企业版 2.0 常见问题

用户运营版

Lity

2025 年 1 月

目录

安装部署

1. 环境

Q：中心支持安装在哪些系统?

A：中心可以部署在 Windows 系统和 Linux 系统，Windows 系统支持 win7 及以上，Linux 主要看 glibc（x86_64 (glibc 2.12 及以上版本) AArch64 (glibc 2.17 及以上版本)）满足即可。如需 Linux 版本中心需要申请，需要联系销售操作开通。

Q：系统适配情况是怎么样的?

A：火绒目前对于 linux 系统、windows 系统、MacOS 系统、国产系统已经全面适配。

下图为系统适配详情：

Q：跨网段能否部署客户端?

A：支持跨网段，需要网络互通，终端能访问终端部署页面即可安装。

2. 域名&端口

Q：网络有防火墙需要添加火绒升级白名单需要放开哪些地址?

A：火绒的升级服务用的是 CDN，故没有固定 IP，放开以下域名即可：

2.0 中心：

www.huorong.cn

update.huorong.cn

down4.huorong.cn

down5.huorong.cn

2.0 终端：

down2.huorong.cn

down3.huorong.cn

down7.huorong.cn

1.0 中心：

update.huorong.cn

down4.huorong.cn

down5.huorong.cn

1.0 终端：

down2.huorong.cn

down3.huorong.cn

down7.huorong.cn

以上 IP 均开放 443 以及 80 端口，如果是网闸需要填写 IP 可以 ping 一下域名然后获取

IP 填写

Q：火绒使用的端口有哪些?

A：使用的端口可以在配置工具中进行确认，如果安装过程中有提示端口冲突，可以修改为环境里没有占用的其他端口，默认的使用情况如下图：

中心管理端口：通过该端口访问控制中心后台可对终端进行管控

终端部署端口：通过该端口访问终端部署页面可下载客户端且中心与终端通讯也是此端口

中心远程端口：中心使用远程桌面时中心将获取到的数据回传至控制端的端口

终端远程端口：中心使用远程桌面时中心获取被控端数据的的端口

本地数据库端口：管理中心与本地 mysql 数据交互的端口

Q：端口冲突如何处理?

A：端口冲突可以更改为没有被占用的端口；但是如果已经部署了终端那么终端部署端口不能随意修改，修改后之前部署的终端会链接不到中心，需要覆盖安装或者使用迁移工具

进行迁移。

3. 授权

Q：授权如何激活使用?

A：控制中心电脑可以连接外网：登录中心点击未授权直接输入序列号密码即可进行激活；

控制中心电脑无法连接外网：需要使用离线升级工具激活授权，下载工具后同步数据，之后将 conf 文件夹和离线升级工具拷贝到可以连接外网的机器运行离线升级工具输入序列号密码激活授权，激活完成后将数据和工具拷贝回控制中心电脑更新即可。

Q：序列号和密码如何获取?

A：授权的序列号和密码在发送的授权邮件中，可以通过邮箱查找。如果找不到了可以提供邮箱地址，联系销售重新发送。

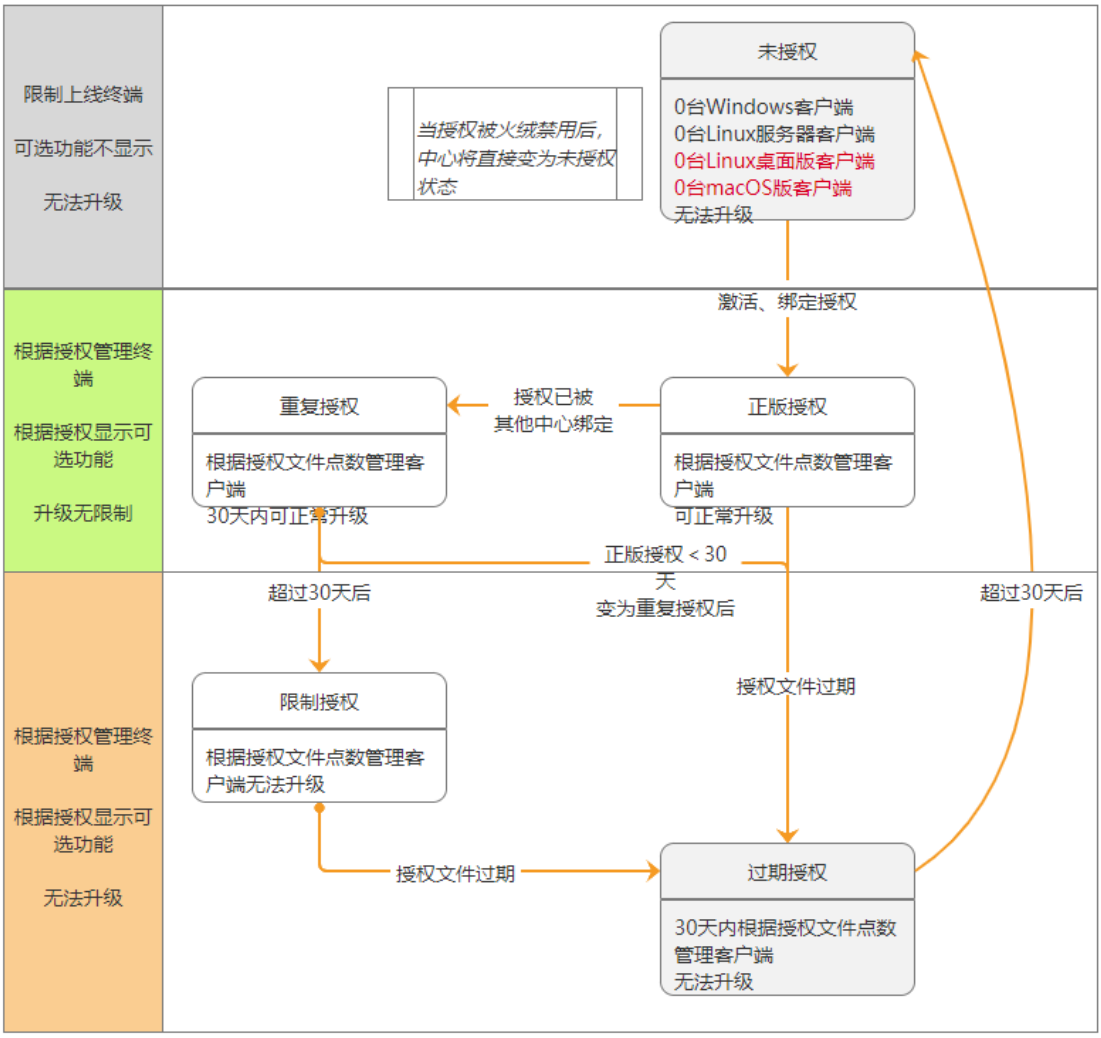
Q：不再使用的终端机器是否占用授权?

A：离线终端即不占用授权。

Q：重复授权/授权到期有什么影响?

A：重复授权：在其他中心激活后会变为重复授权，可以重新激活一下授权。重复授权 30 天内可以正常管控升级，30 后变为限制授权只能管控终端无法升级；

授权到期：未超过 30 天版本、病毒库无法升级其他功能正常使用；过期授权超过 30 天版本、病毒无法升级、终端重启后会从中心离线无法上线，保留中心最后一次配置的防护策略。



4. 安装

Q：控制中心如何下载安装?

A：使用序列号密码登录火绒官网下载安装包，之后双击安装激活授权即可。

Q：中心已经安装完成，终端如何安装部署?

A：共有五种部署方法：

1）网页访问部署：客户机浏览器地址栏访问控制中心 IPv4/IPv6 地址，点击下载客户端，双击安装即可。

2）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。

3）域部署：可以通过域部署工具生成部署脚本可携带静默参数，通过导入到 AD 域开机组策略中进行批量部署。

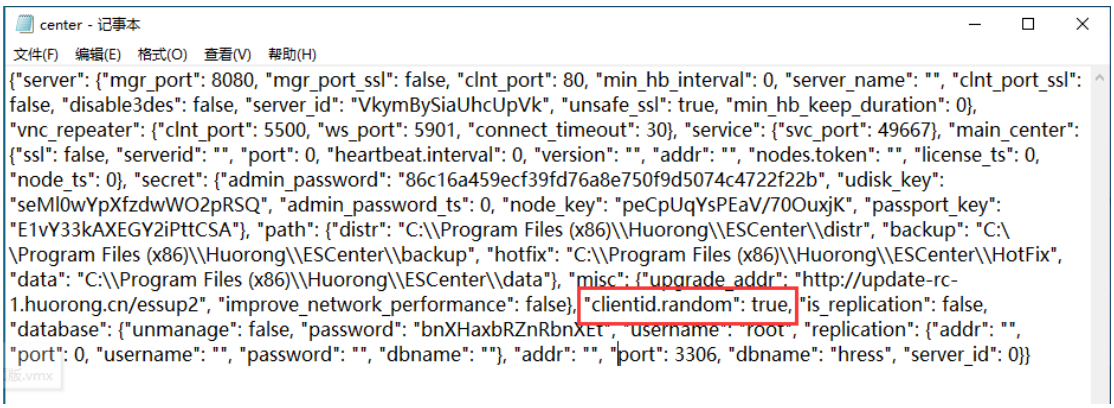
4）三方桌管推送：如有第三方桌面管理软件，可推送火绒客户端安装包，推送时携带静默安装参数/S。

5）如是 linux 系统安装，可以访问终端部署页面命令，将其复制/输入到 linux 的 dos 命令行下进行安装。

Q：是否可以将安装火绒终端的电脑做镜像，然后批量安装?

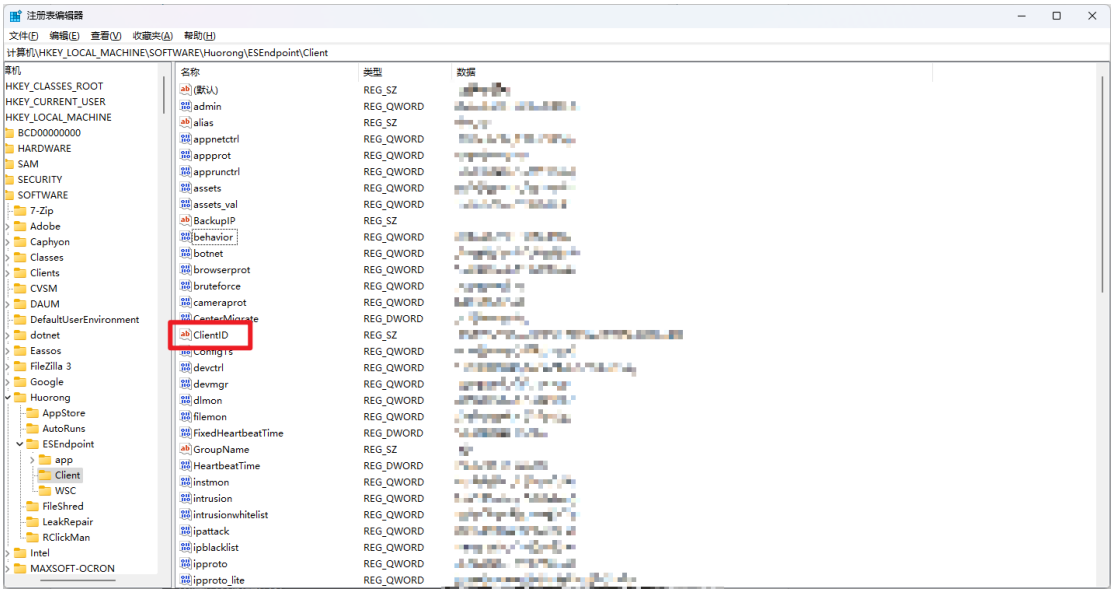
A：有两个方法实现：

1）在中心修改：打开 C:\Program Files (x86)\Huorong\ESCenter\sysconf 中的 center 将"clientid.random":false,改为"clientid.random":true,如果没有这个值可以手动添加下" clientid.random":true,



2）在终端将火绒终端注册表的 clientID 里面数据删掉，然后再做镜像（终端上线后会自己自动再生成）

计算机\HKEY_LOCAL_MACHINE\SOFTWARE\Huorong\ESEndpoint\Client 右侧 ClientID



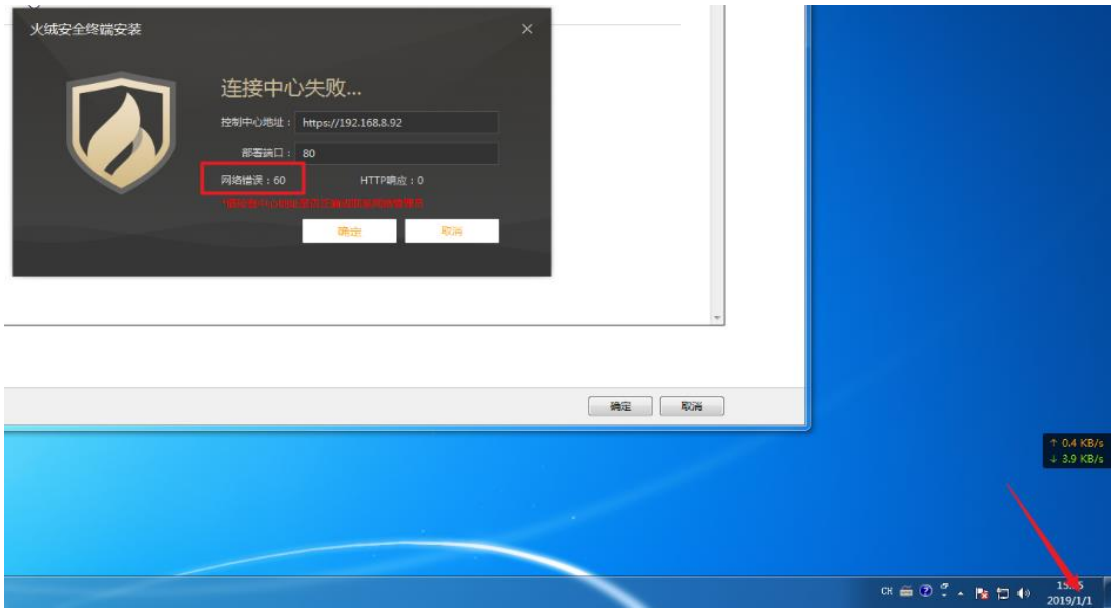
Q：终端安装报错如何处理？

A：

1）终端安装报错，网络错误：35　HTTP 响应：0

部署端口填写错误，需要修改为正确的端口

2）终端安装报错，网络错误：60　HTTP 响应：0



https 安装时间问题，需要同步下终端和中心机器的系统时间，或者使用 http 安装

3）终端安装报错，网络错误：0　HTTP 响应：404

中心文件缺失，可以手动升级中心或使用离线升级工具进行升级操作

4）终端安装报错，网络错误：7　HTTP 响应：0

主机或代理连接失败，可以重新访问部署链接下载终端安装包，确认下网络是否正常

5）终端安装报错，网络错误：28　HTTP 响应：0

终端与中心网络不互通导致，现象表现为终端无法通过部署链接访问到部署页面。需要排查网络或端口是否有限制

Q：终端安装后提示服务异常？

A：服务异常一般是驱动没有起来，方便的话可以重启电脑。

首页

Q：异常终端是什么？

A：异常终端可能是终端退出或者终端服务异常，可以到异常终端电脑确认看下，如果是服务异常了可以重启一下电脑看能否恢复。

Q：服务器性能是服务器这台电脑性能么?

A：服务器性能是安装火绒控制中心电脑的性能显示，其中的网络流量也是这台电脑的上传和下载情况。

Q：已部署的数量是怎么计算的?

A：已部署数量为主中心所有终端加下级中心所有终端的总和。

Q：近期安全事件时间能否自定义?

A：首页中安全事件无法自定义事件如需查看更多时间可点击事件日志-安全事件总览，自定义时间后进行查看。

终端管理

1. 终端概况

Q：勾选终端下发了终端升级的任务，终端病毒库升级到最新了，但是版本升不上去?

A：终端版本如果是 2.0.4.4 需要安装 sha2 补丁，安装完成后再进行升级；

如果是其他版本策略中查看下是否勾选仅升级病毒库，取消勾选后再下发升级查看。

Q：终端概况中终端颜色为什么不同?

A：橙色为正常在线状态；灰色为离线状态，未连接中心，终端可能关机、卸载或者网络与中心不通；红色为异常状态，终端可能退出或者服务异常，可以到终端电脑确认，如果是服务异常可以重启后观察。

Q：终端隔离是什么意思？

A：终端隔离会阻止除火绒外的所有 tcp/udp 连接，相当于给终端断网隔离。

Q：删除终端和卸载终端有什么区别？

A： 删除终端是删除离线的终端，在线终端是无法删除的，删除后终端将不在中心列表显示。后续终端连接中心会再次出现在列表中；

卸载终端是对终端下发强制卸载，在设置管理员密码，无人值守的情况下也是可以卸载的，终端电脑无需做任务操作，在线终端会在下发后不久接受任务并完成卸载，离线终端需要在 30 天内上线才能接收到任务完成卸载。（如火绒版本过低可能不支持该功能）

Q：加入黑名单是什么意思？

A：加入黑名单后，终端自动从中心删除并不再占用授权，用于释放授权。加入黑名单的终端可在【终端管理】-【终端黑名单】查看及管理。

2. 分组管理

Q：组织架构可以同步什么设备信息？

A：目前只能同步域环境的组织架构。

Q：组织架构同步后终端是否自动安装并进入对应分组？

A：开启自动分组终端时，将根据设置将对应范围的终端按照设置的分组方式，重新自动分组。

Q：如果设置了分组规则，在这个分组的终端 IP 或者名字变更不符合分组规则，是否会自动调整？

A：不会自动调整，分组规则是针对未分组的终端，若是终端已经在某个分组，即使发生变化也不会再匹配其他规则。

Q：如果同时满足 IP 分组规则和命名分组规则，终端最终会到哪个分组?

A：看规则的排序，规则是从上往下进行匹配。

Q：分组顺序如何调整?

A：点击分组管理后鼠标放在右边列表分组名称前面会出现拖动改变顺序的提示，点击鼠标左键拖动即可调整分组顺序。

3. 终端黑名单

Q：终端黑名单怎么使用?

A：点击添加可以选中终端加入列表实现释放授权，也可以勾选列表中的终端删除取消黑名单让终端连接中心接受管控。

4. 标签管理

Q：标签管理这个功能是做什么用的?

A：可以根据自身企业应用场景自定义标签，以此来作为条件对终端进行进一步区分，方便用户标识及管理企业内的终端。相当于是给终端添加备注。

5. 文件分发

Q：文件分发都支持什么类型文件，文件上传是否有大小限制?

A：支持上传可执行程序、脚本、文档和压缩包等；最大支持上传 16G 的文件。

Q：文件分发能否自定义路径?

A：可以，中心可以在下发的时候创建文件夹并可以自主选择是否替换同名文件。

Q：选择以系统权限运行后给终端下发了软件进行安装，没能安装成功是什么原因?

A：以系统权限运行时，不会出现任何的程序界面，是在服务会话下运行。只能下发双击后不需要任何交互(比如 bat 脚本文件 双击后自动安装完成无需任何点击的程序) 可以成功安装，对需要手动点击下一步和选择安装位置的程序是不行的，这种需要选择接收并运行，如果有运行参数的话可以填写参数。

Q：如何实现下发软件静默安装?

A：静默安装需要软件自身支持分发安装且软件厂商有提供静默安装参数，在分发时填写运行参数并选择以系统权限执行即可实现静默安装。

6. 计划任务

Q：计划任务设置后怎么查看终端是否执行?

A：可以在事件日志-终端管理日志-计划任务日志中查看计划任务执行的情况。

Q：如果终端与控制中心断开，控制中心之前设定的定时任务会继续执行吗?

A：终端同步任务后即使后续不连接中心也会自动执行计划任务的，等终端连接中心后相关的日志会上传到中心。

Q：计划任务设置后能否重新编辑?

A：计划任务除了任务名称外都可以重新编辑。

Q：任务执行时间过期后立即执行是什么意思?

A：比如设置了 10 点的病毒查杀任务，但是终端 10 点没有开机，11 点才开机。勾选“任务执行时间过期后立即执行”11 点开机后会立即执行查杀任务。

7. 任务管理

Q：为什么设置了计划任务，在任务管理没有显示?

A：任务管理这里记录的是中心对终端下发的任务记录，计划任务需要在事件日志-终端管理日志-计划任务日志位置进行查看。

Q：下发任务后是否可以停止?

A：下发任务后，点击终止任务，未接收到任务的终端不会再响应任务；正在执行任务的终端，病毒查杀任务会立即终止查杀，其他任务需等待任务执行完成。

Q： 下发任务的有效期是多长时间呢?

A：默认情况是 1 天，可以在任务管理页面，右上角设置进行编辑，有效期最大值是 30 天。远程桌面、文件分发、卸载终端任务的有效期不受该设置影响。

8. 终端发现

Q：终端发现这个功能是做什么的?

A：终端发现，可以帮助管理员发现中心子网地址下，需要安装但没有安装火绒安全终端的计算机，以免出现漏管漏控的情况，此功能分为地址资源、未确认终端和已发现终端三个页面。

Q：我这里都没有安装火绒，只有控制中心，怎么扫描不到?

A：需要先安装终端，通过这个终端的 IP 去发现这个 IP 段其他需要安装但没有安装火绒的机器。

Q：终端发现-未确认终端，这里都是需要安装火绒的计算机吗?

A：扫描发现的设备不一定都是需要安装的计算机，可能是网络设备、移动设备等，需要进行判断确认的，通过编辑进行备注即可。

Q：终端发现-已发现终端，为什么有的计算机没有显示终端名称?

A：已发现终端位置的设备安装火绒后，会显示设备名称的，没有安装火绒的情况下是不会显示的。

9. 设备管理

Q：设备管理是做什么的?

A：设备管理功能让需要使用禁用设备的终端用户主动向中心发起申请，中心管理员审批通过，该终端才能使用此设备，审批时管理员能够设置该设备的使用期限，审批通过的设备信息会显示在设备管理--信任设备的列表中，管理员随时能够删除此信任设备。

防护策略

1. 策略部署

Q：新建的策略如何应用到终端?

A：在防护策略-策略部署位置可以给不同终端分组应用不同的策略，在部署防护策略这列点击后选择即可应用成功。

Q：终端分组已经应用了策略，但是终端为什么没有生效?

A：可以看下终端概况中策略同步情况，可能是终端未能同步策略导致，可以勾选终端下发一个同步策略的任务，等任务执行完成后观察看下。

2. 策略管理

Q：策略点击后无法修改，都是灰色?

A：默认防护策略是相当于模板无法进行修改的，可以点击新建策略以默认策略为模板新建一个，然后进行自定义的设置。

Q：终端升级后弹窗提示能否关闭不提示?

A：可以策略通知设置将"自动升级-完成时"开关关闭，关闭后将不再弹窗提示。

Q：通知设置的常规模式和免打扰模式怎么设置?

A：常规模式是没有开启免打扰模式，基础配置中未勾选开启免打扰模式的弹窗提示情况，可以根据需求开启或者关闭弹窗提示，开启为橙色，即有弹窗提示，灰色为关闭即不提示；

免打扰模式是基础配置中勾选了开启免打扰模式时的弹窗提示情况，也是可以根据需求开启或者关闭弹窗提示，开启为橙色，即有弹窗提示，灰色为关闭即不提示。

Q：文件实时监控出现大量报毒日志该如何处理?

A：将火绒的信任区清空后进行全盘查杀，全盘查杀后重启电脑观察是否还有问题。

Q：系统加固拦截了需要使用的脚本/程序怎么设置放过?

A：根据日志中显示的对应项目在策略防护系统加固-自动处理规则中选择对应的功能添加日志中显示的操作进程，如果操作进程为系统进程比如：cmd.exe；reg.exe；net.exe；net1.exe；explorer.exe；dllhost.exe；svchost.exe 不可以添加，可以添加日志中的父进程勾选包含子程序。

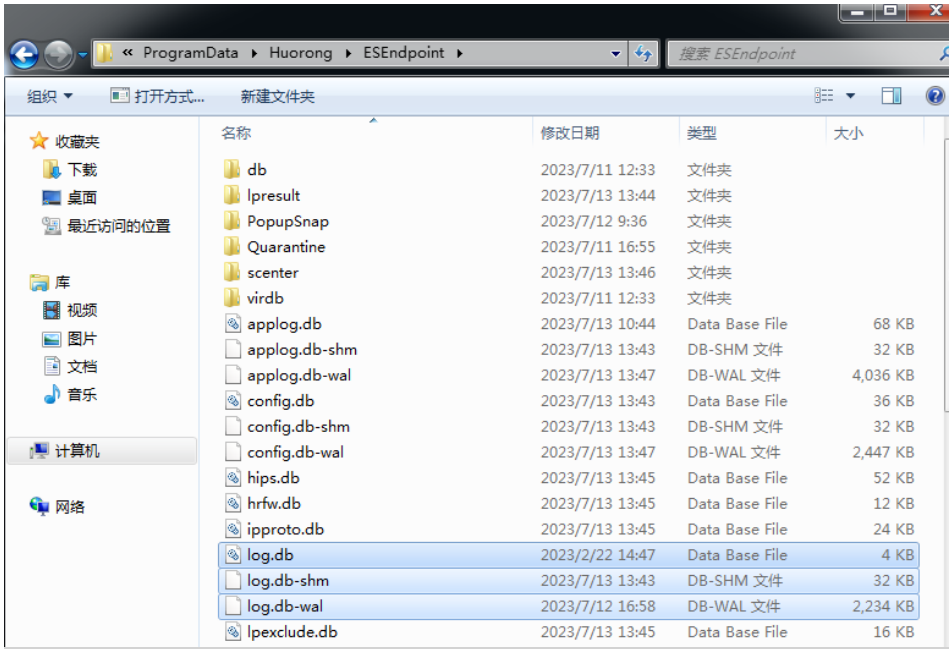
Q：系统免疫拦截了需要使用的脚本/程序怎么设置放过？

A：系统免疫拦截不支持添加白名单自动处理。需要提取信息联系官方客服确认：

1. 火绒终端日志；

2. 拦截的文件；

3. 终端电脑火绒的三个 log 文件（路径：C:\ProgramData\Huorong\ESEndpoint 下的 log.db、log.db-shm 和 log.db-wal；）



Q：安装软件被火绒拦截如何放过？

A：策略中找到软件安装拦截点击添加规则将要安装的软件选中添加白名单就不会再拦截了。

Q：是否可以手动添加软件不让它安装？

A：目前暂不支持手动添加软件阻止安装，可以在程序执行控制添加程序阻止运行。

Q：暴破攻击防护-smbv2 拦截如何处理？

A：smbv2 暴破一般是病毒或共享导致的，日志里的远程地址是发起攻击的机器，可以通过以下三个步骤进行排查：

1.排除病毒因素：对远程地址对应的终端进行全盘查杀+专杀工具扫描；

2.排除共享因素：将火绒升级至最新版本，如本地地址机器存在共享服务或共享打印机，可在不影响业务的情况下临时关闭， 如未出现新的拦截日志，需在远程地址机器上查看是否存在本地地址凭据或该共享的快捷方式，若存在，将凭据删除后重新添加或删除此共享的快捷方式，再观察解决情况；

3.若上面两点都确认没有问题，但仍然有暴破攻击日志出现，需要在有日志出现的时候进行抓包联系官方客服确认。

Q：暴破攻击防护-smbv1 拦截如何处理?

A：对远程地址对应的终端进行全盘查杀+专杀工具扫描，查杀后重启电脑观察。

Q：远程登录防护都能拦截哪些远程?

A：远程登录防护开启后将阻止所有的 RDP 远程（系统的远程桌面）连接，不影响向日葵这类远程工具使用。

Q：能否实现只允许访问特定的地址?

A：IP 协议控制可以设置 IP 地址和端口，来实现功能；先设置一个放行的策略，远程 IP 填写输入可以访问的 IP 端，优先级设置为 1；再设置一个阻止的策略优先级为 2，即可实现。

Q：联网控制如何使用?

A：开启功能后可以选择是允许联网还是阻止联网，如果允许联网的话可以添加阻止联网的规则。

Q：网站内容控制添加 https 网址后没有拦截?

A：确认策略已同步后可以通过以下方法排查处理：

1.网址填写是否正确，https 网址暂不支持使用通配符；

2.重启终端电脑；

3.清理浏览器缓存，无痕模式访问；

4.同一个进程去访问同一个域名，期间没有关闭过网站内容控制功能的话只会记录一条日志。

Q：程序执行控制拦截了软件后设置信任文件和添加自定义规则没生效如何处理?

A：程序执行控制如果要放过的话需要在对应规则名称中找到拦截项目将开关关闭，自定义规则是添加程序进行拦截，信任文件不能放过程序执行控制的。

Q：禁止 U 盘使用怎么设置，禁止后是否可以允许个别 U 盘使用?

A：在策略的设备控制中开启功能，然后将 U 盘设备改为禁用即可禁止 U 盘使用。禁止后如有需要使用的 U 盘有三种方式可以实现：1）注册 U 盘；2）将需要使用的 U 盘添加到设备控制白名单；3）需要使用的 U 盘在终端进行申请，然后中心审批通过即可使用。

Q：开启设备控制后打印机无法使用，但是没有禁用打印机?

A：查看设备控制的日志看下是否为其他项目拦截了打印机，火绒的设备是通过系统的设备管理器获取，如果打印机在设备管理器中被识别为其他类型火绒也会按照这个类型禁用。

Q：漏洞修复的策略已经勾选"关闭 Windows 自动更新"但是系统还是自动更新重启?

A：目前此功能不支持 win10 及以上系统和 winserver2016 及以上系统。

Q：软件禁用是做什么的?

A：自定义黑白名单，对终端用户已安装的软件进行检测，并且对违规用户处置 (只会提示终端电脑，不会对软件禁用;如果选择隔离违规终端，终端隔离后无法通过终端概况给终端恢复，只能通过卸载软件)。

Q：违规外联是做什么的?

A：检测终端是否有链接外部网络的能力或者是否使用公司指定的网络环境链接外网，并对违规终端进行处置。

3. 信任文件

Q：中心添加信任文件后终端没有显示?

A：中心添加的信任文件不会在终端显示，终端看不到信息。保证终端策略与中心是同步状态即可生效。

Q：已经添加信任文件终端还是报毒，如何处理?

A：终端是否在线，在线才能同步中心的设置；终端在线情况下策略是否显示同步，如终端概况策略同步显示为"否"需要下发同步策略任务，任务完成后再观察；规则添加是否正确，规则正确才能匹配成功放过。

Q：需要排除一个程序这个程序可能在 C\D\E 各种盘符下，应该怎么写?

A：可以使用通配符*\程序名称。

4. U 盘管理

Q：U 盘注册后只剩 5M 空间，剩余空间去哪儿了?

A：U 盘注册后会有两个分区，5M 空间是其中一个分区，打开 U 盘后双击 HRSafeUDisk.exe 程序即可看见另一个分区。

Q：终端升级后注册 U 盘出现问题，5M 空间无法操作?

A：出于安全考虑 2.0.15.0 版本升级后注册 U 盘 5M 空间改为只读，无法操作是正常情

况。

Q：注册 U 盘丢失了中心是否能取消注册?

A：中心可以取消，在中心将这条记录删除掉，就不会再识别此 U 盘。

Q：注册 U 盘失败如何处理?

A：查看是否开启 U 盘禁用，注册时需要暂时关闭 U 盘禁用进行注册。

Q：U 盘注册时禁止 U 盘在外网使用，但是在外网还是能使用?

A：注册 U 盘时的外网指的是未安装火绒终端的电脑；不勾选允许外网使用的情况下注册 U 盘在脱离中心的终端上也是无法使用的。

5. 终端动态认证

Q：终端动态认证的二维码用什么扫描?

A：微信搜索火绒安全小程序打开后点击“+”扫描即可生成动态口令；或者下载 Google Authenticator 这个 APP、TOTP 这类的 APP 都可以使用。

Q：终端动态认证开启后终端输入口令提示错误?

A：确认电脑时间与手机时间是否一致，口令是 30 秒一刷新，如果时间误差超过 30 秒会出现口令错误的情况。

漏洞修复

Q：下发漏洞修复任务后怎么查看任务执行情况和补丁安装情况?

A：任务下发后可以通过任务管理查看任务是否执行，补丁是否安装成功可以通过事件日

志-漏洞修复来查看是否安装成功。

Q：补丁文件管理是所有的补丁么?

A：补丁文件管理是当前已下载缓存在中心的所有补丁列表。

资产管理

1. 资产登记

Q：是否支持终端自主选择要进入的分组?

A：支持的，在登记设置中勾选该项即可。(勾选后，仅在安装时会显示该登记项，重新登记的内容不包括分组登记)

2. 软件管理

Q：下发的是强制卸载任务，但终端还是弹出卸载程序的窗口需要手动卸载是什么原因?

A：由于软件的类别、名称、版本体量非常大，目前无法对全部的软件都支持强制卸载。

如您有需要添加的软件，可提供该软件的安装包，我们分析后会添加强制卸载支持。

中心管理

1. 账号管理

Q：账号设置中的下次登录修改密码是每次登录都需要修改吗?

A：不是的，只需要修改一次。

Q：默认 admin 账号能重命名吗?

A：可以在账号管理中点击 admin 账号的账号设置进行重命名。

Q：管理员账户登录地址可进行限制这个功能在哪个位置?

A：点击中心管理-账号管理，找到需要限制的地址的账号点击对应账号设置。

Q：登录超时自动登出在哪设置呢?

A：点击中心管理-账号管理，右上角设置打开后可以设置账号自动登出时间。

2.多级中心

Q：多级中心的三种授权方式：独立授权、动态分配、自定义分配，互相有什么区别呢?

A：独立授权：下级控制中心连入后默认均为独立授权，独立授权时下级控制中心使用自己的授权，与上级控制中心的授权互无关联。

动态分配：下级控制中心根据自己需要向上级控制中心索取授权，使用上级控制中心的授权。但不可超过上级控制中心授权的总终端台数。 注：动态分配时，下级控制中心获得授权点数后将会持续占用，即使有终端下线，授权点数并不会因此减少。当上线的终端数超过授权点数后下级控制中心会继续向上级控制中心索取授权。因此 动态分配是一个只能增加但不会减少的授权获取方式。

自定义分配：选择此项后，下方自定义分配输入框启用。手动输入需要分配给下级控制中心的授权台数。

Q：如果授权方式选择动态分配或自定义分配，上下级中心网络通信故障时是否会有影响。

A：会有影响。当出现通信故障时，下级中心的授权状态会变更为未授权，终端无法上线。

Q：为什么在点击登录下级中心时提示“连接失败，中心加密方式不统一”？

A：如上下级中心的加密方式不同（即一个中心使用了 SSL 加密，另一中心未启动该选项）则会弹出该提示。可手动输入下级中心的地址和账号密码登录或统一加密设置。

3.中心迁移

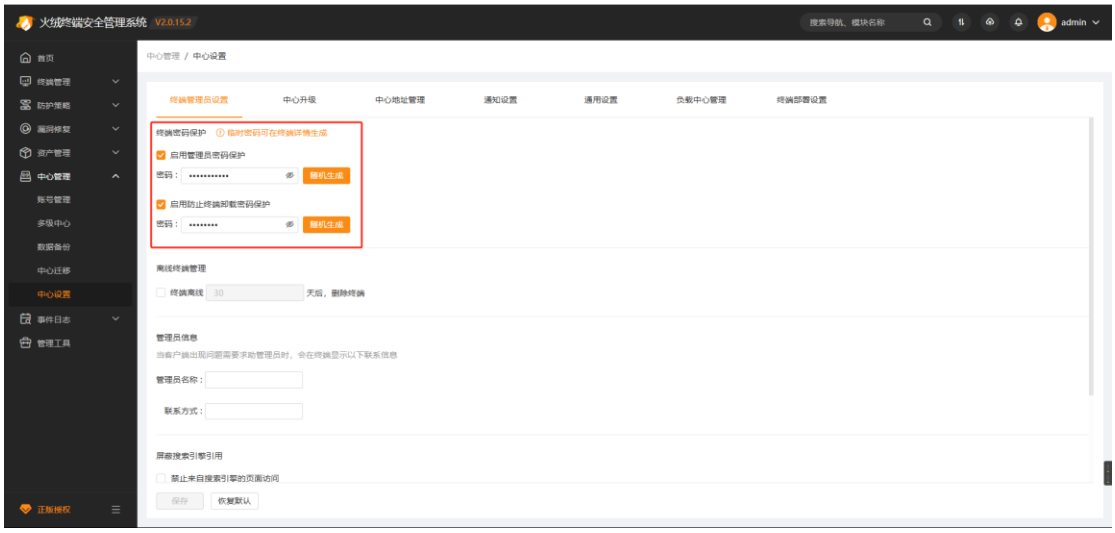
Q：中心迁移需要满足什么条件?

A：终端与新中心、旧中心三者的网络两两连通，否则可能会导致终端无法迁移成功；新旧中心的配置，需要内存硬盘等保持一致或者新中心配置更高。

4.中心设置

Q：是否可以禁止终端用户修改设置、退出和卸载火绒？如何设置？

A：火绒企业版支持设置密码保护，第一个密码可限制终端修改设置和退出火绒终端；第二个密码可限制终端用户随意卸载火绒。



Q：长时间没有上线的终端删除，如何操作？

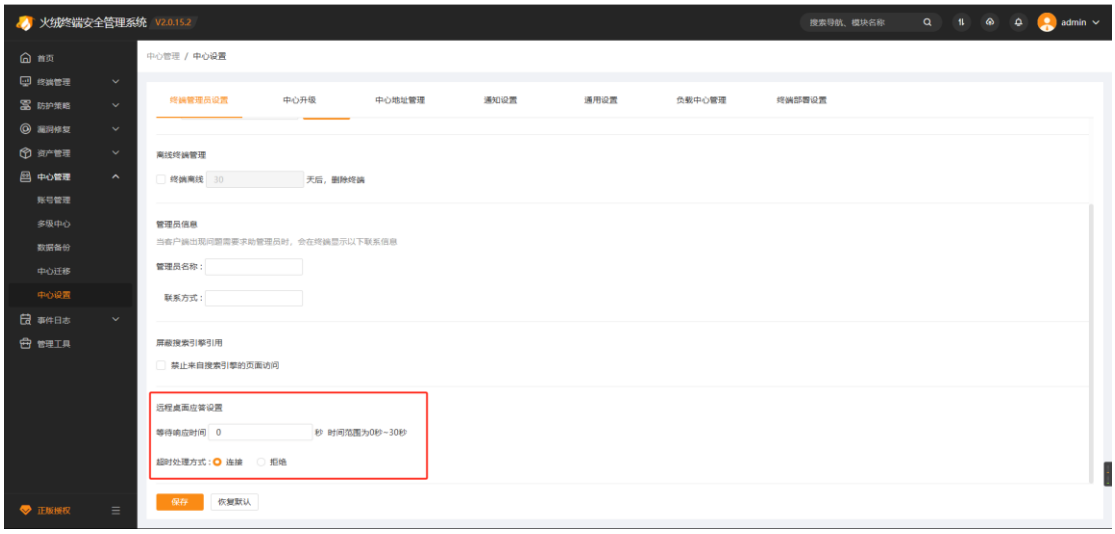
A：可开启离线终端管理，开启后可以自动删除长时间没有上线的终端。天数可以在 7-180 之间自定义。

Q：屏蔽搜索引擎引用的作用是什么？

A：主要针对公网部署用户，开启后，控制中心地址不会通过搜索引擎搜索到。

Q：远程桌面是否可以设置不经终端同意直接远程？

A：可以，响应时间调整为 0，超时选择允许即可，如图。



Q：中心地址管理的作用是什么？

A：在这里添加的地址，如终端离线后，会尝试连接这里的中心，连接成功后可接受其他控制中心的管理。如终端机器经常去其他区域的公司出差，可以考虑使用该功能，在出差期间可正常接受管控。

Q：邮件告警中的发件邮箱配置，如何填写？

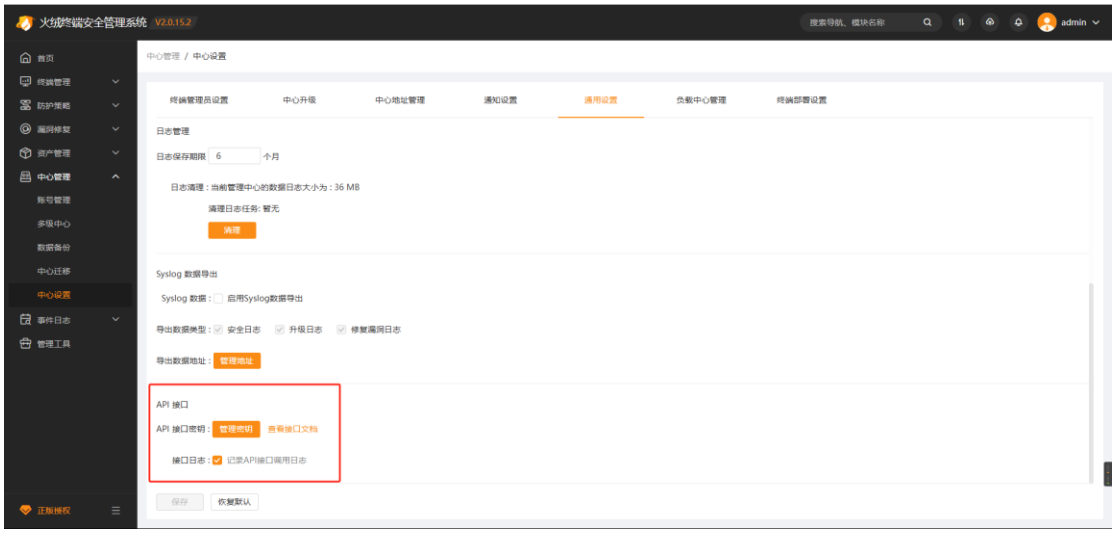
A：常见邮箱（如 QQ、网易 163、126 等）可依据官方指引进行设置，密码一般为独立授权码。企业单独部署的邮件服务请依据邮件服务说明进行设置。

Q：时间同步功能是以什么时间为标准呢？

A：以安装控制中心的系统时间为标准，终端会同步控制中心的系统时间。

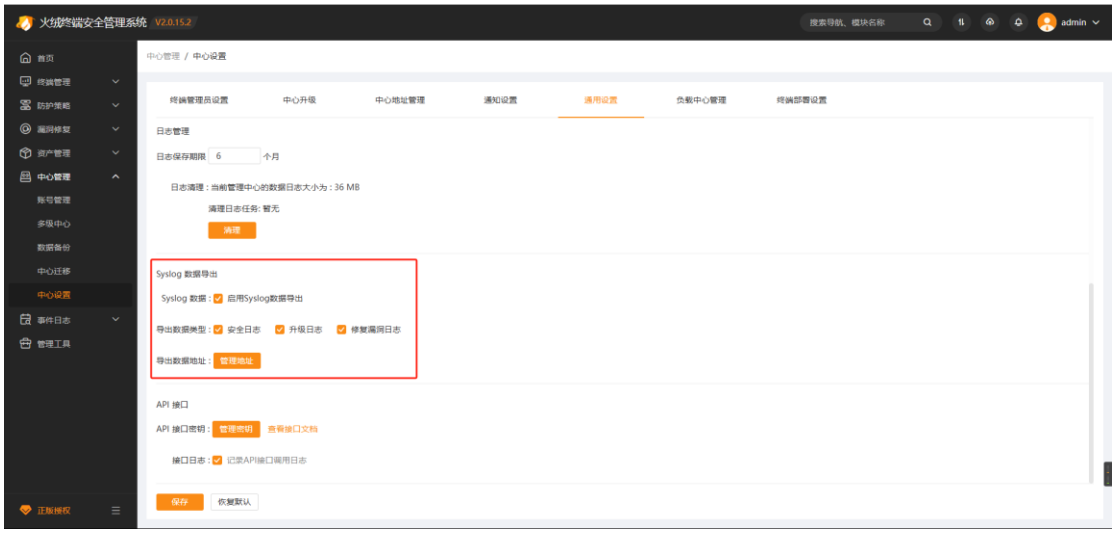
Q：火绒是否有提供 API 接口？支持哪些功能？

A：有 API 接口，详情可以登录中心后点击中心管理-中心设置-通用设置中 API 接口，如图：



Q：火绒是否可以将中心日志导出至其他平台?

A：支持。火绒的 syslog 导出功能可以将日志导出至其他的 syslog 服务器。



事件日志

Q：安全事件总览中这两个颜色的区别是什么意思?

A：是在线和离线的区别，灰色为离线，蓝色为在线。

Q：为什么中心日志的时间和终端日志的时间不一致呢?

A：终端日志的时间为实际时间，中心的日志时间为日志上传到中心后解析完成的时间。

Q：事件日志中的数据导出管理，作用是什么?

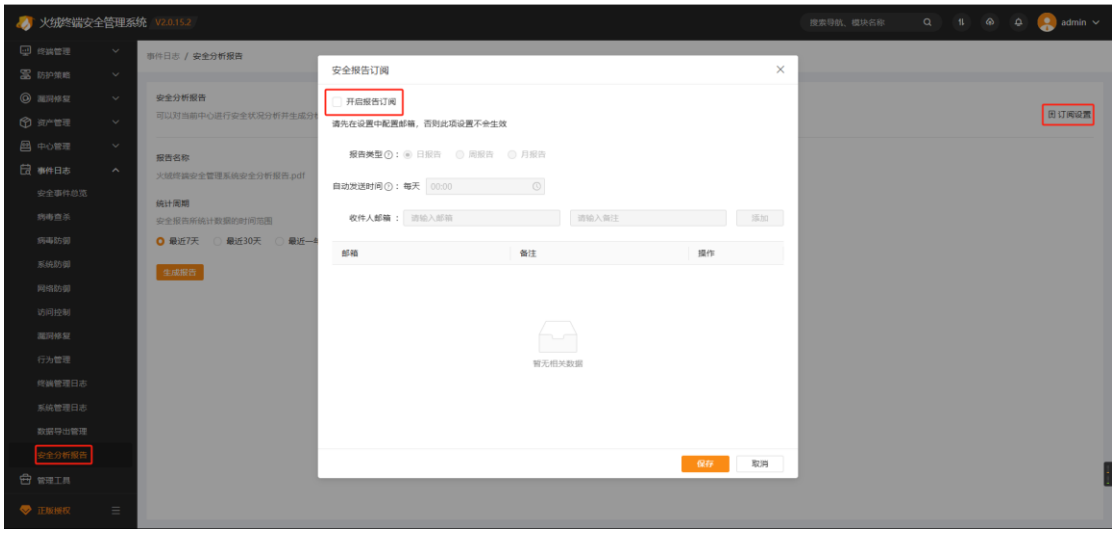
A：管理员导出的全部数据都会在这里展示，并支持再次下载和删除等操作。

Q：安全分析报告是否支持导出 word 版本?

A：暂不支持，目前只有 pdf 版本。

Q：是否可以定时将安全分析报告发送到指定邮箱?

A：支持，开启订阅即可。



管理工具

Q：火绒是否支持域环境下的部署?

A：支持域部署，可以使用火绒的域部署工具进行配置，如选择开机脚本并静默安装，则无需系统的管理员权限。(说明文档在下载按钮旁)

Q：控制中心不能连接互联网，如何激活授权/如何更新?

A：使用离线升级工具可以更新授权和病毒库。(说明文档在下载按钮旁)

Q：想修改 Windows 终端连接的控制中心地址，如何修改?

A：在控制中心下载中心迁移工具，双击运行后输入新的中心地址即可。

其他

Q：中心登录黑屏

A：排查方法：

1.端口是否冲突

2.监测工具是否提示异常，截图（可以看到中心版本）

3.提取日志：

火绒控制中心的监测工具日志；

C:\ProgramFiles(x86)\Huorong\ESCenter\log 文件夹以及 daemoncenter.exe.log；

C:\Program Files(x86)\Huorong\ESCenter\nginx 目录下的 logs 文件夹

Q：漏洞修复安装失败

A：Windows7 与 server2008R2 系统，可尝试先安装【万能补丁】:

（需联网使用）万能补丁下载地址：

https://down5.huorong.cn/tools/hr_patch_install_tool.exe

无法连接互联网环境，可访问地址手动下载：

32 位：

http://download.windowsupdate.com/d/msdownload/update/software/crup/2014/10/windows6.1-kb947821-v34-x86_49649cb633aa4ff044cd70602ac777a0ec6f8630.msu

64 位：

http://download.windowsupdate.com/d/msdownload/update/software/crup/2014/10/windows6.1-kb947821-v34-x64_cc4a605bcda8288af75983312e8fb25367e98fdd.msu

Q：漏洞修复下载失败

A：排查方法：

1.内网——中心是否使用离线升级工具下载同步了补丁，是否勾选了从中心下载补丁，终端是否正常在线；

2.中心外网终端内网——是否勾选了从中心下载补丁，终端是否正常在线，是否可以 ping 通微软域名；

3.外网——终端是否可以 ping 通微软域名

download.windowsupdate.com

download.microsoft.com

catalog.sf.dl.delivery.mp.microsoft.com

Q：sha2 签名补丁下载失败

A：可以下载补丁后手动安装

系统	补丁号	下载地址
Server 2008 R2 x64 sp1	KB4474419	http://download.windowsupdate.com/c/msdownload/update/software/secu/2019/09/windows6.1-kb4474419-v3-x64_b5614c6cea5cb4e198717789633dca16308ef79c.msu
Win7 x64 sp1	KB4474419	http://download.windowsupdate.com/c/msdownload/update/software/secu/2019/09/windows6.1-kb4474419-v3-

		x64_b5614c6cea5cb4e198717789633dca16308ef79c.msu
Win7 x86 sp1	KB4474419	http://download.windowsupdate.com/c/msdownload/update/software/secu/2019/09/windows6.1-kb4474419-v3-x86_0f687d50402790f340087c576886501b3223bec6.msu
Server 2008 x64 sp2	KB4474419	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/09/windows6.0-kb4474419-v4-x64_09cb148f6ef10779d7352b7269d66a7f23019207.msu
Server 2008 x86 sp2	KB4474419	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/09/windows6.0-kb4474419-v4-x86_fd568cb47870cd8ed5ba10e1dd3c49061894030e.msu
Vista x64 sp2	KB4474419	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/09/windows6.0-kb4474419-v4-x64_09cb148f6ef10779d7352b7269d66a7f23019207.msu
Vista x86 sp2	KB4474419	http://download.windowsupdate.com/d/msdownload/update/software/secu/2019/09/windows6.0-kb4474419-v4-x86_fd568cb47870cd8ed5ba10e1dd3c49061894030e.msu

Q：sha2 签名补丁安装失败：

A：可尝试先安装【万能补丁】补丁安装后重启电脑再尝试安装 sha2 签名补丁：

（需联网使用）万能补丁下载地址：

https://down5.huorong.cn/tools/hr_patch_install_tool.exe

无法连接互联网环境，可访问地址手动下载：

32 位：

http://download.windowsupdate.com/d/msdownload/update/software/crup/2014/10/windows6.1-kb947821-v34-x86_49649cb633aa4ff044cd70602ac777a0ec6f8630.msu

64 位：

http://download.windowsupdate.com/d/msdownload/update/software/crup/2014/10/windows6.1-kb947821-v34-x64_cc4a605bcda8288af75983312e8fb25367e98fdd.msu

Q：从中心下载组件失败

A：排查方法：

1.重新下载再次安装

2.专杀扫描重启电脑后再次下载安装

3.检查网络是否有限制

4.确认中心版本和病毒库时间（大概率中心病毒库时间是 1970-01-01）

a）手动尝试升级

b）使用离线升级工具进行升级

c）卸载中心那台机器上的终端，然后重启—右键中心图标—属性—打开文件所在位置，找到 upgrade 这个文件夹，打开删除里面的数据，然后再打开中心手动升级，升级完成后重新下载终端安装包进行部署

Q：远程桌面黑屏

A：1）端口是否有限制

2）是否开启防火墙或其他安全软件拦截

3）重启中心服务尝试能否恢复

Q：手机微信小程序口令没有了，终端如何清除掉终端动态口令

A：电脑重启后进入系统安全模式，将以下位置删除

文件：\Huorong\ESEndpoint\bin\HrCredProv*.dll

注册表：计算机

\HKEY_LOCAL_MACHINE\SOFTWARE\Huorong\ESEndpoint\app\totp