奇固科威厂站网络安全监测软件(HKW-AGENT 探针)
使用说明书 V1.4.2

杭州奇固科威信息安全技术有限公司

2025 年 02 月 26 日

目录

HKW-AGENT 探针使用说明

版本：Ver 1.1.3

一、安装前准备工作

1. 安装包确认

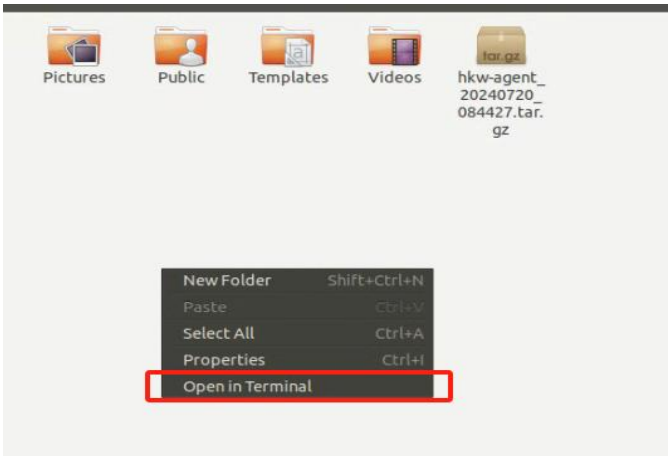
安装包名称：hkw-agent_[System]_[Version]_[yyyymmdd]_[hhmmss].tar.gz（如图示 1）

图示 1：安装包名称

2. 安装包解压

（1）将安装包文件放置在用户根目录下(/home/[user]/，非 root 用户根目录)（如图示 1）

（2）在该目录右键选中`Open in Terminal`或`打开终端`（如图示 2）

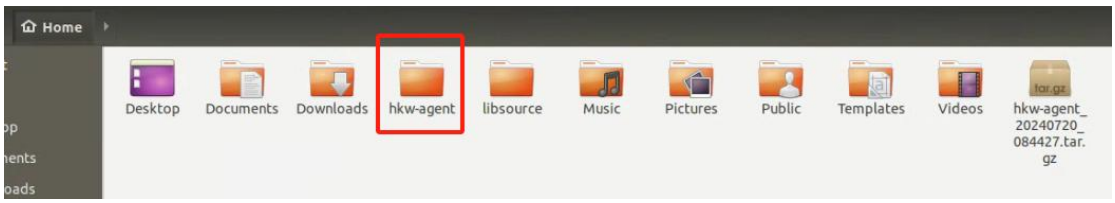


图示 2：打开终端

（3）在终端中执行`tar -zxvf hkw-agent_[System]_[Version]_[yyyymmdd]_[hhmmss].tar.gz`命令后会生成一个`hkw-agent`新文件夹（如图示 3、4）

```
linkqi@linkqi:~$ tar -zxvf hkw-agent_20240810_115816.tar.gz
hkw-agent/
hkw-agent/stop_service.sh
hkw-agent/cmdmgr_start.sh
hkw-agent/uninstall_service.sh
hkw-agent/restart_service.sh
hkw-agent/start_service.sh
hkw-agent/lib/
hkw-agent/lib/libinotifytools.so
hkw-agent/lib/libcrypto.so.1.1
hkw-agent/lib/libboost_iostreams.so.1.65.1
hkw-agent/lib/libudev.so
hkw-agent/lib/libboost_thread.so.1.65.1
hkw-agent/lib/libboost_system.so.1.65.1
hkw-agent/lib/liblog4cplus-2.0.so.3
hkw-agent/lib/libboost_iostreams.so
hkw-agent/lib/libssl.so.1.1
hkw-agent/lib/libcrypto.so
hkw-agent/lib/libboost_filesystem.so
hkw-agent/lib/libssl.so
hkw-agent/lib/libboost_system.so
hkw-agent/lib/libboost_thread.so
hkw-agent/lib/libboost_filesystem.so.1.65.1
hkw-agent/lib/liblog4cplus.so
hkw-agent/bin/
hkw-agent/bin/hkw-agent
hkw-agent/bin/hkw-agent-cmdmgr
hkw-agent/config/
hkw-agent/config/.keyfilepaths.bak
hkw-agent/config/ConfigSet.ini
hkw-agent/config/keyfilepaths
hkw-agent/config/.portwhitelist.bak
hkw-agent/config/portwhitelist
hkw-agent/config/.ConfigSet.ini.bak
hkw-agent/config/networkwhitelist
hkw-agent/config/.networkwhitelist.bak
hkw-agent/status_service.sh
```

图示 3：解压命令输入

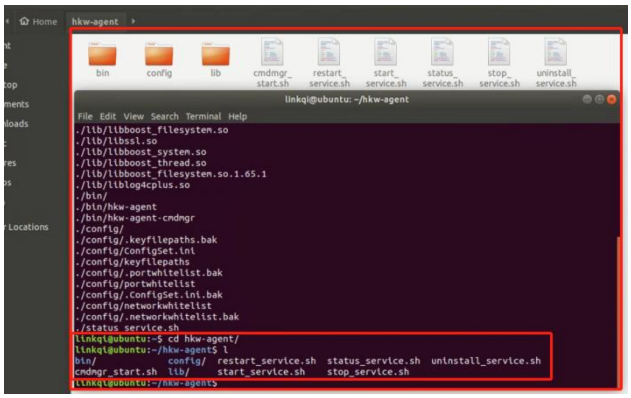


图示 4：解压完成

二、激活

1. 进入软件目录

双击`hkw-agent`文件夹进入或终端输入`cd hkw-agent`（如图示 5）

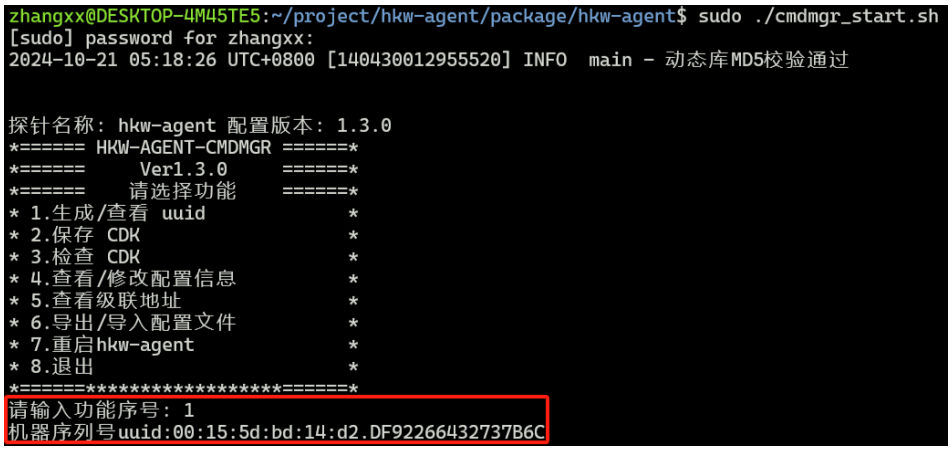


图示 5：hkw-agent 内文件及终端命令

2.获取用户 uuid 及保存授权

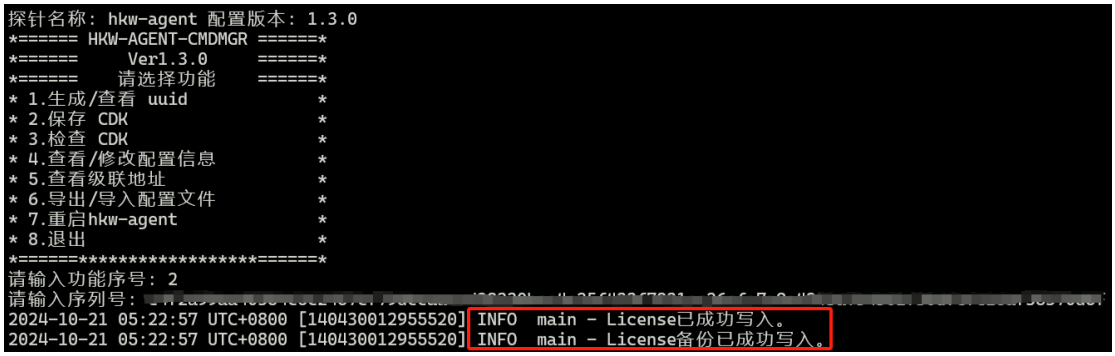
（1）获取 uuid，在命令行执行`sudo ./cmdmgr_start.sh`启动配置工具，在主菜单输入 1，将获取到的用户 UUID 完整提供给相关人员以获取设备激活码（如图示 6、7）

图示 6：运行配置文件，生成 uuid



图示 7：生成提示

（2）保存激活码(CDK)，主菜单输入 2，选择“保存 CDK”功能，在“请输入序列号：”后面输入获取到的激活码，等待返回“License 已成功写入。”即完成授权激活；或将获取到的 license.key 文件放置于”/etc/hookwe/hkw-agent/”目录下，目录不存在需自行创建；检测授权是否匹配。（如图示 8）



图示 8：保存激活码

（3）检测激活码（CDK）是否有效，CDK 有效会显示“License 有效”，CDK 无效会显示“License 无效”（如图示 9）

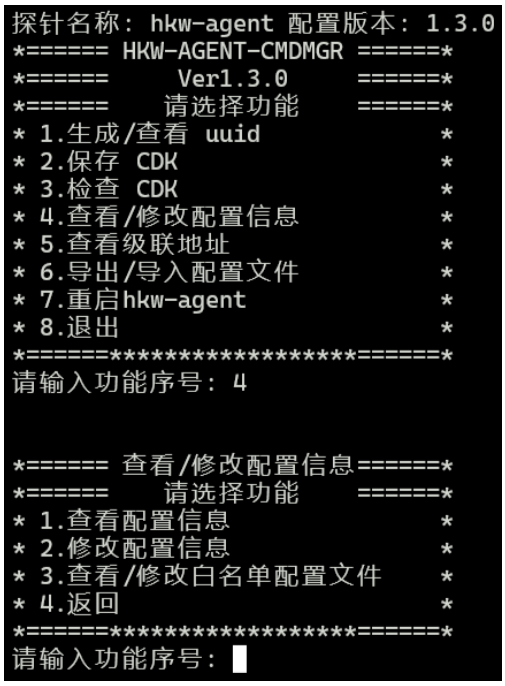
图示 9：检查 CDK

三、使用命令行工具修改配置信息

1.设置远程调试、级联地址

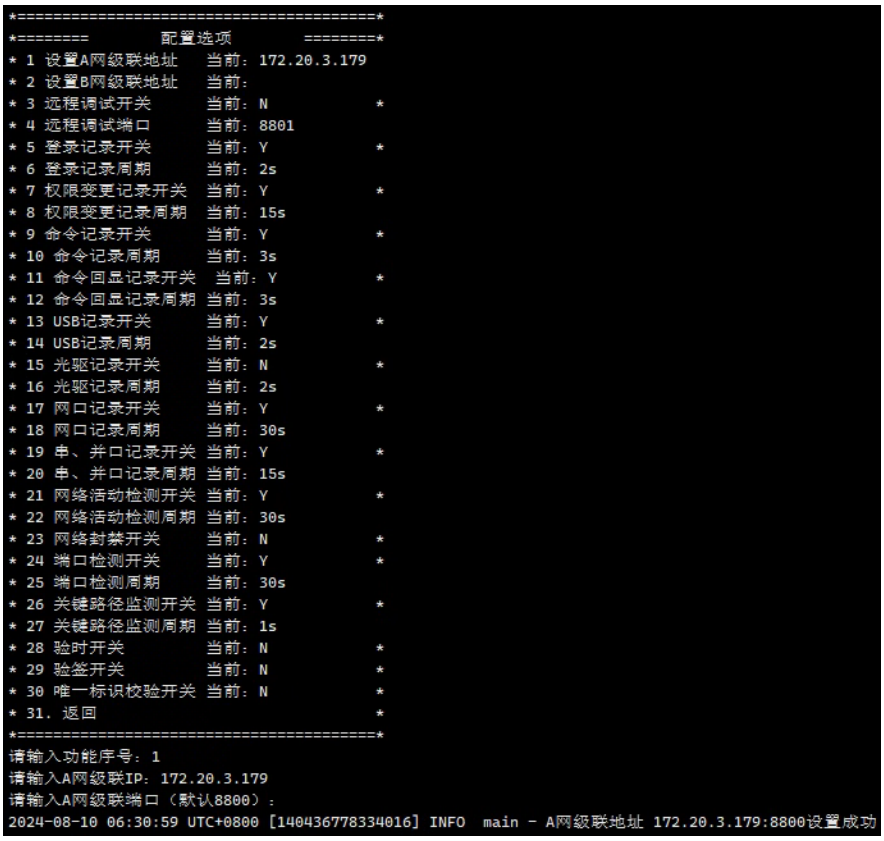
激活完成后，在主菜单输入 5，二级菜单选择“修改配置信息”。设置远程调试：选择设置远程调试开关（默认关闭），开启后可使用图形化界面设置探针相关功能；设置级联地址：选择设置 A 网级联地址（若单网安地址推荐优先设置 A 网级联），分别输入网安地址、网安端口（端口默认 8800），出现“A 网级联地址

xxx.xxx.xxx.xxx:xxxx 设置成功”表示级联地址设置成功；查看级联地址：在主菜单输入 6 即可查看已设置级联地址信息（如图示 10、11、12、13）

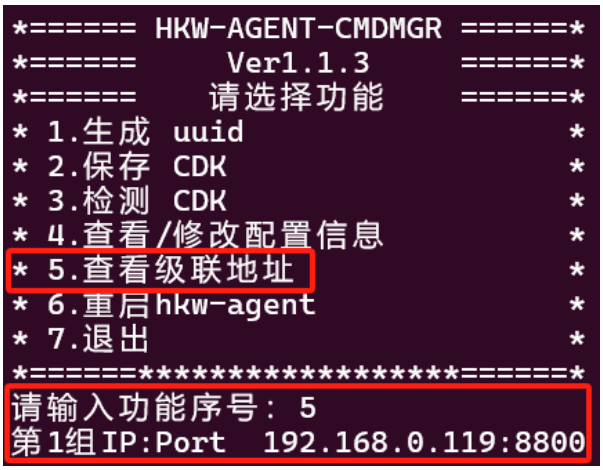


图示 10：修改配置信息

图示 11：配置菜单选项详情



图示 12：配置网安地址



图示 13：查看级联地址

2. 设置检测项功能启停

配置菜单选项中，支持以下功能记录控制：

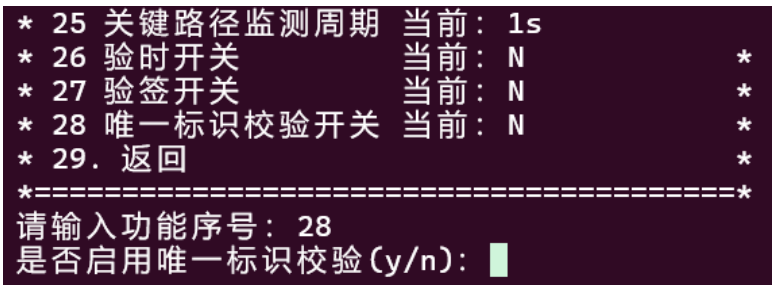
（1） 远程调试：远程调试开启功能后，可使用图形化配置工具对探针进行配置

（2） 登录记录：对用户本地、GUI、ssh 等方式登录进行记录及上报

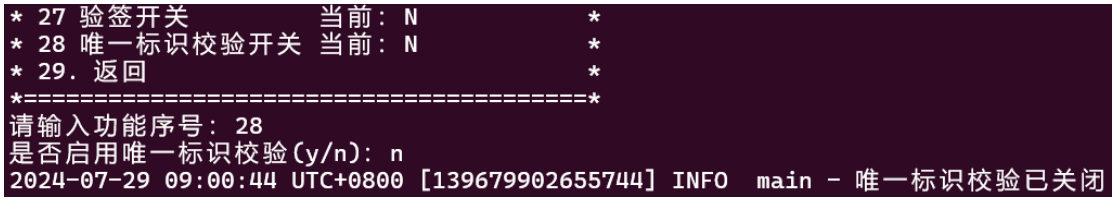
（3） 权限变更记录：对用户添加、删除、修改密码和修改用户组行为进行记录及上报

（4） 命令记录：对命令行命令进行记录及上报
（5） 命令回显记录：对命令行系统输出信息进行记录及上报
（6） USB 记录：对 U 盘设备使用情况进行记录，插入、拔出等操作发现 U 盘设备插入则及时上报
（7） 光驱记录：对光驱存在，读取和推出等事件进行记录及上报
（8） 网口记录：检测网口是否存在接入，或存在拔出情况进行记录及上报
（9） 串、并口记录：对串、并口占用和释放事件进行记录及上报，用户需根据实际情况对串、并口名称进行设置
（10） 网络活动检测：用户手动设置许可网络连接服务白名单，此功能会记录未在白名单允许的网络活动，并将检测异常数据上报
（11） 网络封禁：对检测到的非白名单网络连接进行封禁操作，封禁为临时行为，重启后失效；网络封禁依赖于网络活动检测，网络检测无数据捕获着
（12） 端口检测：用户手动设置许可端口服务白名单，此功能会记录未在白名单允许的端口活动，并将检测异常数据上报
（13） 关键路径监测：用户手动设置监测文件或目录绝对路径，设置监测的文件或目录出现增加、变更、删除和权限修改操作时会触发记录和上报
（14） 验时：开启时间校验功能
（15） 验签：开启签名校验功能
（16） 唯一标识校验：开启唯一标识校验

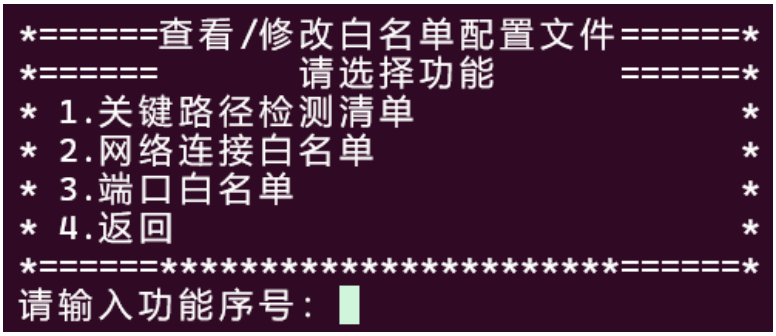
网络活动、端口和关键路径监测需先在“查看/修改配置信息”->“查看/修改白名单配置文件”中设置需要启动功能项白名单，避免出现服务启动失败问题（如图 14、15、16、17）



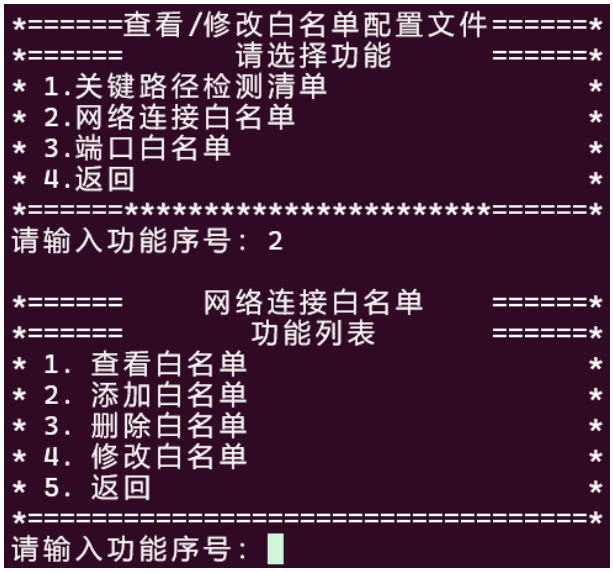
图示 14：功能开关



图示 15：启动/关闭均有信息返回结果



图示 16：白名单配置项



图示 17：白名单编辑功能项

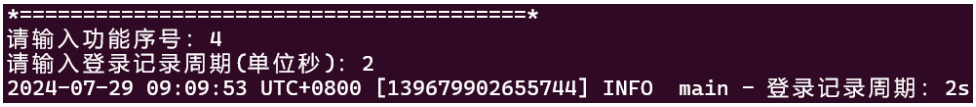
3. 设置检测项周期

配置菜单选项中，支持以下功能监测周期修改：

（1） 登录记录周期，单位秒
（2） 权限变更记录周期，单位秒
（3） 命令记录周期，单位秒
（4） 命令回显记录周期，单位秒
（5） USB 记录周期，单位秒
（6） 光驱记录周期，单位秒
（7） 网口记录周期，单位秒
（8） 串、并口记录周期，单位秒
（9） 网络活动检测周期，单位秒
（10） 端口检测周期，单位秒
（11） 关键路径检测周期，单位秒

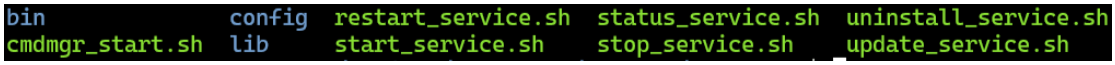
如图示 18、19

图示 18：检测周期修改



图示 19：修改完成后提示信息

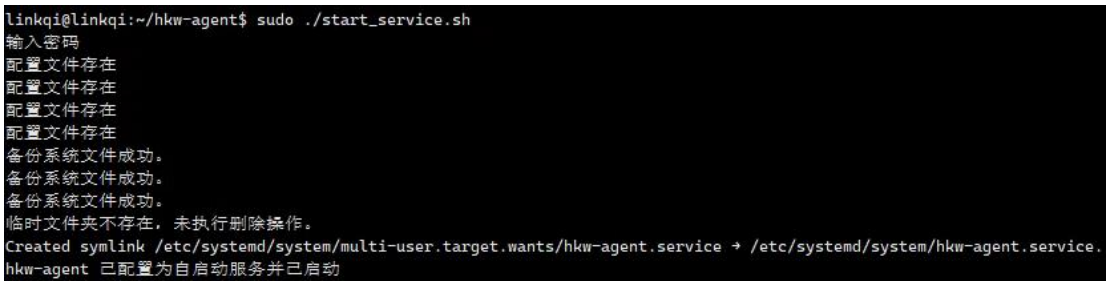
在非首次部署时修改完配置信息或白名单文件，需重启探针服务使其生效，可使用配置工具重启服务，或执行重启脚本`sudo ./restart_service.sh`；脚本需以 root 用户权限运行。（如图示 19）



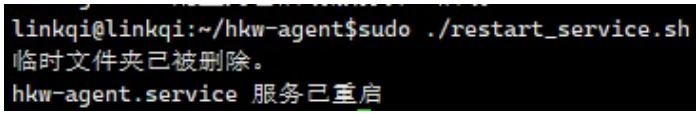
图示 20：探针相关脚本

四、 首次启动

在修改配置文件完成后，以 root 用户权限执行`./start_service.sh`，`start_service.sh`脚本仅在首次启动时使用，此脚本会将探针服务部署自启动相关服务，并完成相关环境部署；后续修改配置文件后，已 root 用户权限执行`./restart_service.sh`重启服务让配置文件修改生效。（如图示 20、21、22）



图示 21：执行启动脚本信息



图示 22：执行重启脚本信息

五、 使用 GUI 配置工具修改配置信息（可选）

1. GUI 工具使用前置条件

GUI 配置工具依赖探针相关功能才可正常使用，依赖功能如下：

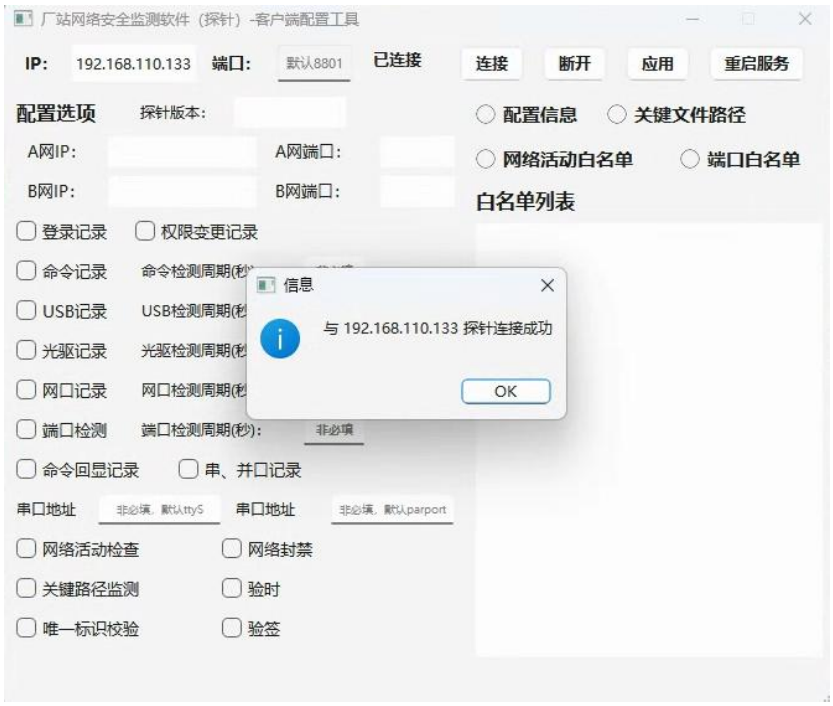
（1） 需要激活探针
（2） 需要使用命令行配置工具开启远程调试功能
（3） 需要执行`start_service.sh`启动探针

2. GUI 配置工具使用指南

(1)连接探针

GUI 配置工具（如图示 23）需要在 IP 地址输入探针设备 IP 地址，端口默认 8801，输入 IP 及端口后点击连接，连接结果会跳出提示信息（如图示 24）。

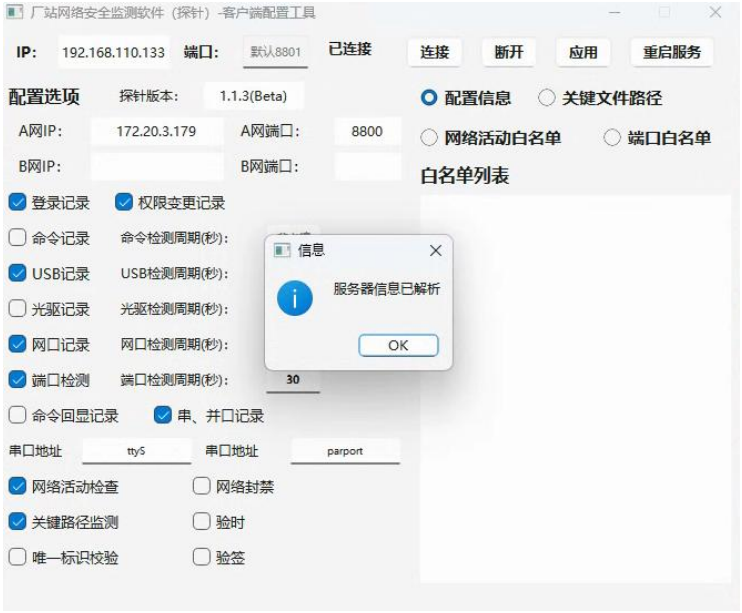
图 23：GUI 配置工具



图示 24：连接探针提示

(2)获取、修改探针信息

在与探针建立远程连接后会自动显示当前探针配置信息，配置选项只有启用项勾选框显示勾选、信息栏显示信息（如图示 25）；设置探针启动项，勾选相关项目即可，需要设置周期的项目自行设置检测周期（单位：秒），串、并口记录项需要用户设置需要检测的串、并口地址，如：串口 ttyS、并口 parport。



图示 25：探针信息项显示

(3)应用探针修改配置

在设置完成配置项目后，点击应用按钮将设置应用，应用完成会有信息提示。（如图示 26）

图示 26：保存探针设置信息

(4)获取、修改关键文件路径信息

获取当前探针配置信息需要选中"关键文件路径"，信息会显示在白名单列表，可在白名单列表中修改相关内容。（如图示 27）

图示 27：获取关键文件路径信息

(5)应用修改后信息

在修改完关键文件路径内容后，点击保存按钮将内容保存，保存完成会有信息提示。（如图示 28）

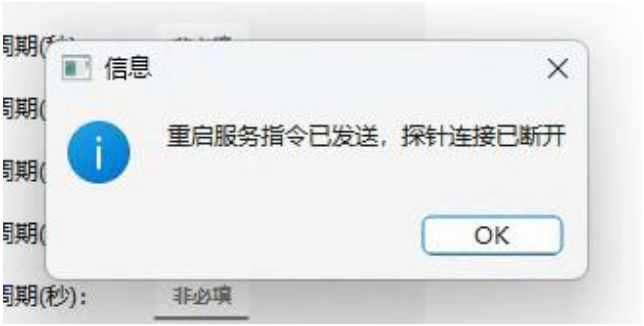
图示 28：保存修改内容

(6)网络活动、端口白名单修改回传

参考关键文件路径获取、修改及回传步骤完成设置。

(7)重启探针

所有修改项修改后均需重启服务后生效，点击重启服务按钮，向探针发送重启指令，即可完成探针配置修改。（如图示 29）



图示 29：执行重启指令发送

六、 停止服务

若想暂时停止探针服务，可以 root 用户权限执行`./stop_service.sh`，用以暂时停止服务功能，停止功能在未重启服务或设备时有效。（如图示 20、30）

```
linkqi@linkqi:~/hkw-agent$sudo ./stop_service.sh
临时文件夹已被删除。
停止 hkw-agent.service 服务...
hkw-agent.service 服务已停止
```

图示 30：执行停止脚本信息

七、 卸载服务

如若结束探针服务使用，使用 root 权限运行`./uninstall_service.sh`脚本，完全停止服务，清除自启动项，卸载并删除服务各项文件及运行记录。（如图示 31）

```
linkqi@linkqi:~/hkw-agent$ sudo ./uninstall_service.sh
系统文件已恢复。
系统文件已恢复。
临时文件夹不存在，未执行删除操作。
停止 hkw-agent.service 服务...
禁止 hkw-agent.service 自启动...
Removed /etc/systemd/system/multi-user.target.wants/hkw-agent.service.
卸载 hkw-agent.service 服务...
hkw-agent.service 删除成功
hkw-agent 卸载完成...
```

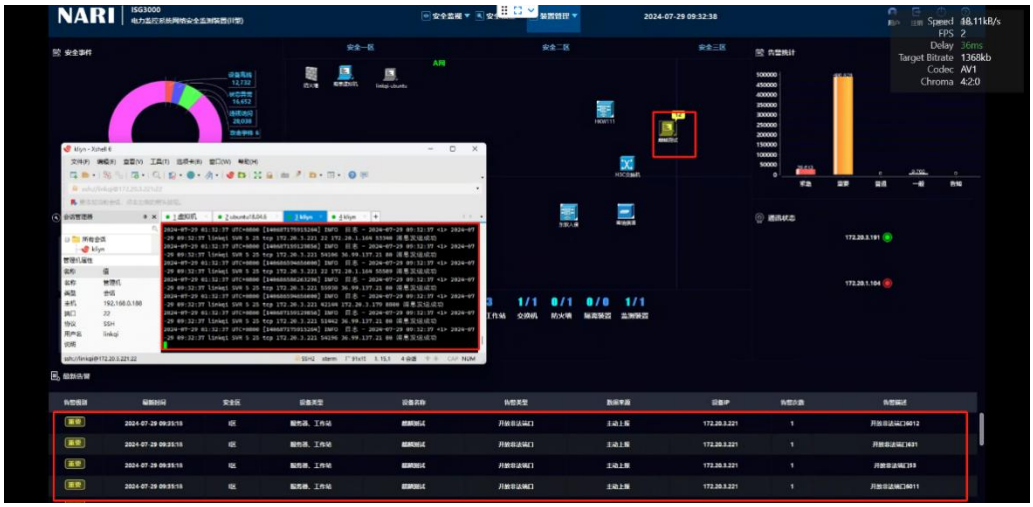
图示 31：卸载探针服务

八、 更新服务

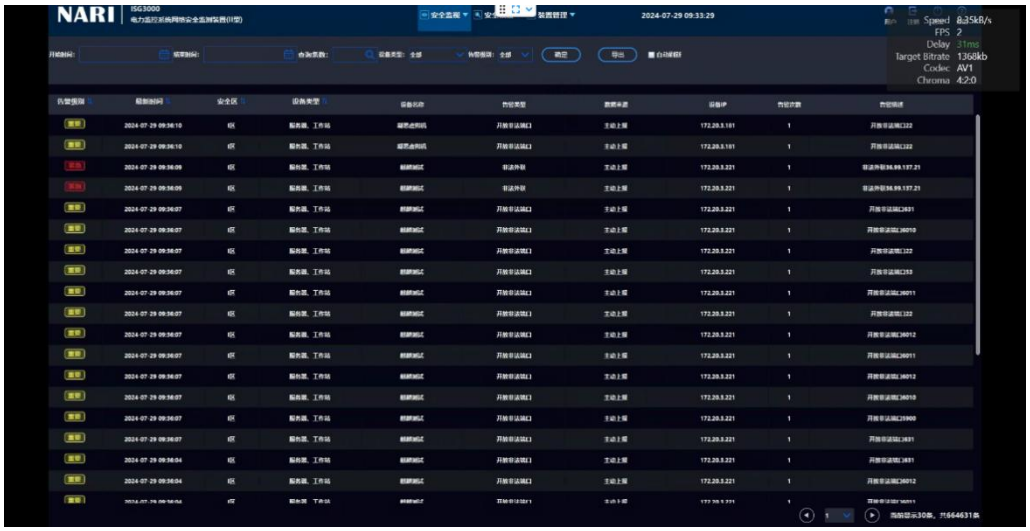
若需要更新服务将安装包改名为`update.tar.gz`，将安装包放置在`xxx/hkw-agent/`目录下，使用`./ update_service.sh`执行更新操作。

探针与网安

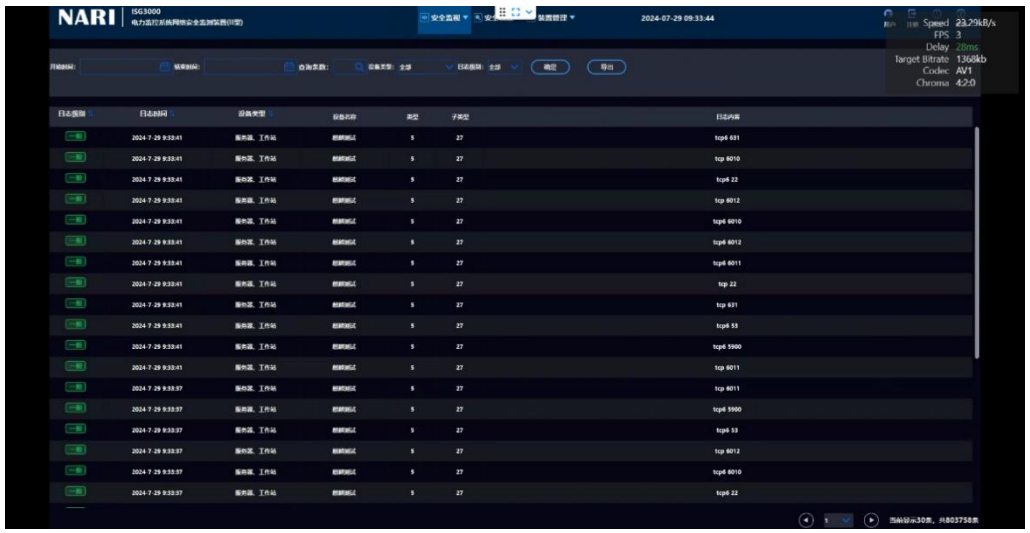
探针成功与网安建立连接后，可在网安中查看探针在线状态及回传相关信息，以下仅供展示，界面以实际项目网安为主。（如图示 32、33、34）



图示 32：探针与网安



图示 33：探针上传信息



图示 34：网安事件列表

注：软件版本可能存在不同，以实际产品为准。