火绒安全
HUORONG SECURITY

火绒终端安全管理系统 1.0

安装部署手册

2022/03/29

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

用户隐私和数据安全声明

1、火绒尊重用户的隐私权、数据所有权，不会上传用户的任何文件、数据等信息。

2、火绒仅在用户中心控制台联网升级的情况下，上传用户许可相关信息（License），用于验证正版授权。

目录

概述

欢迎阅读《“火绒终端安全管理系统 1.0”安装部署手册》。为了能够更好的服务于用户，特别编写本手册，管理员可在本文中了解安装部署时需要的软硬件要求、网络要求以及安装要求。本手册还详细介绍了部署和卸载“火绒终端安全管理系统 1.0”的步骤，帮助管理员实现在较短的时间内完成网络内部署众多客户端的安装作业，快速的实现整个网络反病毒体系的部署。

“火绒终端安全管理系统 1.0”是秉承“情报驱动安全”新理念，全面实施 EDR 运营体系的新一代企事业单位反病毒&终端安全软件。本产品能帮助用户完成终端安全软件的统一部署、全网管控，集强大的终端防护能力和丰富方便的全网管控功能于一体，性能卓越、轻巧干净，可以充分满足企事业单位用户在目前互联网威胁环境下的电脑终端防护需求。

Tips:

如果您想了解“火绒终端安全管理系统 1.0”核心技术及理念策略，请参阅《“火绒终端安全管理系统 1.0”技术白皮书》。

如果您是初次体验“火绒终端安全管理系统 1.0”，想要快速了解使用方法及操作流程，请参阅《“火绒终端安全管理系统 1.0”使用手册》。

如果您想了解“火绒终端安全管理系统 1.0”产品的详细介绍，请参阅《“火绒终端安全管理系统 1.0”产品说明书》。

安装部署

安装需知

1、软硬件要求

服务端：

- Windows 版本（暂不支持 Linux/Unix/Mac 版本）：
  - Windows XP （SP3）、Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows 10
  - Windows Server 2003（SP1 及以上） /2008/2012/2016/2019
- 包含 32 位以及 64 位
- 内存：至少 2GB
- 硬盘：建议 60GB 以上
- 网卡：具备以太网兼容网卡，支持 TCP/IP 协议
- IE 支持：支持 IE8 及以上
- 是否支持虚拟机：支持

客户端：

- Windows 终端
- 系统版本：支持版本与服务端相同
- 内存：至少 1GB
- 硬盘：建议 40GB 以上
- 网卡：具备以太网兼容网卡，支持 TCP/IP 协议
- 是否支持虚拟机：支持

Linux 终端

- 系统版本：支持 CentOS、Ubuntu、SUSE、Deepin 等发行版，仅支持 64 位
- GNU libc：2.12 及以上
- 内存：至少 1GB
- 硬盘：建议 40GB 以上
- 网卡：具备以太网兼容网卡，支持 TCP/IP 协议
- 是否支持虚拟机：支持

2、网络环境要求

火绒终端安全管理系统默认的通讯端口：

- 控制中心及端口：80
- 数据库端口：3306
- 中心远程端口：5901
- 终端远程端口：5500

通讯端口均可修改，但是请确保防火墙或者类似的安全设备不会阻碍通讯端口

3、管理系统安装要求

- 控制中心需要具有长期固定的 IP 地址或者域名和端口
- 终端安装部署时候需要用到控制中心的 IP 地址或者域名和端口
- 建议选择专用服务器系统、非经常性大负荷运转的服务器

4、安全终端安装方式

安装方式	说明
网页安装	通过访问火绒控制中心终端部署的安装链接下载安装客户端，终端不需要做任何配置
域部署工具	通过在域服务器上安装域部署工具，向域用户强制推送安装火绒终端安全软件

5、部署参考

全站部署

- 在服务中心部署火绒控制中心以及控制台
- 通过网页安装或者域部署工具的方式安装火绒安全终端

升级方式

1、管理系统：

- 自动升级、手动升级、离线升级工具升级
- 连接外网时，推荐开启自动升级。及时获取到更新
- 只连接内网时，推荐下载离线升级工具进行升级

2、安全终端：

- 只通过内网连接控制中心，自动升级
- 自动升级策略为开机后每小时检查一次
- 可通过终端管理发送终端升级任务，手动升级

3、管理策略：

- 根据不同的分组可以采取不同的策略进行管理防护
- 可为终端每周一次进行全面扫描（闲暇时）
- 为所有终端设置卸载密码，避免用户自行卸载客户端
- 经常查看事件日志并且分析病毒，下发查杀指令保护终端并且及时更新升级
- 可为终端设置为开机杀毒，保证终端安全

部署管理系统

管理系统包括火绒终端安全管理系统以及火绒安全终端

安装管理系统

1、火绒控制中心是火绒终端安全管理系统的管理室，部署于服务端，采用 B/S 架构，可以随时随地的通过浏览器打开访问。

2、主要负责全网安全监控、终端管理、策略定制分发、统一杀毒防护以及事件日志查询等。

3、获取安装包后，只需双击安装包，打开安装程序即可安装

部署管理系统地址：

安装完火绒终端安全管理系统之后，运行配置工具进行地址、端口等配置。


配置工具
中心地址
安装部署手册
终端部署地址:
全部IP
外网端口
终端部署端口:
80
SSL
中心远程端口:
5901
终端远程端口:
5500
数据库设置
本地数据库端口:
3306
文件存放
补丁保存目录:
C:\Program Files (x86)\Huorong\ESCenter\HotFix
浏览
文件分发目录:
C:\Program Files (x86)\Huorong\ESCenter\distr
浏览
其它
中心密钥:
Qt0xw1EZX9E
重新生成
超级管理员密码:
默认密码admin
修改
备用中心
将当前中心设为备用中心
保存
取消

字段		说明
终端部署地址	域名部署	通过自定义域名进行终端部署 支持 HTTP 协议以及 HTTPS 协议
	IP 部署	通过动态获取 IP 进行终端部署。 多网卡中任一 IP 地址均可访问
终端部署端口		通过该端口进行终端，部署端口默认为 80（HTTP）
SSL		如需进行 HTTPS 配置，可在此添加 Crt、Key 文件
中心远程端口		中心下发远程桌面时中心使用的 VNC 远程端口
终端远程端口		中心下发远程桌面时终端使用的 VNC 远程端口
本地数据库端口		数据库端口默认为 3306
补丁保存目录		漏洞修复补丁存放在中心的目录
文件分发目录		文件分发上传的文件保存的目录
中心访问秘钥		用于控制中心间通讯加密
超级管理员密码		默认账号及密码都为 admin
将当前中心设为备用中心		默认不勾选，勾选后可将当前中心配置为备用中心
修改终端部署地址或者端口后，已经部署的终端需要重新下载覆盖安装客户端		

安装授权 Lisence 文件：

第一步：登录火绒终端安全管理系统：通过配置工具设置的控制中心地址访问管理系统（默认为 http://localhost:80），输入账号以及密码即可登录（账号密码默认都为 admin）

第二步：登录火绒终端安全管理系统后，在页面的左侧点击“未授权”。

第三步：在授权信息页面中点击“浏览”后选择授权文件。

第四步：点击“更新授权”，即可完成对管理系统的授权安装。

注：

安装授权文件后，“未授权”字样将会变为“正版授权”，代表授权文件安装成功；后续的更新授权也采用上述操作即可。

如果未授权或者授权到期，请及时更新授权，否则无法更新版本、病毒库，管理在线终端的数量也将进行限制。

安装火绒安全终端

火绒安全终端部署在需要统一保护的服务器或者客户端、执行病毒查杀以及实时监控等安全操作，并且向控制中心传递安全事件信息

1、Windows 终端安装

网页安装：

第一步：访问客户端软件安装网址（http(s)://IP 地址:端口）。

第二步：点击下载 Windows 版本，下载 Windows 安装包【installer(http(s)IP 或域名端口).exe】。

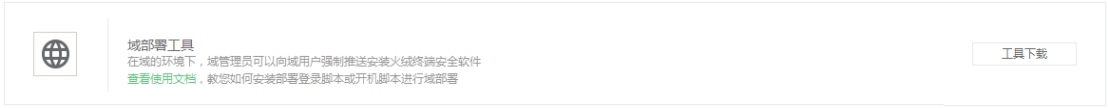
第三步：运行客户端安装包。（管理控制中心的 IP 或域名、端口如有变化，将安装包名称后半部分中带有的 IP 或域名、端口地址更换为管理控制中心 IP 或域名、端口。）

注：推荐将安装包下载保存后进行安装；使用 IE8 以及以下浏览器直接安装客户端会存在无法连接控制中心的情况。

第四步：安装成功后会自动连接上控制中心。

域部署工具安装：

在管理工具界面下载域部署工具，并且在域服务器上部署开机或者登录脚本，即可对域内用户完成自动安装部署（含使用帮助文档）



注意事项：

- 如果管理控制中心的 IP 或者域名端口没有变化，客户端安装包名称后半部分请勿改动，否则客户端无法连接控制中心，无法正常安装。
- 如果已经安装了个人版客户端，安装火绒安全终端的时候需要先卸载个人版客户端，然后重启电脑（否则服务异常），才能正常使用。
- 客户端安装后将会在 30 秒左右自动连接上控制中心。

2、Linux 终端安装

安装流程

第一步：访问客户端软件安装网址（http(s)://IP 地址:端口）。

第二步：点击下载 Linux 版本，下载 Linux 安装包。

第三步：将下载好的安装包发送至 Linux 服务器客户端并执行。

```
[root@localhost ~]# chmod 0755 linux-inst.sh
[root@localhost ~]# ./linux-inst.sh
Verifying archive integrity... All good.
Uncompressing huorong installer  100%
installing huorong enterprise linux
init install directory
please input huorong center domain[:port]192.168.3.205
move file to /usr/local/huorong
"./huorong/bin" -> "/usr/local/huorong/bin"
"./huorong/bin/hipsdaemon" -> "/usr/local/huorong/bin/hipsdaemon"
"./huorong/bin/hrclient" -> "/usr/local/huorong/bin/hrclient"
"./huorong/bin/hrupdate" -> "/usr/local/huorong/bin/hrupdate"
"./huorong/bin/hrfix" -> "/usr/local/huorong/bin/hrfix"
"./huorong/lib" -> "/usr/local/huorong/lib"
"./huorong/lib/libhipsdb.so" -> "/usr/local/huorong/lib/libhipsdb.so"
"./huorong/lib/libxsse.so" -> "/usr/local/huorong/lib/libxsse.so"
"./huorong/lib/libcobra.so" -> "/usr/local/huorong/lib/libcobra.so"
"./huorong/lib/libexscan.so" -> "/usr/local/huorong/lib/libexscan.so"
"./huorong/lib/libbot.so" -> "/usr/local/huorong/lib/libbot.so"
"./huorong/lib/libvxf.so" -> "/usr/local/huorong/lib/libvxf.so"
"./huorong/lib/libstdc++.so.6" -> "/usr/local/huorong/lib/libstdc++.so.6"
"./huorong/lib/libnat.so" -> "/usr/local/huorong/lib/libnat.so"
"./huorong/lib/libssl.so.1.1" -> "/usr/local/huorong/lib/libssl.so.1.1"
"./huorong/lib/libcurl.so.4" -> "/usr/local/huorong/lib/libcurl.so.4"
"./huorong/lib/libcrypto.so.1.1" -> "/usr/local/huorong/lib/libcrypto.so.1.1"
"./huorong/lib/libdt.so" -> "/usr/local/huorong/lib/libdt.so"
"./huorong/lib/libcodecs.so" -> "/usr/local/huorong/lib/libcodecs.so"
"./huorong/share/virdb/prop.db" -> "/usr/local/huorong/share/virdb/prop.db"
"./huorong/share/virdb/pset.db" -> "/usr/local/huorong/share/virdb/pset.db"
"./huorong/share/virdb/hwl.db" -> "/usr/local/huorong/share/virdb/hwl.db"
"./huorong/share/virdb/troj.db" -> "/usr/local/huorong/share/virdb/troj.db"
"./huorong/un.huorong" -> "/usr/local/huorong/un.huorong"
"./huorong/VERSION" -> "/usr/local/huorong/VERSION"
move file to /usr/local/share/xsse
"./xsse/libvxf.dat" -> "/usr/local/share/xsse/libvxf.dat"
"./xsse/libvxf.tdl" -> "/usr/local/share/xsse/libvxf.tdl"
centos 6
installed
[root@localhost ~]#
```

第四步：安装成功后会自动连接上控制中心。

注意事项：

- Linux 终端仅支持 64 位操作系统。
- 安装需要 root 权限。
- 需要 GNU libc 2.12 及以上版本。

卸载管理系统

为了保证火绒终端安全管理系统能够正常运行，系统可为客户端软件设置了密码保护以及卸载保护，修改配置、退出程序、卸载软件都需要提供管理员密码。

卸载管理系统

卸载方法一 ：

第一步，进入 Windows 控制面板，选择“添加/删除程序”

第二步，找到并且选择火绒终端安全管理系统，右键“卸载/更改”

第三步卸载程序将引导您完成火绒终端安全管理系统卸载

卸载方法二 ：

第一步，点击 Windows 的【开始】菜单 -> 【程序】 -> 【火绒终端安全管理系统】 -> 【卸载火绒终端安全管理系统】

第二步，卸载程序将引导您完成火绒终端安全管理系统卸载

卸载火绒安全终端

1、Windows 终端卸载

卸载方法一：

第一步，进入 Windows 控制面板，选择“添加/删除程序”

第二步，找到并且选择火绒安全终端，右键“卸载/更改”

第三步，输入客户端卸载密码，单击【确定】

第四步，卸载程序将引导您完成火绒安全终端卸载

卸载方法二 ：

第一步，点击 Windows 的【开始】菜单 -> 【程序】 -> 【火绒安全终端】 -> 【卸载火绒安全终端】

第二步，输入客户端卸载密码，单击【确定】

第三步，卸载程序将引导您完成火绒安全终端卸载

2、Linux 终端卸载

执行“sudo /usr/local/huorong/un.huorong”命令，完成 Linux 火绒终端卸载。