火绒安全
HUORONG SECURITY

企业版

常见问题解答

火绒企业版 V2.0 >>>

公　司：北京火绒网络科技有限公司
地　址：北京市朝阳区红军营南路 15 号瑞普大厦 D 座 4 层
网　址：https://www.huorong.cn
电　话：400-998-3555

版权声明

目录 | CONTENTS

1. 火绒终端安全管理系统 2.0 常见 Q&A

（常见问题较多，在使用过程中可使用 Ctrl+F 对关键字进行搜索。）

1.1 安装部署类

Q：安装中心后配置工具提示端口冲突如何解决？

A：打开火绒配置工具，更改“终端部署端口”对应的端口号，点击“保存”按钮即可。1024 之前可能为系统端口，建议修改大于 1024 的端口号。

Q：火绒支持几种部署方式，分别是什么？

A:

- 网页访问部署：客户机浏览器地址栏访问控制中心 IPv4 地址、IPv6 地址，点击下载客户端，双击安装即可。
- 共享安装：将下载的客户端安装包拷贝到共享目录，复制到各个用户机器，双击安装即可。
- 域部署工具：具体使用方法详见管理工具下载页面使用文档。
- 三方桌管推送：如有第三方桌面管理软件，可推送火绒客户端安装包，推送时携带静默安装参数/S。

Q：如果我个人版加了密码，用域部署工具还能推送安装吗？

A：可以的，会把个人版卸载了然后关机加重启。

Q:安装客户端提示“连接失败，需要输入控制中心 IP 地址和端口”该如何解决?

A：出现此问题可能有两种原因：

1.客户端与控制中心网络环境无法正常通讯

2.客户端安装包名称不正确

对应解决方案：

1.排除网络故障，保证客户端可以和控制中心网络环境正常通讯

2.正确安装包名称应为 installer(https_中心 IPv4 地址:终端部署端口).exe;

正确示例：installer(https_192.168.1.100:8080).exe

如安装包从回环地址 http://localhost/或 http://127.0.0.1/下载则需将安装包名称修改为实际地址。或通过浏览器访问控制中心实际地址，下载新包即可。

Q:个人版能否升级为企业版客户端?

A: 不能升级为企业版，且个人版与企业版客户端不能共存，安装企业版需卸载个人版重启后再安装企业版。

Q：刚安装完成，控制中心的账号和密码是什么

A：账号和密码默认均是 admin ，初次登录后需将密码修改为强口令。

Q：域部署推送安装后无反应是为什么?

A：排查方法如下

登录脚本：

检查被勾选终端是否具有域管理员权限，确认是域中否有其它组策略限制安装软件，终端如有 UAC 限制，手动输入管理员账户密码进行安装。

开机脚本：

- 检查域目录 NETLOGON 中是否存在 hrInst.exe 程 序以及 hrsetup.bat 批处理
- 检查域目录 SYSVOL\scripts 目录中是否存在 hrInst.exe 程序以及 hrsetup.bat 批处理
- 检查创建的 GPO 所对应的唯一 ID 目录中是否存在导出的安装脚本
- 打开 server 系统管理工具{Active Directory 用户和计算机}，检查链接 GPO 的分组中是否存在计算机（开机脚本针对计算机单位生效，如分组中无计算机，开机脚本不生效）

1.2 产品使用类

Q：刚安装完成，控制中心的账号和密码是什么？

A： 账号和密码默认均是 admin 。

Q：安装好企业版客户端，提示“安全服务异常，无法启动”如何解决？

A：

- 如果您之前安装过火绒个人版/火绒企业版 1.0/2.0，将其卸载后没有重启电脑，紧接着又装了企业版客户端，则会出现该问题，这种情况重启电脑即可解决。
- 如果之前没安装过火绒个人版且出现了该问题（重启电脑无法解决），尝试从管理工

具模块下载专杀工具扫描。如还无法解决问题，需要您联系火绒客服取得技术支持:400-998-3555。

Q：如何防止终端用户自行修改配置、关闭防护、退出火绒以及卸载火绒?

A： 在控制中心管理-中心设置-终端管理员设置中启用管理员密码保护、防止终端卸载密码保护即可。

Q：2.0 支持多语言吗？在哪里切换呢?

A：支持的，中心在登录界面右上角支持“简体中文/English”切换。

火绒终端在界面右上角设置-语言设置中支持 “简体中文/繁体中文/English”切换。

Q：在哪里可以将 AD 域的组织架构直接导入为分组呢?

A：打开终端管理模块-分组管理，选择组织架构，启用 LADP 设置，填写所需参数即可，填写示例：域名为 Test.com，user 为组织单位名称。即 ou=user,dc=Test,dc=com,多路径换行输入。

Q：动态口令验证失败是为什么?

A：排查如下

- 确定手机显示当前动态口令的时间和所输入动态口令机器的时间误差在小于一分钟之内
- 确定当前所使用的动态口令是中心目前的二维码所产生的动态口令，而不是中心重新

生成过的二维码，因为没有重新扫描，导致验证失败。

Q：我已经下发了任务中止的操作，为什么终端还在执行任务？

A：任务中止指的是中心下发的任务中止，不能终止终端正在执行的任务。

例：下发快速查杀任务，因中心跟终端之间有默认 30s 的通讯时间，在终端没有接收到中心的任务之前，如果将任务终止了，那终端将不执行快速查杀任务，如果终端已经接收到中心的任务了则无法停止。

Q：我已经把某网站添加为信任网址了，为什么恶意网站拦截还是会拦截呢？

A：信任区是针对于病毒而言的，信任区的信任网址只对 web 扫描功能生效，对恶意网址拦截、网站内容控制不生效。

Q：终端的信任区病毒为什么不扫描呢？下发任务时已经勾选了查杀终端信任区

A:检查终端信任区中的文件是否在中心-信任区中添加为信任了,如果在中心添加了信任，则不查杀终端信任区的文件。如果是终端手动自行添加的信任区，则会查杀该信任区的文件。

Q：中心下发卸载软件任务，不能强制卸载吗？

A：支持强制卸载软件。

1、可以强制卸载火绒终端

2、对于部分软件可以直接卸载（不支持卸载带自保的软件），如果您有遇到无法强制卸载的软件可以拨打 400-998-3555 联系我们进行反馈

Q：中心文件分发功能，上传文件的最大限制是多少？

A：目前是最大不超过 500M 的文件。

Q：中心的补丁文件管理具体作用是什么？

A：补丁文件管理的作用是为管理员提供管理当前控制中心已缓存的补丁的功能。可根据需要，删除长期不使用的补丁，节省控制中心计算机的磁盘使用空间。

Q：邮件预警功能的邮件服务器自己搭建吗，用第三方的可以吗？

A：都可以。支持第三方服务器系统，设置方法可以参考各邮箱服务商的参数设置说明

例：QQ 企业邮件服务器参数　　SMTP 服务器：smtp.qq.com　　端口：465

Q：屏蔽搜索引擎的功能是做什么的？

A：主要应用于端口映射或公网地址的中心环境。开启该功能后，可防止中心地址在搜索引擎上被搜索到。

1.3 产品咨询类（基于特殊环境）

Q：客户端不能连接外网/控制端不能连接外网/均不能连接外网，如何进行漏洞修复？

A：解决如下

- 当客户端不能连接外网，控制端可以连接外网时，需要在防护策略-策略管理-安全工具-漏洞修复，勾选“从中心下载补丁”即可。

- 当控制端不能连接外网，客户端可以连接外网时，保持默认配置（不勾选“从中心下载补丁”）即可。
- 当客户端和控制端均不能连接外网时，需要在防护策略-策略管理-安全工具-漏洞修复，勾选“从中心下载补丁”并使用离线升级工具进行离线更新。

Q：可以同时安装多款杀软吗？

A：建议您只安装一款杀软，同时安装多款杀软会导致系统资源占用多，影响日常业务办公，还可能会有互相之间有策略冲突而导致死机等现象出现

Q：企业有硬件防火墙，控制中心升级需要放开哪些 IP/域名和端口？

A：火绒的升级方式采用的是 CDN，故没有固定 IP，放开以下域名即可：

- update.huorong.cn
- down4.huorong.cn
- down5.huorong.cn
- www.huorong.cn
- 端口 80 或 443 均可

Q：我这边使用的是网闸，单向数据传输，升级应该放开火绒的什么地址？

需要开放一下地址，在 host 文件中添加以下地址，对应的域名 ip 以当地的为准，对应 IP 可以 PING 获取。

企业版

update.huorong.cn

down4.huorong.cn

down5.huorong.cn

www.huorong.cn

微软

download.windowsupdate.com

download.microsoft.com

Q：域环境下，用户加在了 power user 组内，没有管理员权限，用文件分发功能分发独立补丁包的时候，客户端是否能正常安装呢？

A：文件分发可以正常被接收，但是到了本地以后，您没有管理员权限的话可能安装不上。独立补丁包无法安装，需要管理员权限。

Q：压缩包监控：提供对不同压缩包类型文件的监控防护，压缩包监控防护层级不小于 10 层，压缩包格式支持不少于 30 种？

A：目前最大支持解码压缩包 32 层。支持实时检测并清除≥30 种常用压缩格式文件内部的病毒，包括 rar、zip、tar、gzip、bzip、arj、cab、7z、iso、lzh、z、zlib、wim、rpm 等。

Q：火绒终端不能修改防护策略如何解决？

A： 终端如无特殊情况不建议独立修改防护策略。如需修改策略可在控制中心对其配置防

护策略。如有特殊情况需修改终端策略，输入管理员密码（中心管理-中心设置-终端管理员）即可修改或者输入中心设置的临时密码（终端概况-点击终端名称）。

Q：Xp、Win7 系统微软已经不支持更新迭代，怎么打补丁？

A：微软发布未更新前的补丁我们都可以打；若发现有新的漏洞补丁，火绒可通过网络入侵拦截功能进行防御。（虚拟补丁、热补丁来解决）

Q：是否支持封装部署，GHOST？

A：是支持的

Q：出差人员怎么连接中心，接受管控呢？

A：您可以把中心部署在公网，或使用 VPN 等工具实现网络可达。出差人员即可管控；

Q：IP 协议控制中“本地 IP 与远程 IP”“本地端口与远程端口”有什么区别？制定规则时怎么操作？

A：

- 本地 IP 及端口代表本机电脑的 IP 及端口，若要阻止本地端口无法供其他电脑使用，则禁用本地端口或 IP。
- 若想阻止本地电脑访问其他电脑的某端口，则禁止远程端口或 IP。

Q：火绒可以有效防御 DDos 攻击吗？

A：火绒目前不能用于拦截 DDOS 攻击，火绒虽然检测到数据包有恶意行为并且拦截，但是数据包本身还是占用了您的带宽。目前我们的安全产品没有专门涉及对该方面的攻击进行有效的防护手段，原因是我们软件是做终端安全的，主要针对终端做有效的防护，面对 DDos 攻击，您可以把发起攻击的者的地址利用 IP 黑名单拉黑，拦截含有恶意的数据包入侵。但是 DDOS 攻击，频繁的、大批量的网络请求还是会占用您的带宽，耗用资源，目前最好的方式是网络边界处作防护，将攻击拦截于网络层或其他分层，是最有效的防御手段。