份会在本地拷贝数据形成临时性文件，分段至云端合并备份。故需要终端本地需要有足够大的存储空间，避免因无法拷贝成功导致备份失败。

**创建防护策略**

1. 创建策略前，请确认您终端的内核版本在支持范围内，不再支持范围内的终端将无法进行数据备份。
2. 登录快卫士产品控制台。在控制台上方导航栏，选择**策略中心**。
3. 在左侧导航栏，选择**实时防护-》防勒索策略**。
4. 点击**创建防勒策略**面板，输入**策略名称**，选择终端资产后设置数据备份的具体策略，并单击**保存。**

|  |  |
| --- | --- |
| 配置项 | 说明 |
| 策略名称 | 设置防护策略的名称 |
| 选择终端 | 支持选中单台终端、跨组织选中多台终端或者选中组织分组 |
| 防护目录 | 设置备份终端指定目录。您需要在防护目录路径中新增需要备份的目录地址。配置示例：   * Windows：C:\Program Files (x86)\ * Linux：/usr/bin/   最多可添加10条防护目录路径。快卫士会串行执行各个防护目录地址的备份任务。如果一个防护目录地址下的文件较多，可能会消耗较多的终端资源（CPU和内存）。您可以将一个目录拆分为多个防护地址目录，通过串行执行备份任务，有效地降低备份占用的服务器资源。 |
| 排除指定目录 | 指定不需要备份的目录。快卫士提供了默认的不需要备份的目录，您可以在此基础上修改目录。 |
| 防护文件类型 | 选择需要进行防护的文件类型，支持选择以下类型：   * **全部文件类型**：即针对所有类型的文件进行备份防护。 * **指定文件类型**：即针对指定文件进行备份防护。支持选择文档类、图片类等。  |  | | --- | | 支持同时选中多个文件类型。快卫士仅防护您终端中此处选中的文件类型。 | |
| 数据备份开始时间 | 设置数据备份开始时间。系统默认显示隔天零点。   |  | | --- | | 防护策略创建后，数据备份时会消耗一定量的CPU和内存资源。为避免对您的业务造成影响，建议您选择业务量较小的时段进行数据备份。 | |
| 备份策略执行间隔 | 设置备份策略执行间隔，默认为1天。 |
| 备份数据保留时间 | 设置备份数据保留时间，默认为7天，   |  | | --- | | 超过备份数据保留时间后，备份数据会被自动清理。 | |

创建防护策略后，策略状态默认为关闭状态，若策略需要使用，请及时开启。同时建议您重点关注Agent状态，及时处理Agent异常状态，以确保防勒索备份与恢复任务正常执行。

**资源监控策略**

资源监控策略可以为您提供对应终端系统监控阈值（CPU、系统盘容量、内存、网络流量）、等控制值设置。您可以建立多个策略，针对不同终端进行应用。



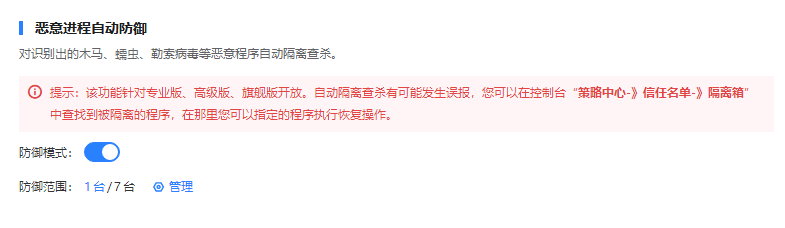
**恶意进程自动防御**

该功能为您自动拦截系统扫描出的常见病毒。

|  |  |  |
| --- | --- | --- |
| 功能 | 支持版本 | 描述 |
| 恶意进程自动防护 | 专业版、高级版、旗舰版 | 能够自动拦截并查杀常见网络病毒，包括主流勒索病毒、DDoS木马、挖矿和木马程序、恶意程序、后门程序和蠕虫病毒等。   |  | | --- | | 自动隔离查杀可能发生误报，您可以在控制台“策略中心-》信任名单-》隔离箱”中找到被隔离的进程，执行恢复操作。 | |

**开启防御能力**

1. 登录快卫士产品控制台。在控制台上方导航栏，点击**策略中心。**
2. 在左侧导航栏，选择**实时防护**-》**恶意进程自动防御。**
3. 开启防御开关，并选择需要防护的终端。



**入侵防护**

入侵中可以对威胁入侵行为的策略阈值进行自定义。系统在防暴力破解、端口扫描、CC攻击均有默认策略阈值。您可以根据不同服务器不同场景设置不同的防护阈值。

|  |  |  |
| --- | --- | --- |
| 功能 | 支持版本 | 描述 |
| 防暴力破解 | 专业版、高级版、旗舰版 | 防暴力破解功能通过在一段时间内禁止登录失败超过限定次数的用户登录，可有效防止您终端被暴力破解。 |
| 防端口扫描 | 高级版、旗舰版 | 防端口扫描功能通过在一段时间内扫描终端开放端口次数判定为恶意连接，封锁IP。 |
| 防CC攻击 | 旗舰版 | 防CC攻击功能通过在一段时间内禁止超过限定次数的连接IP，防止终端被CC攻击。 |

**网页防篡改策略**

网页防篡改可实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。

|  |
| --- |
| 网页防篡改功能为快卫士的增值服务，仅**旗舰版**用户可开通和使用该服务。免费版、专业版、高级版版用户需先升级到旗舰版才可使用网页防篡改功能。 |

**防护原理**

快卫士Agent通过自动化采集获取被保护的终端中写防护目录下文件的进程列表，实时识别异常进程和异常文件变动，并对导致异常文件变动的进程进行阻断，同时发送告警。

**使用限制**

1. 每台终端对应一条防护策略。
2. 每个被防护的目录大小不超过25G。
3. 使用网页防篡改功能前，需要确认终端的内核版本是否在快卫士兼容范围内，

|  |  |  |
| --- | --- | --- |
| 操作系统 | 操作系统版本号 | 内核版本号 |
| Windows（32位或64位） | Windows Server2003、 2008、2012、2016、2019和2022 | 所有版本。 |
| CentOS（64位） | 不限制，以支持的内核版本号为准 |  |
| Ubuntu（64位） | 不限制，以支持的内核版本号为准 |  |
| Debian | 不限制，以支持的内核版本号为准 |  |

**操作步骤**

1. 登录快卫士控制台。在上方导航栏选择**策略中心。**
2. 在左侧导航栏，选择**实时防护-》网页防篡改策略**。
3. 在**网页防篡改策略**页面，点击**添加终端防护**。
4. 在**添加终端防护策略**页签中完成以下配置。



1. 单击**保存。**

在防篡改策略列表中，单击目标服务器的**防护状态**开关，为该终端开启防护服务。



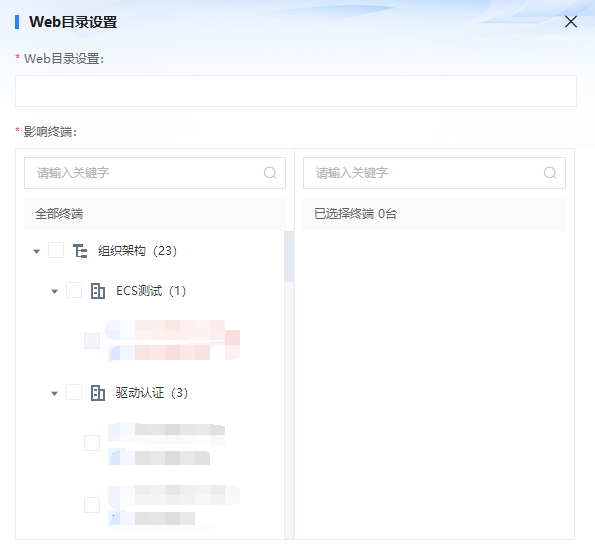
**Webshell防护策略**

网页中检测出Webshell（网站后门）文件，是黑客入侵网站和终端的第一步。如果入侵者通过执行命令，提升网站权限后，可以入侵终端，达到控制整台终端的目的。

|  |
| --- |
| Webshell防护功能为快卫士的增值服务，高级版、旗舰版用户可开通和使用该服务。免费版、专业版用户需先升级到高级版、旗舰版才可使用Webshell功能。 |

**操作步骤**

1. 登录快卫士控制台。在上方导航栏选择**策略中心。**
2. 在左侧导航栏，选择**实时防护-》Webshell防护策略**。
3. 在**Webshell防护策略**页面，点击**新增检查目录**，设置对应终端和检测目录地址**。**



**二次认证**

**微信绑定**

|  |
| --- |
| 辅微信仅支持远程登录终端管理，无法直接登录快卫士控制台管理。 |

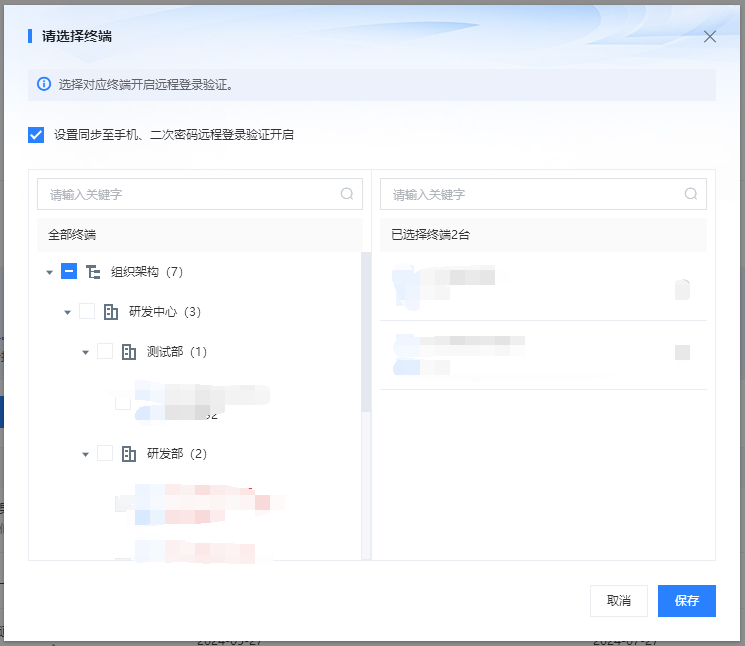
**操作步骤**

1. 登录**快卫士控制台**。在上方导航栏，选择**策略中心**。
2. 在左侧导航栏，选择**二次认证**。

该页面默认选择所有终端开启二次认证后远程登录需要身份验证，您可以根据实际场景设置一段时间内登录无需身份认证。

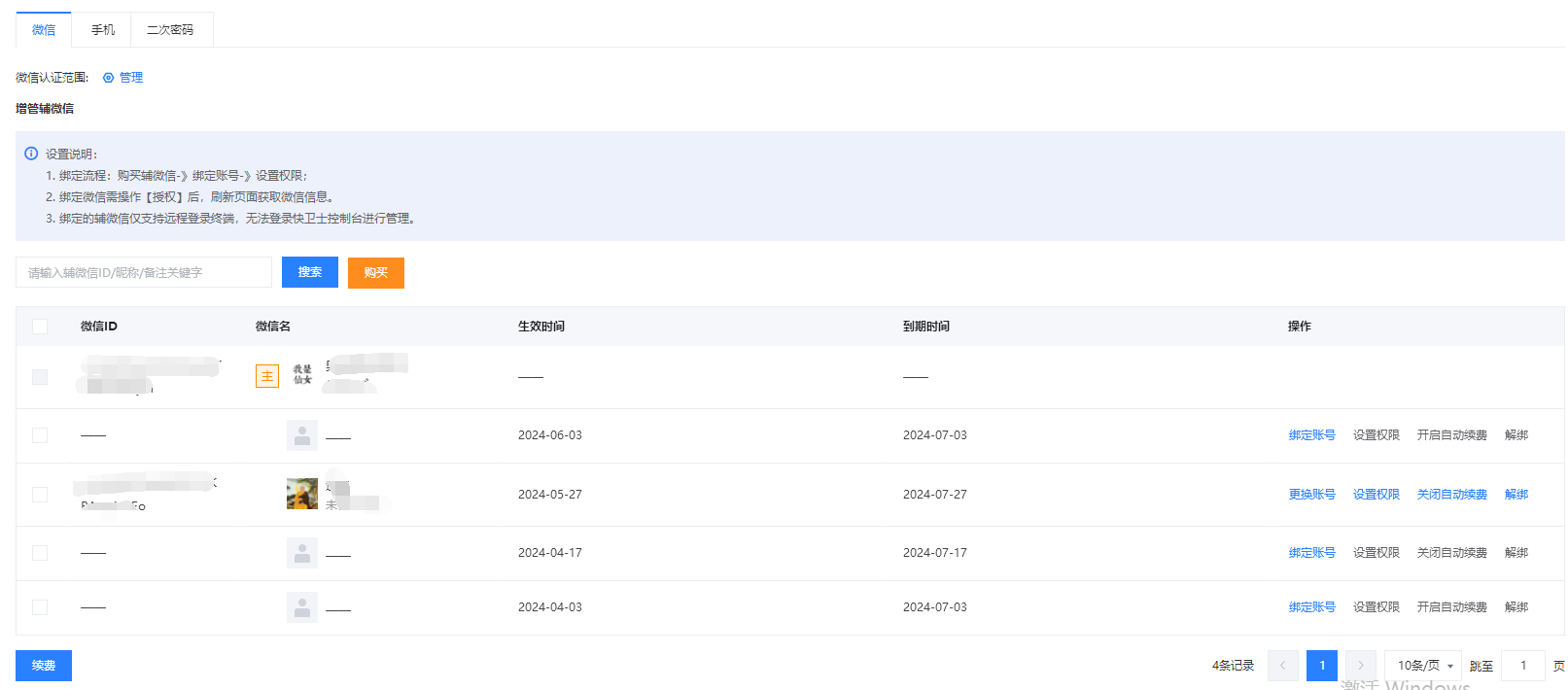


开启二次认证可选择覆盖终端的范围，建议所有终端均覆盖。只要在微信页面设置二次认证覆盖面，默认可同步至手机、二次密码远程登录验证的开启设置。

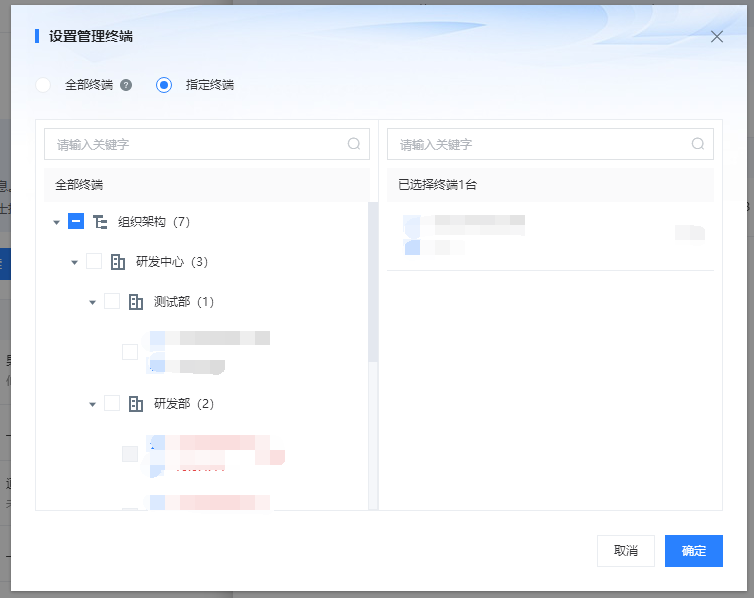


开启微信二次认证时，当账号下未绑定过主微信，可通过点击【绑定账号】进行微信扫一扫绑定。

主账号绑定后，若需要新增辅微信协助您管理终端，则可通过购买辅微信个数后绑定设置。



辅微信绑定成功后，页面自动弹出**设置权限**对话框，对辅微信进行权限设置。默认选择指定服务器，您可以指定辅微信能够远程管理的终端。您也可以根据您的使用场景给辅微信全部终端权限，后续账号下的终端新增删除不影响该辅微信的权限范围。



|  |
| --- |
| 为了避免辅微信到期未及时续费影响协助管理，建议您购买辅微信时勾选“到期自动续费”功能并保持账号下有足够的余额。 |

注：手机绑定、二次密码设置操作步骤与微信绑定相仿。

**合规基线**

|  |
| --- |
| 合规基线策略功能为快卫士的增值服务，仅高级版、旗舰版用户可开通和使用该服务。免费版用户需先升级到**高级版和旗舰版**可使用基线策略功能。 |

系统默认每天凌晨对账号下终端进行基线检测执行，若您的实际场景需要对该策略进行自定义设置，可通过合规基线策略调整。



**安全加固**

安全加固是一种虚拟防火墙，用于控制终端的入流量和出流量。具备状态检测和数据包过滤能力，您可以配置安全规则在云端划分安全区域。

|  |
| --- |
| 安全加固功能为快卫士的增值服务，仅**专业版、高级版、旗舰版**用户可开通和使用该服务。免费版用户需先升级到专业版、高级版、旗舰版才可使用安全防火墙功能。 |

**安全加固功能特性**

* 一台终端至少属于一个安全规则，可以同时加入多个安全规则。
* 一个安全规则可以管理多台终端。
* 安全规则默认访问策略：出入方向均允许所有访问请求，您可按需手动添加允许或拒绝策略的规则。
* 每条安全规则可配置2000条规则数。
* 规则优先级默认为1，您可进行修改。优先级数值越小，优先级越高。优先级范围为1~100。
* 支持协议：全部、TCP、UDP、ICMP。

**场景说明**

当两条安全规则的协议类型、端口范围、授权策略、授权对象都相关。则

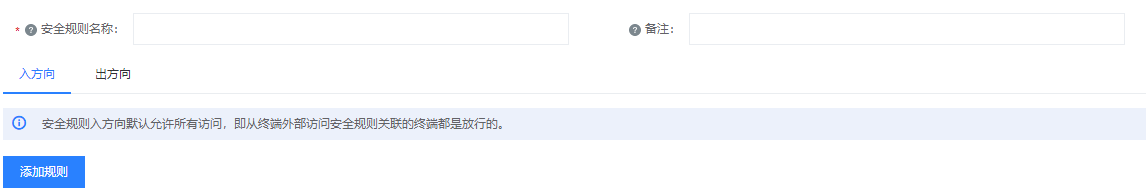
* 优先级相同：拒绝策略的规则优先生效，允许策略的规则不生效。
* 优先级不同：优先级搞的规则生效。

**安全规则建议**

* 不建议为每台终端单独设置一个安全规则，建议将具有相同安全保护需求的终端加入同一安全规则。
* 建议用户设置简洁的安全规则。如果给一台服务器分配了多个安全规则，有可能导致终端同时遵循数百条安全设置，设置变更都可能引起网络不通的故障。
* 添加安全规则时遵循最小授权原则。例如选择开放具体的端口，如80/80。不要设置为端口范围，如1/80，添加安全规则时，谨慎授权0.0.0.0/0（全网段）访问源。

**操作步骤**

1. 登录**快卫士控制台**。在上方导航栏选择**策略中心**。
2. 在左侧导航栏，选择**安全加固**。
3. 点击**创建安全规则**，填写安全规则名称及备注，同时直接开始添加安全规则条数。



1. 勾选对应**安全规则**即可点亮左下角删除，可对规则进行**删除**。但需注意，若规则中有绑定终端，则需要先将规则下的终端移除后方可删除成功。



1. 点击**安全规则**操作列表中**修改**，对安全规则名称和备注进行修改。



1. 点击**安全规则**操作列表中**管理终端**，可对安全规则进行终端的添加及移除。



1. 点击**安全规则**操作列表中**配置规则**，可对选择的安全规则进行规则设置。



**信任名单**

用户可以对于系统误判定为恶意程序或者恶意IP进行加入信任白名单，加入信任白名单的进程或者IP可以在白名单管理中进行管理。而对于误操作隔离查杀的进程也可在信任名单中进行进程恢复处理。

|  |
| --- |
| 信任名单的管理基于产品版本，免费版需要升级至专业版、高级版、旗舰版可以此使用信任名单功能。 |



**漏洞管理**

系统默认每天凌晨对账号下终端进行漏洞检测，您可根据您的实际场景对漏洞检测策略进行自定义设置。



**策略恢复**

|  |
| --- |
| 策略恢复功能为快卫士的增值服务，仅**高级版、旗舰版**用户可开通和使用该服务。免费版、专业版版用户需先升级到旗舰版才可使用策略恢复功能。 |

策略恢复可对快卫士控制台内的以下设置进行备份。

* 远程桌面保护
* 病毒查杀策略设置
* 防勒索防护策略
* 网页防篡改策略
* 安全加固策略
* 入侵防御策略
* 信任名单策略
* 安全报告-开关
* 二次认证-开关
* 通知

备份须知：

1. 以时间为节点，即下载的配置仅保存当时该账号下快卫士内资产的配置信息。
2. 备份配置保存后，若某台资产升级至高阶版本，则恢复配置时不包括后续的高阶版本配置信息。
3. 备份配置保存后，若某台资产降级至低阶版本，则恢复配置时不包括该资产原有的高阶版本配置信息。
4. 配置备份保存后，若某台资产删除，则恢复配置时不包括该资产原有的配置信息。
5. 恢复配置备份，防勒索策略的可恢复版本数需要重新备份后记录。
6. 恢复配置备份不包括文件隔离箱信息。

**威胁检测**

**病毒查杀**

病毒查杀功能是快卫士提供的病毒查杀处理方案，可有效清理终端上的各类恶意威胁。

**支持的扫描查杀的病毒类型**

勒索病毒、木马程序、蠕虫病毒、挖矿程序、钓鱼程序、黑客工具、溢出程序、恶意文件、广告程序、病毒种植程序、僵尸网络、漏洞利用程序、间谍软件、恶作剧病毒、hack工具程序、恶意软件、远程文件下载程序、键盘记录器程序。

|  |
| --- |
| 病毒查杀功能为快卫士的增值服务，仅**专业版、高级版、旗舰版**用户可开通和使用该服务。免费版用户需先升级到专业版、高级版、旗舰版才可使用病毒查杀功能。 |

**查杀方式**

快卫士病毒查杀包括快速查杀和全量查杀。快速查杀主要扫描系统盘中一些重要文件目录。全量查杀可以扫描终端所有硬盘的文件。

选择快速扫描，为了缩短扫描时长，您可以勾选需要扫描的范围。因为病毒启动后一定会有进程运行，所以运行中的进程是必扫内容，您可以根据您的场景，确认系统启动项和敏感目录是否一起扫描。



选择全量扫描，该扫描方式比较耗费时间，全磁盘病毒扫描最长4.5小时，同时病毒检测期间会占用终端一部分内存，建议您选择维护时段或者业务低谷期进行。

|  |
| --- |
| 快速查杀目录（Windows）:敏感目录（/Windows和/Windows/system32本级目录，/Windows /system32/drivers目录和其子目录）+启动项+运行中进程。  快速查杀目录（Linux）：敏感目录（/bin，/sbin，/usr/sbin，/usr/bin，/lib，/lib64， /usr/lib/usr/lib64，/usr/local/lib，/usr/local/lib64，/tmp，/var/tmp，/dev，/proc）+启动项+运行中进程。 |

**扫描模式**

选择极速、均衡、低耗主要区别在于CPU占用率情况。

极速：全速扫描，不限制扫描软件自身的CPU占用率。

均衡：默认项。扫描速度和CPU占用率达到一定平衡，限制CPU占用率不超过30%。

低耗：扫描时尽量少占用CPU资源，限制cpu占用率不超过10%。

**扫描病毒**

* 立即扫描

1. 登录**快卫士控制台**，在上方导航栏，选择**威胁检测**。
2. 在左侧导航栏，选择**病毒查杀**。
3. 在**病毒查杀**页面，点击**快速查杀**或**全量查杀**。
4. 在**选择终端**对话框，选择需要扫描的终端，然后单击**确定**。扫描完成时间根据终端文件量，请您耐心等待。扫描完成后，建议您及时查看并处理扫描结果。

* 定时扫描

通过点击病毒扫描策略设置系统自动病毒扫描时间，参考策略中心-》病毒查杀策略 描述。

**处理告警**

病毒扫描完成后，建议您及时处理病毒扫描所产生的告警，以确保您的终端不受恶意病毒的威胁。

1. 在**病毒查杀**页面，单击**立即处理**。
2. 在检测结果列表中定位到需要处理的告警，单击**操作**列的**立即处理**。如果需要同时处理多个告警，您可以选择需要处理的告警，单击**一键处理**。
3. 在请选择处理方式对话框中选择处理方式，然后单击**确认**。

|  |  |
| --- | --- |
| 处理方式 | 说明 |
| 隔离查杀 | 选择隔离查杀后，该程序无法执行"读/写"操作，同时该程序的进程将被立即终止并列入文件隔离箱中。 |
| 加入白名单 | 如果告警为误报，您可以将该进程加入白名单。进程加入白名单后，当再次发生相同异常时不再进行告警，请谨慎操作。 |
| 忽略 | 忽略本次处理，当发生相同异常时，将再次警告。 |

**漏洞查补**

快卫士支持对主流漏洞类型进行检测并提供一键修复功能。您可以通过快卫士定期自动扫描或一键手动扫描方式，检测终端资产的漏洞风险。漏洞查补功能可以帮助您更全面地了解并修复您资产中的漏洞风险。

漏洞查补功能支持的操作系统类型

|  |  |
| --- | --- |
| 操作系统类型 | 版本 |
| Windows Server | * Windows Server2003 * Windows Server2008 * Windows Server2012 * Windows Server2016 * Windows Server2019 * Windows Server2022 |
| Linux | * CentOS 6、7、8 * Ubuntu16、18、20、22 * Debian 11 * Alibaba Cloud Linux2.1903 LTS |

快卫士系统默认每天对您的终端进行自动扫描。若涉及到部分场景需要选择性自动扫描的终端，您可以在策略中心-》漏洞管理按业务配置。

**Windows系统漏洞**

|  |
| --- |
| 免费版、专业版支持漏洞扫描，漏洞修复功能仅针对**高级版、旗舰版**使用。 |

查看漏洞基本信息

1. 登录**快卫士控制台**。在上方导航栏选择**威胁检测**。
2. 在左侧导航栏，选择**漏洞查补**。
3. 在**漏洞查补**页面，单击**Windows系统漏洞**页签。
4. 在**Windows系统漏洞**页签下，查看和管理快卫士检测到的所有Windows系统漏洞信息。

您可以执行以下操作：

* 查看系统漏洞信息

您可在Windows系统漏洞页签下的漏洞公告列表中，查看检测出您终端需要修复的漏洞。



* 查看漏洞的修复紧急程度建议

漏洞的建议修复紧急度用不同颜色的图标表示，图标中的数据表示存在该漏洞所影响的终端数量。以下是图标颜色和漏洞修复紧急度的对应关系：

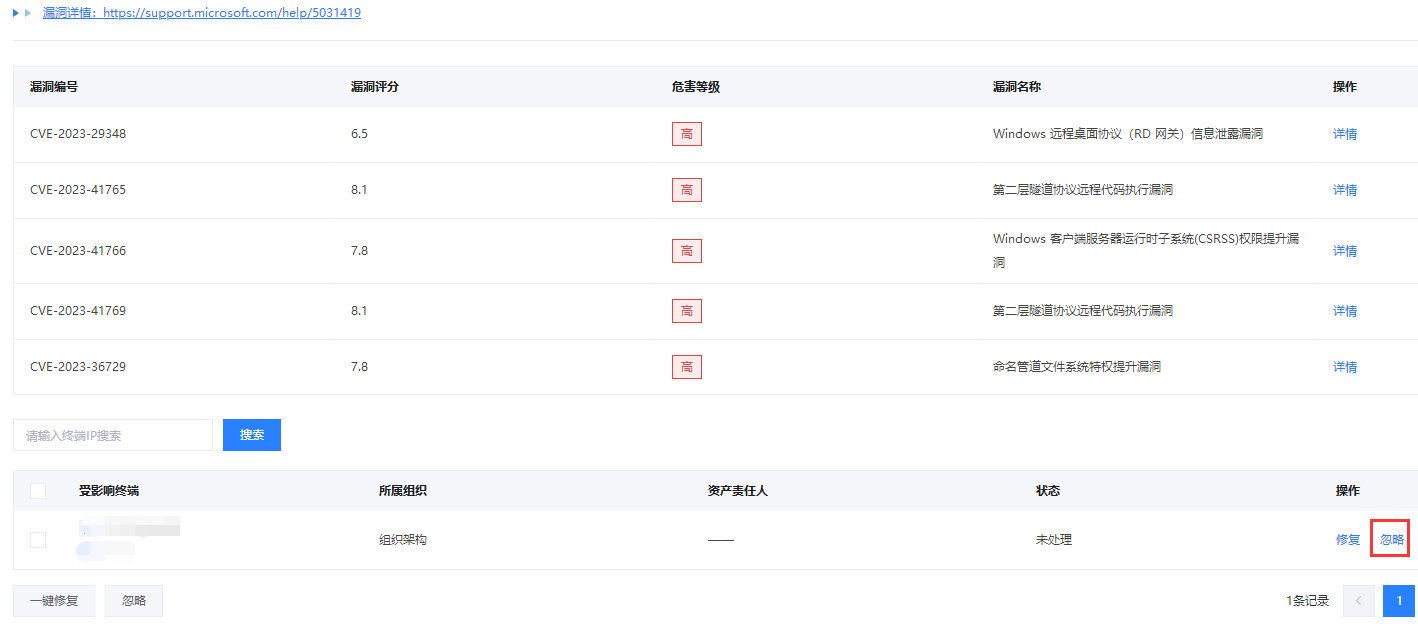
红色图标：表示漏洞修复紧急度为**高危**。

橙色图标：表示漏洞修复紧急度为**中危**。

灰色图标：表示漏洞修复紧急度为**低危**。

* 补丁管理

您可以在系统漏洞内嵌页中查看对应的漏洞详情和漏洞对应的受影响终端信息。您可以忽略漏洞，快卫士将不再对被忽略的漏洞进行告警。



忽略的漏洞会归档到补丁管理中。如需恢复快卫士对忽略漏洞的检测和告警提示，可在补丁管理页面中移除该漏洞。



* 搜索漏洞

您可以在Windows系统漏洞页签下，使用以下功能中的一个或者多个组合筛选或搜索目标漏洞：

通过漏洞修复的紧急程序（高危、低危）搜索漏洞。

输入漏洞编号搜索漏洞（漏洞编号支持模糊搜索）。



* 导出漏洞

您可在Windows系统漏洞页面，单击



图标，将快卫士检测到的对应列表中所有Windows系统漏洞导出并保存到本地。导出的文件为Excel格式。

* 查看漏洞详情和处理漏洞

1. 在**Windows漏洞公告**列表，单击**漏洞公告**或者对应操作栏的**修复**，可展开**漏洞详情**面板。您可以查看该漏洞的**漏洞详情**和**待处理漏洞数量**及待处理漏洞关联终端。
2. 在漏**洞详情**面板中，查看漏洞详情并处理漏洞。

您可以根据需要执行以下操作：

* 在漏洞详情页签下，查看该漏洞详情说明。在待处理漏洞页签下，直接跳至漏洞详情下的漏洞影响终端资产列表。您可以在漏洞影响的终端列表，查看该漏洞影响的所有终端、漏洞的状态等信息，并可对漏洞执行一键修复或忽略的操作。
* 查看漏洞详细状态。

修复成功：漏洞已执行一键修复并修复成功。

未修复：漏洞待修复。

修复中：漏洞正在修复处理中。

修复失败：漏洞修复失败，可能因为漏洞文件已被修改、漏洞文件已不存在、终端配置问题导致。

**Linux软件漏洞**

* 查看漏洞基本信息

1. 登录**快卫士控制台**。在上方导航栏，选择**威胁检测**。
2. 在左侧导航栏，选择**漏洞查补**。
3. 在漏洞查补页面，单击Linux软件漏洞页签。
4. 在Linux软件漏洞页签下的漏洞列表中，查看快卫士检测到的Linux软件漏洞关联的漏洞名称。

漏洞的建议修复紧急度用不同颜色的图标表示，图标中的数据表示存在该漏洞所影响的终端资产数量。以下是图标颜色和漏洞修复紧急度的对应关系：

红色图标：表示漏洞修复紧急度为**高危**。

橙色图标：表示漏洞修复紧急度为**中危**。

灰色图标：表示漏洞修复紧急度为**低危**。

* 补丁管理

您可以在漏洞名称面板中查看对应的漏洞详情和漏洞对应的受影响终端信息。您可以忽略漏洞，快卫士将不再对被忽略的漏洞进行告警。

忽略的漏洞会归档到补丁管理中。如需恢复快卫士对忽略漏洞的检测和告警提示，可在补丁管理页面中移除该漏洞。

* 搜索漏洞

您可以在Linux软件漏洞页签下，使用以下功能中的筛选或搜索目标漏洞：

通过漏洞修复的紧急程序（高危、中危、低危）搜索漏洞。

输入漏洞名称、编号、服务器IP搜索漏洞（支持模糊搜索）。



* 导出漏洞

您可在Linux系统漏洞页面，单击



图标，将快卫士检测到的对应列表中所有Linux系统漏洞导出并保存到本地。导出的文件为Excel格式。

* 查看漏洞详情和处理漏洞

1. 在**Linux软件漏洞**列表，单击漏**洞名称**或者对应操作栏的**查看**，可展开**漏洞详情**面板。您可以查看该漏洞的漏**洞详情**和**受影响终端**信息。
2. 在**漏洞详情**面板中，查看漏洞详情并根据修复建议进行手动修复漏洞。

**合规基线**

合规基线功能针对终端操作系统进行安全检测，并提供检测结果说明和加固建议。基线检查功能可以帮您进行系统安全加固，降低入侵风险并满足安全合规要求。

快卫士的基线检测功能支持检测操作系统的弱口令、账号权限、身份鉴别、密码策略、访问控制、安全审计和入侵防范等安全配置，并提供检测结果，针对存在的风险配置给出加固建议。

|  |
| --- |
| 合规基线功能为快卫士的增值服务，仅高级版、旗舰版用户可开通和使用该服务。免费版和专业版用户需先升级到**高级版和旗舰版**可使用合规基线功能。 |

**执行基线检测**

前提条件：您已购买快卫士高级版，仅高级版、旗舰版支持基线检测功能。

**基线检测方式**

快卫士基线检测功能支持周期性自动检测和即时手动检测。

周期性自动检测：快卫士默认每天凌晨2点自动执行基线检查。

即时手动检测：您可以在基线检测页面进行立即检查，实时查看终端资产中是否存在对应的基线风险。

**即时手动检测步骤**

1. 登录**快卫士控制台**。在上方导航栏，选择**威胁检测**。
2. 在左侧导航栏选择**合规基线**。
3. 点击**立即检查**，选择需要检测的终端资产执行。
4. 在基线检查结果列表中查看具体的基线风险项



**周期性自动检测步骤**

通过设置合规基线策略进行自定义周期性自动检测。参考策略中心-》合规基线。

**网页防篡改**

网页防篡改可实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。

|  |
| --- |
| 网页防篡改功能为快卫士的增值服务，仅**旗舰版**用户可开通和使用该服务。免费版、专业版、高级版版用户需先升级到旗舰版才可使用网页防篡改功能。 |

**防护原理**

快卫士Agent通过自动化采集获取被保护的终端中写防护目录下文件的进程列表，实时识别异常进程和异常文件变动，并对导致异常文件变动的进程进行阻断，同时发送告警。

**正常进程加入白名单防止被拦截**

您可以在快卫士控制台的**威胁检测-》网页防篡改**页面的告警列表中，查看快卫士检测出的异常文件变动告警、异常进程和该进程尝试写文件的次数。如果您确定改异常文件相关的进程是正常的业务，可将该进程添加到白名单中。网页防篡改功能不再对加入到白名单中的进程进行拦截。

**限制条件**

* 每台终端对应一条防护策略。
* 每个被防护的目录大小不超过25G。

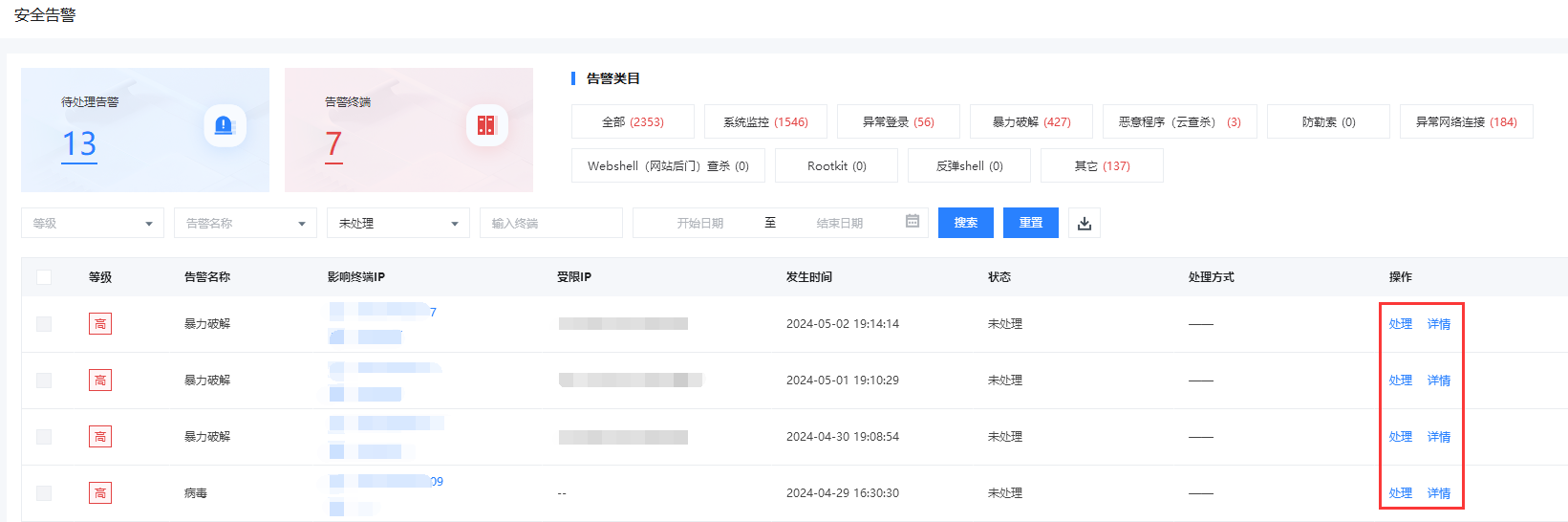
网页防篡改策略设置，参考策略中心-》实时防护-》网页防篡改策略。

**告警与响应中心**

|  |
| --- |
| 对于上锁的功能为快卫士的增值服务，仅**专业版、高级版旗舰版**用户可开通和使用该服务。免费版用户需先升级到专业版、高级版、旗舰版才可使用对应告警功能。 |

**处理告警事件**

1. 登录**快卫士控制台**。在上方导航栏，选择**告警与响应中心**。
2. 在左侧导航栏，选择**安全告警**。
3. 在**安全告警事件**页面，定位到目标告警事件，单击操作列的**详情**或者**处理**。



点击上方导航栏“告警与响应中心”模块的数字，页面自动切换至该页面并筛选出待处理的告警信息。



**日志报表**

**安全报告**

快卫士支持订阅安全周报，展现每周的终端资产安全趋势以及关键安全事件与风险，以满足等保测评以及审计的需要。

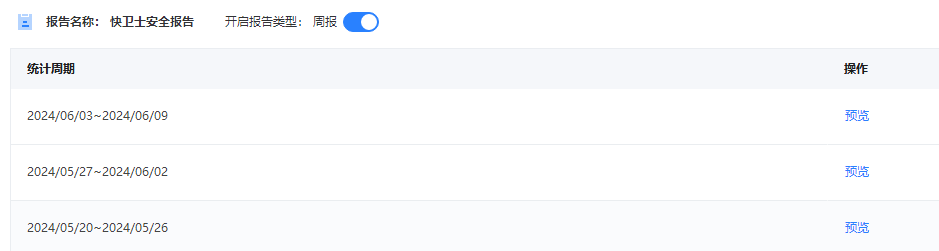
|  |
| --- |
| 安全报告功能为快卫士的增值服务，仅**高级版和旗舰版**用户可开通和使用该服务。免费版、专业版用户需先升级到高级版、旗舰版才可使用安全报告功能。 |

**操作步骤**

1、登录快卫士控制台。在上方导航栏，选择**日志报表**。

2、在左侧导航栏，选择**安全报告**。

安全报告默认关闭，您可以根据需要开启报告，系统会按照周统计方式向您推送。



**操作日志**

当您登录快卫士控制台，所有进行的编辑操作均在此模块中显示。修改记录实时生成，无法删除。您可根据时间、终端IP或操作关键字搜索。



**日志分析**

快卫士日志分析功能为您提供准确实时的日志查询和日志分析能力。

日志分析会为您自动创建快卫士的专属日志库，您可以在快卫士控制台查看专属日志库信息。

|  |
| --- |
| 日志功能为快卫士的增值服务，仅旗舰版用户可开通和使用该服务。免费版、专业版、高级版用户需先升级到**旗舰版**可使用日志分析功能。 |

**日志类别及字段说明**

日志分为安全日志、终端日志。

安全日志，包括漏洞日志、基线日志、恶意文件检测日志、安全告警日志。

终端日志，包括登录流水日志、暴力破解日志、客户端事件日志（客户端的状态变更事件）。

**日志分类**

1. **安全日志**

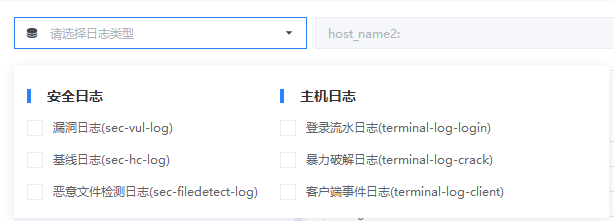
|  |  |  |  |
| --- | --- | --- | --- |
| 日志类型 | \_topic\_ | 快快字段 | 字段说明 |
| 漏洞日志 | sec-vul-log | loophole\_data | linux漏洞扩展信息 |
|  |  | saas\_instance\_id | Agent实例ID |
|  |  | host\_ip | 资产的公网IP |
|  |  | host\_ip\_lan | 资产的私网IP |
|  |  | computer\_name | 主机名称 |
|  |  | vul\_name | 漏洞名称 |
|  |  | operation | 操作（新增<new>、忽略<ignore>、修复<fix>） |
|  |  | repair\_status | linux修复状态 ，取值：   * 1->已修复 * 2->待修复 * 3->完成修复待重启 * 4->修复中 * 5->修复失败, * 6,7已被占用不可定义， * 8=Linux Ubuntu的修复包需要升级到Ubuntu 专业版方可使用   windows修复状态，取值：   * -1未知 * 1未安装， * 2已安装， * 3已忽略， * 4安装失败， * 5正在修复 * 6下载成功 * 7下载失败 * 8修复成功需要重启且已经重启 |
|  |  | created\_at | 开始时间戳，单位秒， 也用于表示事件发生的时间。 |
| 基线日志 | sec-hc-log | title | 检查项名称 |
|  |  | level | 基线检查项风险   * 1-低 * 2-中 * 3-高 |
|  |  | saas\_instance\_id | Agent实例ID |
|  |  | operation | 操作，取值：   * new：新增。 * verity：验证。 * ignore：忽略。 |
|  |  | strategy\_name | 基线策略名称 |
|  |  | status | 状态 ，取值：   1. 0-未处理 2. 1-已处理 3. 2-已处理不显示 |
|  |  | created\_at | 开始时间戳，单位秒， 也用于表示事件发生的时间。 |
| 恶意文件检测日志 | sec-filedetect-log | event\_id | 告警ID |
|  |  | event\_name | 告警名称 |
|  |  | md5 | 文件的MD5值 |
|  |  | result | 检测结果，取值：   * 0：文件安全。 * 1：存在恶意文件。 |
|  |  | file\_path | 文件路径 |
|  |  | level | 1：低 2：中 3：高 |
|  |  | created\_at | 开始时间戳，单位秒， 也用于表示事件发生的时间。 |
| 安全告警日志 | sec-security-log | type | 数据源，取值：  1 => '暴力破解',// 暴力破解 高  2 => '端口扫描',// 异常网络连接 中  3 => 'CC攻击',//异常网络连接 高  4 => '恶意进程（云查杀）',//恶意程序（云查杀） 高  5 => '勒索病毒', //防勒索 高  6 => '木马程序(windows)',//恶意程序（云查杀） 高  7 => '蠕虫',//恶意程序（云查杀） 高  8 => '恶意广告',//恶意程序（云查杀） 中  9 => '黑客工具',//恶意程序（云查杀） 高  10 => '溢出程序',//恶意程序（云查杀） 高  11 => '恶意文件',//恶意程序（云查杀） 高  12 => 'CPU告警',//信息收集 低  13 => '内存告警',//信息收集 低  14 => '网络下载速率告警',//信息收集 低  15 => '网络上传速率告警',//信息收集 低  16 => '系统盘容量不足告警',//信息收集 低  17 => '非法登录告警',//异常登录 高  18 => '异常位置登录告警',//异常登录 高  19 => 'Agent异常关机',//其他 低  21 => '异常账号登录告警',//异常登录 中  // 22 => '网页防篡改',// 无分类  23 => '病毒',// 恶意程序（云查杀） 高  24 => '溢出攻击',// 异常网络连接 高  25 => '主机重启告警',// 其他 中  26 => '广告程序',// 恶意程序（云查杀） 高  27 => '病毒种植程序',// 恶意程序（云查杀） 高  28 => '僵尸网络',// 恶意程序（云查杀） 高  29 => '勒索病毒',// 恶意程序（云查杀） 高  30 => '漏洞利用程序',// 恶意程序（云查杀） 高  31 => '间谍软件',// 恶意程序（云查杀） 高  32 => '恶作剧病毒',// 恶意程序（云查杀） 高  33 => '蠕虫病毒',// 恶意程序（云查杀） 高  34 => 'hack工具程序',// 恶意程序（云查杀） 高  35 => '恶意软件',// 恶意程序（云查杀） 高  36 => '远程文件下载程序',// 恶意程序（云查杀） 高  37 => '木马程序(linux)',// 恶意程序（云查杀） 高  38 => '挖矿程序',// 恶意程序（云查杀） 高  39 => '盗号钓鱼程序',// 恶意程序（云查杀） 高  40 => '键盘记录器程序',// 恶意程序（云查杀） 高  41 => '恶意进程自动防御',// 恶意程序（云查杀） 高  42 => 'Webshell拦截',// Webshell拦截 高  43 => 'RootkitAlarm',// Rootkit检测 高  44 => '反弹shell',// 反弹shell 高  45 => 'Agent自适应防护',// 高 |
|  |  | input | 告警详情。  说明：告警类型不同，detail字段包含的内容也不同。 |
|  |  | saas\_instance\_id | Agent实例ID |
|  |  | host\_ip | 资产的公网IP |
|  |  | host\_ip\_lan | 资产的私网IP |
|  |  | level | 告警等级： 1：低 2：中 3：高 |
|  |  | name | 告警名称 |
|  |  | created\_at | 开始时间戳，单位秒， 也用于表示事件发生的时间。 |
|  |  | user\_id | 用户id |
|  |  | host\_id | 服务器id |

1. **主机日志**

|  |  |  |  |
| --- | --- | --- | --- |
| 日志类型 | \_topic\_ | 快快字段 | 字段说明 |
| 登录流水日志 | terminal-log-login | saas\_instance\_id | 实例ID |
|  |  | host\_ip | 服务器的IP地址 |
|  |  | login\_ip | 登录服务器的IP地址 |
|  |  | port | 登录服务器的端口 |
|  |  | login\_type | 登录方式： 1.普通密码 2.微信二维码 3.手机验证码 4.二次密码 5.备用密码 |
|  |  | username | 控制台用户名 |
|  |  | created\_at | 开始时间戳，单位秒， 也用于表示事件发生的时间。 |
|  |  | user\_id | 用户id |
|  |  | host\_id | 服务器id |
|  |  | host\_ip\_lan | 私网ip |
|  |  | name | 计算机名 |
| 客户端事件日志（客户端的状态变更事件） | terminal-log-client | host\_ip | 服务器IP地址 |
|  |  | agent\_version | 客户端版本 |
|  |  | system\_type | 系统类型  1-windows  2-linux |
|  |  | client\_status | 客户端状态：  1是正常 ， 2是错误， 3是停止， 4是静默， -1是未安装， -2是卸载 |
|  |  | created\_at | 开始时间戳，单位秒， 也用于表示事件发生的时间。 |

**操作步骤**

1. 登录快卫士控制台-》日志报表-》日志分析。
2. 选择需要查询的日志类别



1. 在选定的日志类别中选择希望筛选的字段



1. 默认选择相对时间15分钟内的信息，您可以在调整时间筛选。



1. 为了方便您的使用，您也可以通过设置自动刷新时间进行系统信息自动更新。

**用户中心**

**用户账号**

当您作为企业管理者，您可以通过用户账号模块进行管理子账号。当子账号信息较多时，在子账号列表中可通过用户名、姓名或备注信息进行搜索。

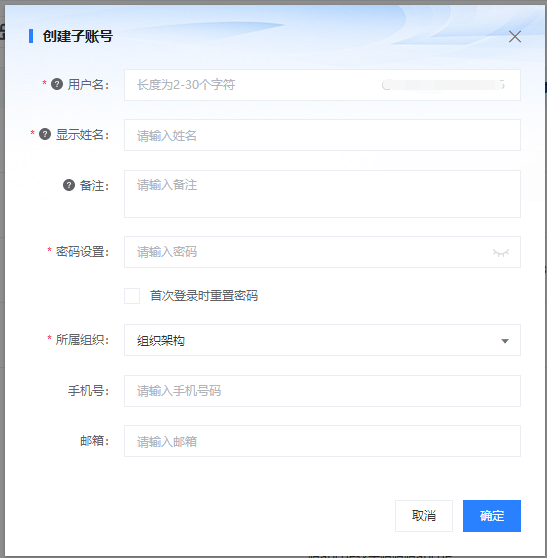


* **新增子账号**

通过列表点击**创建子账号**按钮



在创建子账号弹窗中根据您的实际场景输入子账号信息：用户名、显示姓名、备注、密码设置、首次登录时重置密码、所属组织、手机号、邮箱。



|  |
| --- |
| **用户名**：长度为2-30个字符，格式为英文字母、数字，可包含特殊字符中的点号（.）、下划线（\_）、连字符（-）和半角冒号（:）  **显示姓名**：最多包含30个字符  **备注**：长度不大于300字符  **密码设置安全指标**：   * 8-32个字符 * 包含大、小写字母、数字、符号 * 至少包含2种 |

**子账号密码策略设置**

若需要对子账号密码的设置有要求，可通过子账号密码设置策略功能执行。



**子账号分配角色**

若您设置的子账号需要协助您进行管理，您可以赋予子账号角色权限。



|  |
| --- |
| 若选择多个角色，该子账号的权限为多个角色相叠加。 |

角色权限您可参考用户中心-》角色权限。

**组织架构**

企业管理员可以查看和管理组织中的部门信息。组织架构树后的数字代表该节点的分支及分支成员数量。

选择**组织架构**树根节点，并点击**新建分支**按钮，可创建一级分支节点。



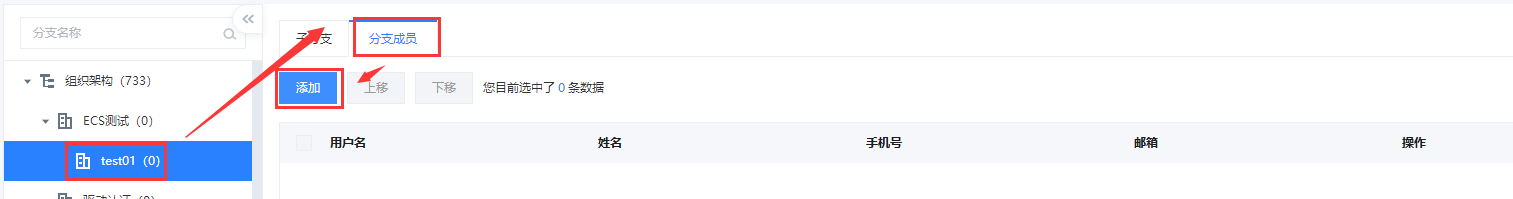
若您的一级分支节点需要有下级节点时，您只需要选择对应的一级分支节点进行新建分支。



为了方便您的管理，您的分支可进行排序操作。



每个分支若有对应的成员，您可以选择**组织架构树**的**分支节点**，在**分支成员页签**中，**添加**成员。成员信息取自于您建立的子账号信息。



在分支成员页签中，您可以对分支成员进行排序、删除、分配角色操作。

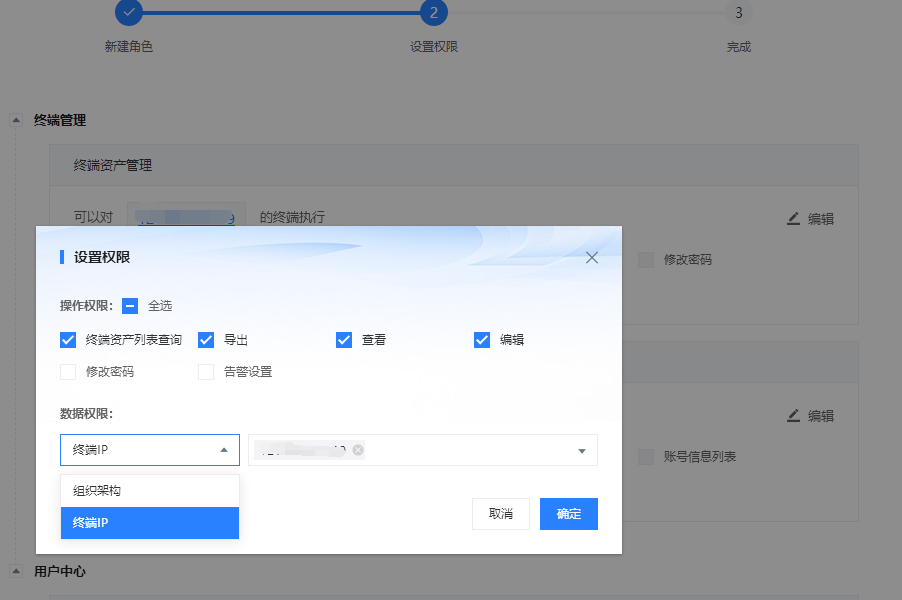


**角色权限**

该功能支持对企业角色赋予功能权限设置。在角色权限列表中，您可以通过关键字进行模糊搜索角色信息。

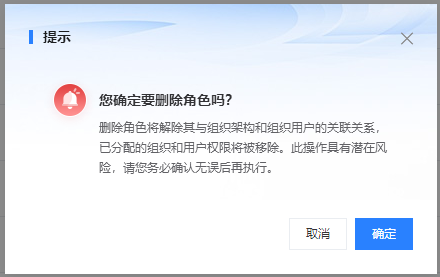


在角色权限页面中，您可以对角色进行增编管理。对于数据权限的设置，您可以指定终端IP生效，也可以指定组织架构层级生效。



角色的删除

当角色有被赋予组织架构或者用户的关联关系时，删除操作具有潜在风险，建议您确认无误后执行。



**系统管理**

**部署安装**

安装说明详见：[安装手册](https://cex1rtlpay.feishu.cn/wiki/OGSBwefhZi77Vvk56lLcwi2Fn8f?from=from_copylink)

卸载说明详见本文档中接入快卫士-》卸载Agent。

**账号安全**

该功能支持您对登录快卫士控制台账号的安全设置，包括账号密码策略、账号登录保护等。

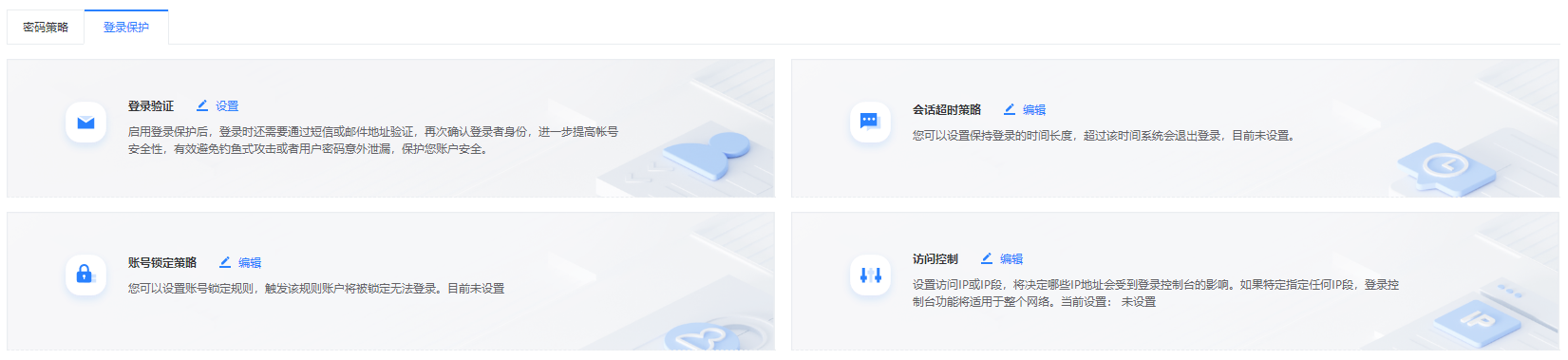
**密码策略**

通过对密码字符种类、长度、有效期进行设置。

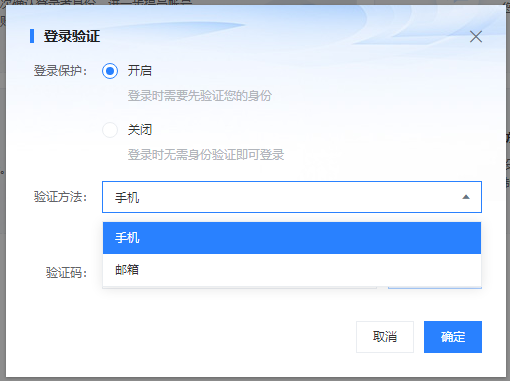


**登录保护**

通过对账号登录保护的4种方式进行设置。



* 登录保护包括登录快卫士控制台时的登录验证，该登录验证支持手机或者邮箱接收验证码来确认。



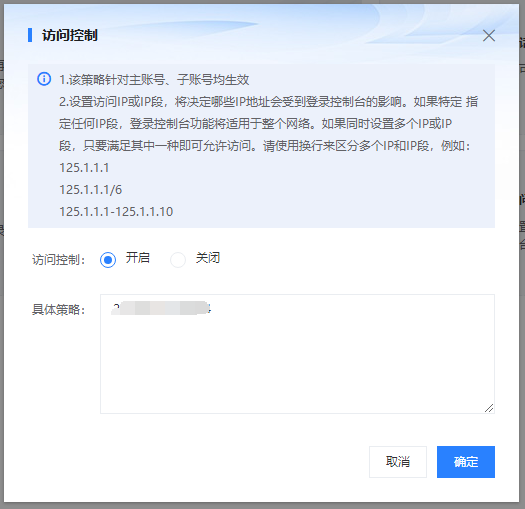
* 可以通过登录控制台的时长设置，超过该时间控制台将自动执行账号退出操作。



* 可以通过设置账号锁定规则，来达到账号安全的目的。



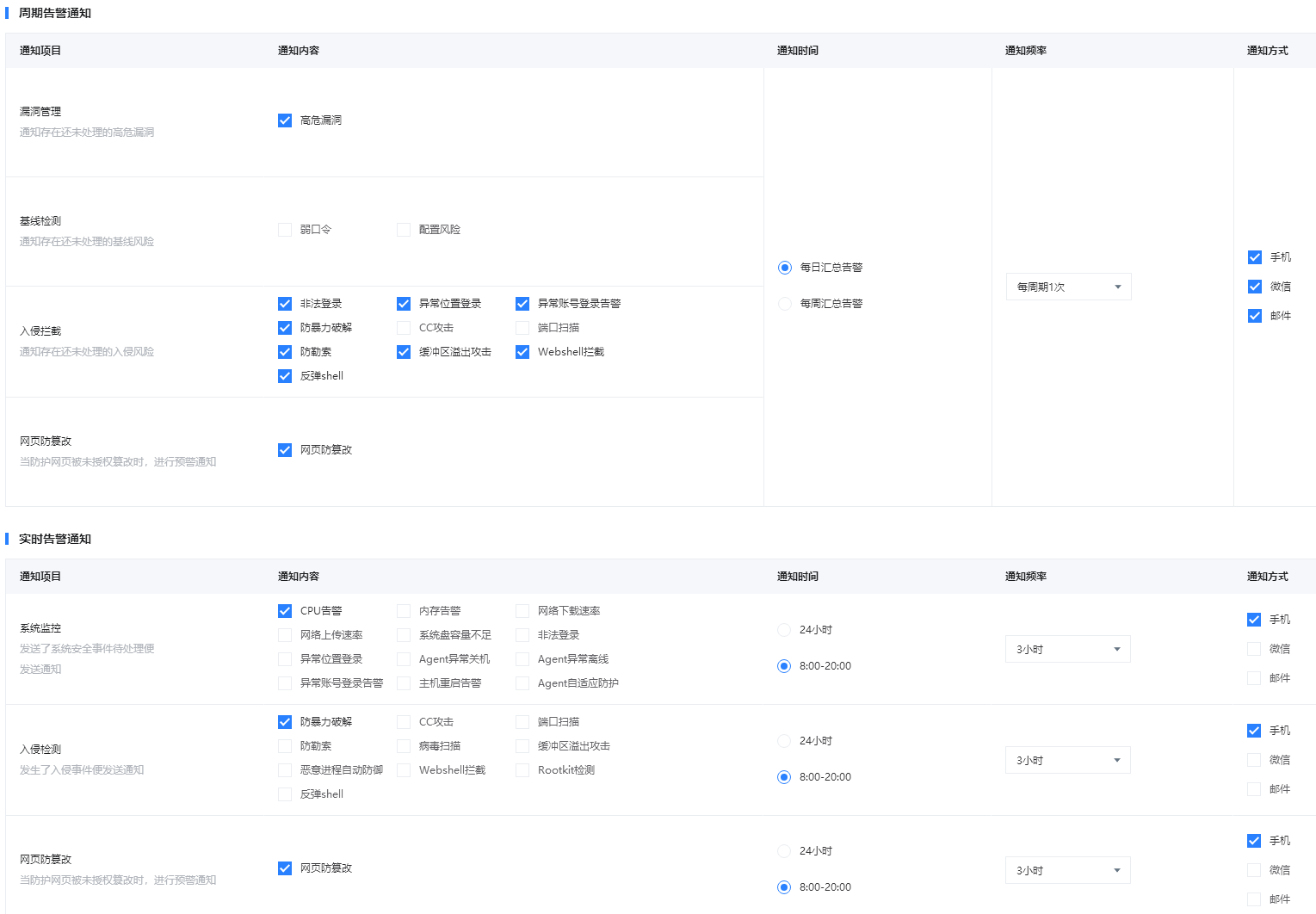
* 通过设置登录访问IP/IP段来限制非符合条件的登录。



**通知设置**

您可对事件的通知内容、通知时间、通知方式进行操作，通知方式包括手机、微信、邮件、飞书机器人、钉钉机器人、企业微信机器人，微信/短信/邮件通知方式默认全部选择，通知时间默认24小时。您可根据自己的使用场景进行选择。若您选择通知时间为8:00-20:00，则在这之外的时间出现的异常情况不再进行通知。

|  |
| --- |
| 微信/短信/邮件通知限制说明：   * 若您未绑定手机、邮箱，则无法常进行三通道提醒。 * 当前告警通知默认发送账号联系人。 * 每个联系人每天最多接收5条告警。请到 快卫士控制台-》告警与响应中心 中查看全量日志。 * 告警通知有可能被当成垃圾信息而拦截，如未收到告警通知，请确认是否被拦截。 |

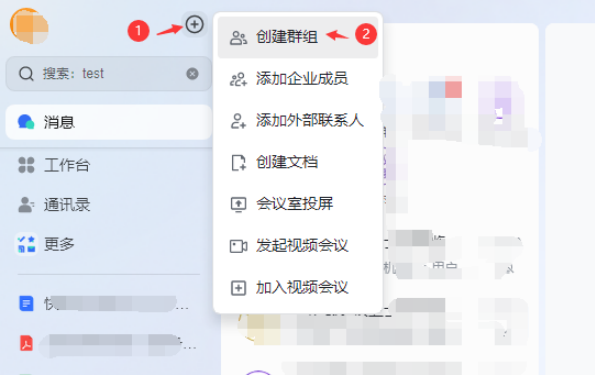


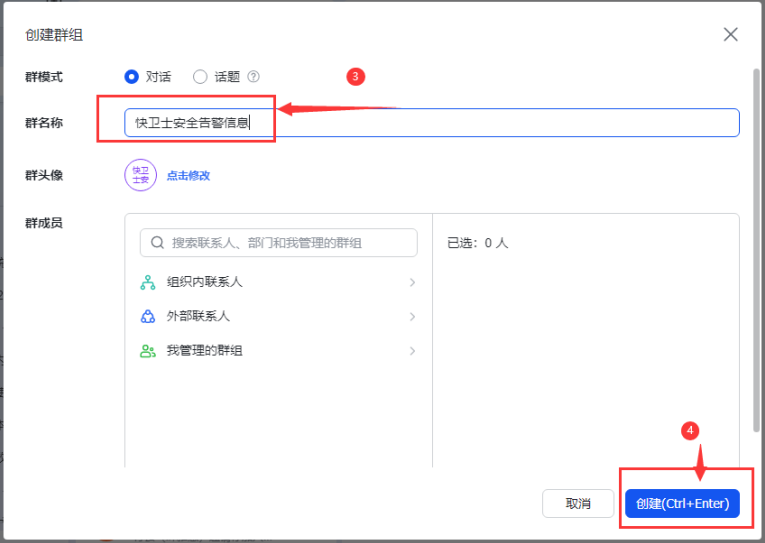
**飞书机器人设置**

|  |
| --- |
| * 飞书机器人仅针对专业版、高级版、旗舰版本主机进行告警信息的发送。 * 每个飞书群每分钟最多接收10条告警。 |

设置步骤：

1. 登录飞书创建群组





1. 添加机器人

进入群聊-》设置



1. 群机器人-添加机器人



1. 添加自定义机器人



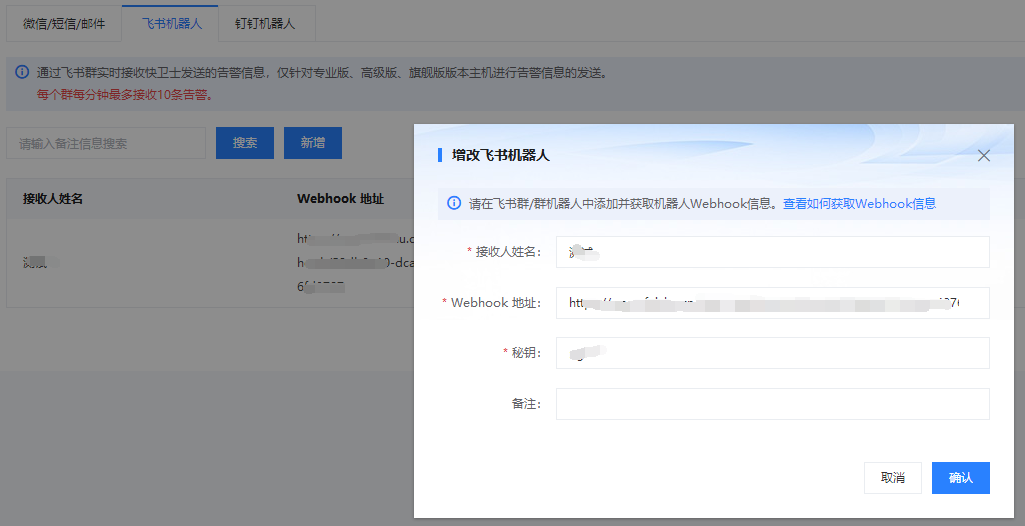


1. 点击“复制”，复制出Webhook链接。并在安全设置区中设置对应需要校验的【秘钥】信息。



1. 到快卫士控制台-通知-飞书机器人进行设置：

将刚刚复制的Webhook链接，黏贴到“Webhook地址”栏中，并填写好秘钥、接收人姓名、备注等信息。点击“确认”，并发送检测消息后，设置完成。

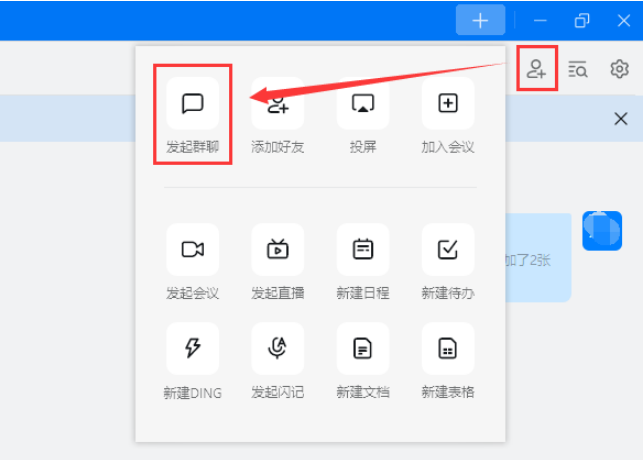


**企业钉钉机器人设置**

|  |
| --- |
| * 钉钉机器人仅针对专业版、高级版、旗舰版本主机进行告警信息的发送； * 每个钉钉群每分钟最多接收10条告警。 |

设置步骤：

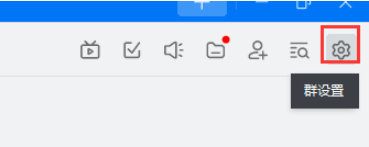
1. 登录钉钉创建群聊





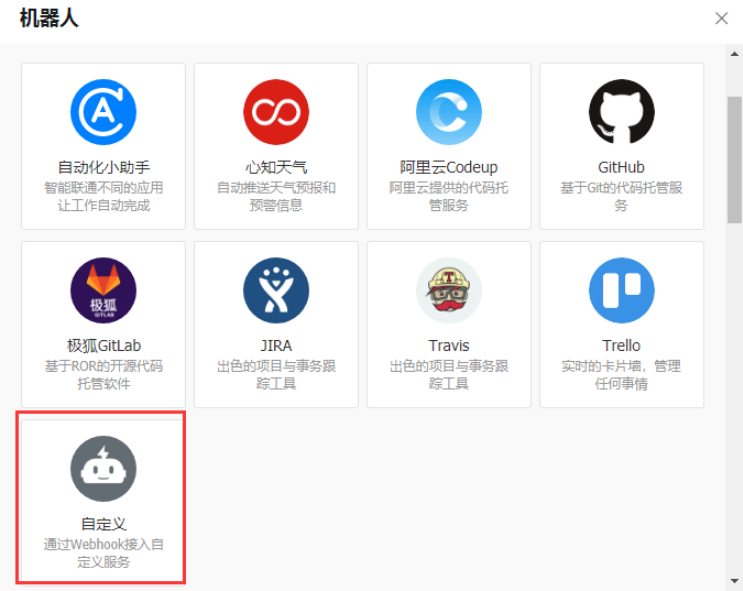
1. 添加机器人

进入群聊-》设置



1. 群机器人-》添加机器人





1. **必须要设置：安全设置**。参考下图设置

机器人名字：快卫士告警

安全设置：请选择“加签”

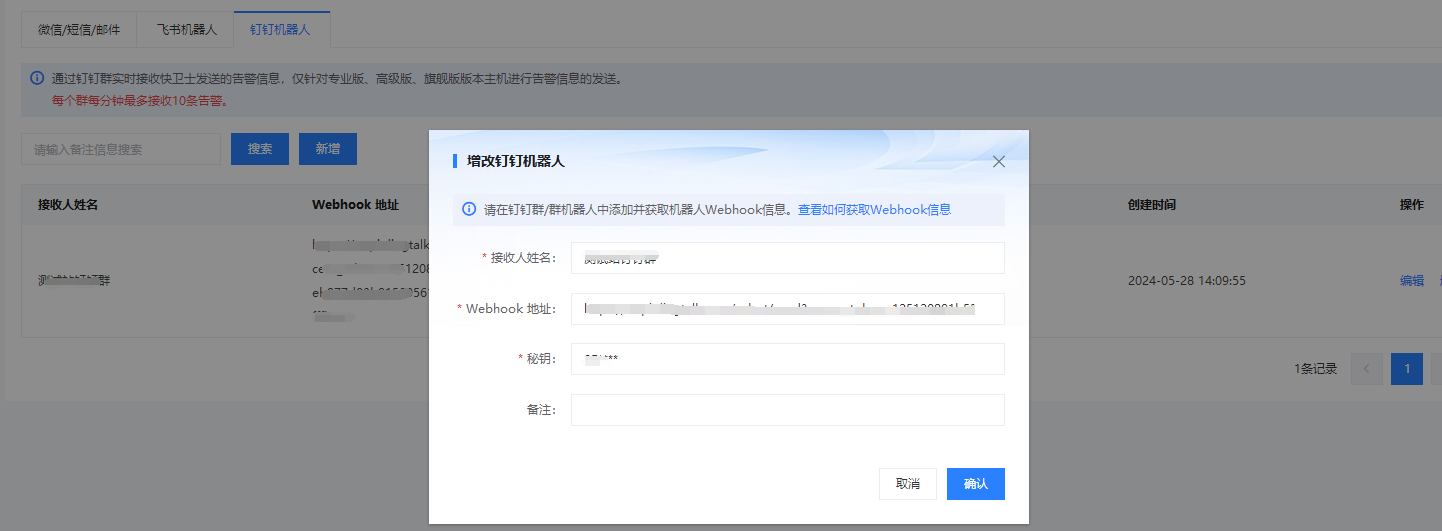


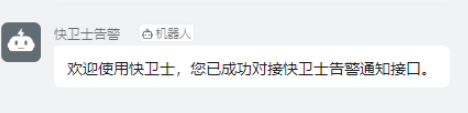
1. 添加完成后,点击 “复制” 复制链接



6、到快卫士控制台-》通知-》钉钉机器人进行设置：

将复制的Webhook链接，黏贴到“Webhook地址”栏中，将复制的加签链接，黏贴到“秘钥”栏中，并填写好接收人姓名、备注等信息。点击“确认”，并发送检测消息后，设置完成。



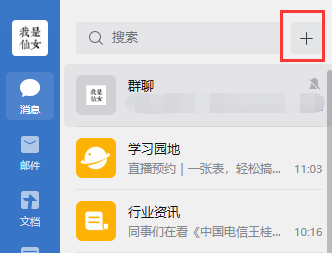


**企业微信机器人设置**

|  |
| --- |
| * 企业微信机器人仅针对专业版、高级版、旗舰版本主机进行告警信息的发送； * 每个企业微信群每分钟最多接收10条告警。 * 企业微信机器人不支持企业微信外部群。 |

设置步骤：

1. 登录企业微信创建群聊，选择联系人后创建



1. 添加机器人。进入群聊-》设置-》消息推送。

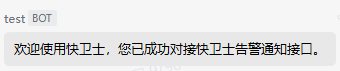


1. 添加自定义消息推送。填写名称和简介内容，复制Webhook地址内容。

|  |  |
| --- | --- |
|  |  |

1. 到快卫士控制台-》通知-》企业微信机器人进行设置：

将复制的Webhook链接，黏贴到“Webhook地址”栏中，并填写好接收人姓名、备注等信息。点击“确认”，并发送检测消息后，设置完成。



**相关协议**

[快卫士服务等级协议（SLA）](https://cex1rtlpay.feishu.cn/docx/XD2IdMDM1o6Sf1xC08vcSSjAnEd?from=from_copylink)