

迪康终端安全管理系统

问题处理手册

迪康大成科技有限公司

V.2606

一、 迪康客户端安装失败

原因一：360 软件拦截

验证方法：查看杀毒软件隔离区是否存在迪康文件

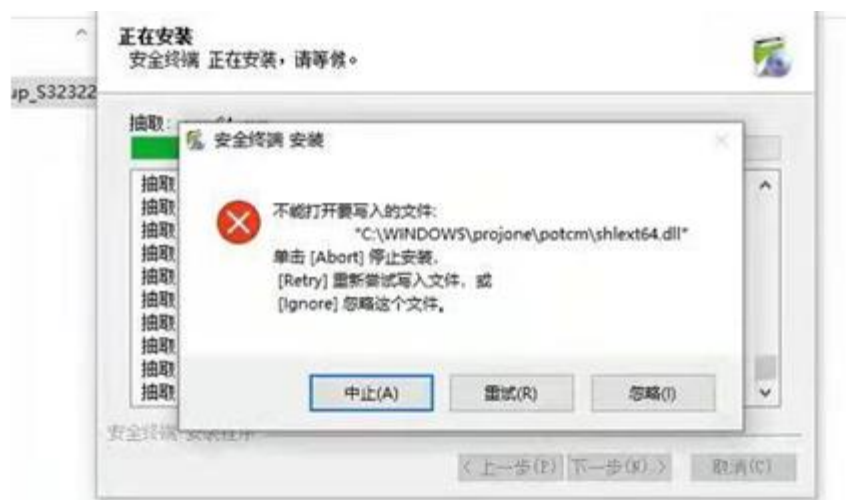


解决办法：临时退出杀毒软件，重新允许安装程序



原因二：程序被占用

现象：



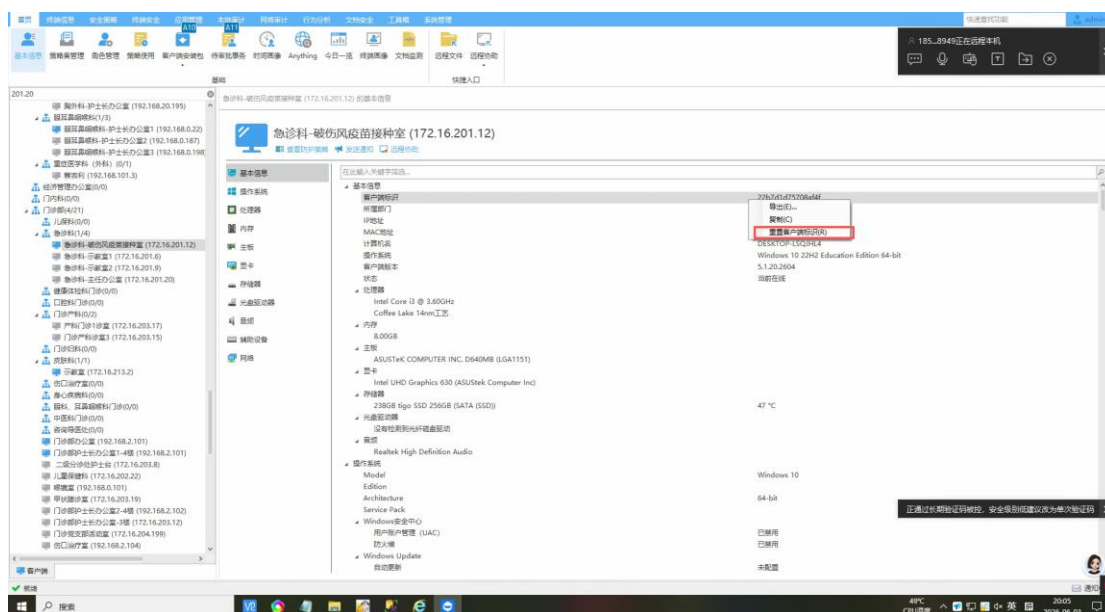
原因：程序被占用，或者电脑做了磁盘保护，c:/windows/下禁止写入文件。

解决办法：点击忽略，即可安装成功

二、安装客户端后控制台看不到或反复上线、下线。

现象：表现为安装客户端后控制台上看不到；控制台上客户端地址一直在变化；控制台上显示客户端反复上线、下线。

解决办法：控制台按住 shift，右击客户端标识处，重置客户端标识，被重置的客户端会去到未分组里面，重新备注分配组织架构即可。



三、 客户端未上线排查步骤

一、客户端侧排查（前台操作）

1. 呼出客户端信息窗口：按下 Ctrl+Shift+Alt+Y，检查是否能弹出客户端信息窗口。
 - 不能弹出：直接重新安装客户端（建议先退出杀毒软件）。
 - 能弹出：进入下一步。
2. 验证服务器地址：检查客户端中配置的服务器地址是否与目标服务器 IP 一致。
 - 不一致：修改为正确的服务器 IP（默认密码：123456）。
3. 检查通信环境：暂时退出杀毒软件、防火墙等安全软件；使用 ping 命令测试客户端与服务器的网络连通性。
4. 检查服务器磁盘空间：登录服务器，确认客户端所在磁盘的剩余空间是否充足（空间满会导致服务异常）。

二、后台深度排查（命令行/日志）

（一）客户端进程与卸载界面

1. 尝试呼出卸载界面。
 - 若能呼出：跳至（二）。
 - 若不能呼出：执行以下检查：

```
tasklist | find "pobus64.exe"
tasklist | find "poda32.exe"
tasklist | find "poda64.exe" （64 位系统需检查此项）
```

若上述任意进程缺失，说明客户端未正常运行。处理：关闭杀软，重新安装客户端并重启系统。
若进程都在但卸载界面仍无法呼出，可能是热键冲突。手动执行
C:\windows\projone\potcm\clientstat.exe，若成功弹出则正常；否则说明客户端组件被破坏。处理：关闭杀软重装；若无法重装，可将 pobus、poda 相关文件改名，再执行 taskkill /f /im pobus64.exe 等命令，之后重新安装客户端。

（二）网络与端口连通性

2. 检查客户端与服务器的 13001 端口连接：netstat -ano | find "13001"
 - 若有连接（且进程为 pobus）：跳至（三）。
 - 若无连接：按顺序排查：
 - 2.1 测试网络层：ping 服务器 IP。不通则检查服务器防火墙是否关闭，确认网络链

路。

2.2 测试端口可达性: telnet 服务器 IP 13001。若系统无 telnet, 可通过控制面板安装。

连接失败时: 在服务器上执行 `netstat -ano | find "13001"` 检查端口是否监听。未监听则服务器服务未启动或异常, 检查磁盘空间, 清理后重启服务器。

从其他电脑 telnet 该服务器 13001: 能通则当前电脑防火墙拦截; 不通则服务器端防火墙拦截, 需双方放行 13001 端口。

2.3 检查客户端组件加载: 查看客户端目录下 `pomqc3/pomqc364.dll` 是否能被删除 (能删除说明未加载)。未加载则系统不支持或文件损坏, 需重装客户端。

(三) 客户端上线状态与日志

3. 查看 `pobus` 日志, 搜索是否有“上线了”字样。无则上线模块卡死, 需重启客户端或重装; 有则进入下一步。

(四) 客户端标识 (CID) 获取

4. 从注册表读取 CID: 路径 `HKLM\SOFTWARE\WOW6432Node\projone\podlp` (32 位系统去掉 `WOW6432Node`), 找到 `cid` 值并复制。若不存在则客户端被破坏, 退出杀软后重装; 存在则进入下一步。

(五) 服务器端连接验证

5. 在服务器上检查客户端 IP 连接: `netstat -ano | find "客户端 IP 地址"`。无连接则网络仍有问题; 有则进入下一步。

(六) 服务器业务日志与 MQ 服务

6. 检查服务器日志中的 CID 记录: 进入服务器安装目录下的 `/log/pobusiness` (Linux 为 `latestlog`), 搜索步骤 4 复制的 CID, 查找“client online on mq:客户端标识”。
 - 找到: 跳至 (七)。
 - 未找到: 执行以下子检查:
 - 6.1 使用测试工具 `testPomqc3_CSharp.exe` 验证 MQ。配置服务器地址、端口 13001, 总机号 `default`, `channel` 为“`getsubers`”, `request` 为“`{channel:clients}`”, 点击 Request 查看 Response。

无 Response 则 MQ 服务异常, 重启 `pomqs3.exe`。

有 Response 则在返回中查找 CID: 找不到则 MQ 上未上线, 重启 `pomqs3`; 能找到则进入 6.2。
 - 6.2 检查服务器安装目录下的 `temp\clients` 文件。文件不存在则服务器写文件失败; 存在但无该 CID 则 `pomqs3` 无法写入; 有 CID 则 `pobusiness` 卡死。

（七）异常日志分析

7. 全面检索该 CID 的所有日志记录，检查是否有异常报错（如外网 IP 被封、连接超时等），据此定位问题。

四、 禁用无线网卡电脑无法联网

解决办法： 在客户端使用快捷键清空策略，平台修改策略后在客户端进行更新策略的操作 在平台取消勾选禁用无线网卡后生成离线策略在客户端导入

五、 屏幕壁纸及屏保不生效黑屏

原因： 与第三方壁纸软件冲突或被杀软拦截 一些软件会禁止进入屏保，比如视频播放器，锁屏软件(比如 360)或远程软件

解决办法： 1) 试下 windows 自带的屏保是否能用 2) 关闭第三方软件或卸载、退出杀软，若还未生效建议重启电脑

六、 远程协助黑屏

原因： 采用了其它第三方远程后，高速远程模式下有机率会出现黑屏现象 解决方法：出现这种问题后建议用户采用“兼容模式”

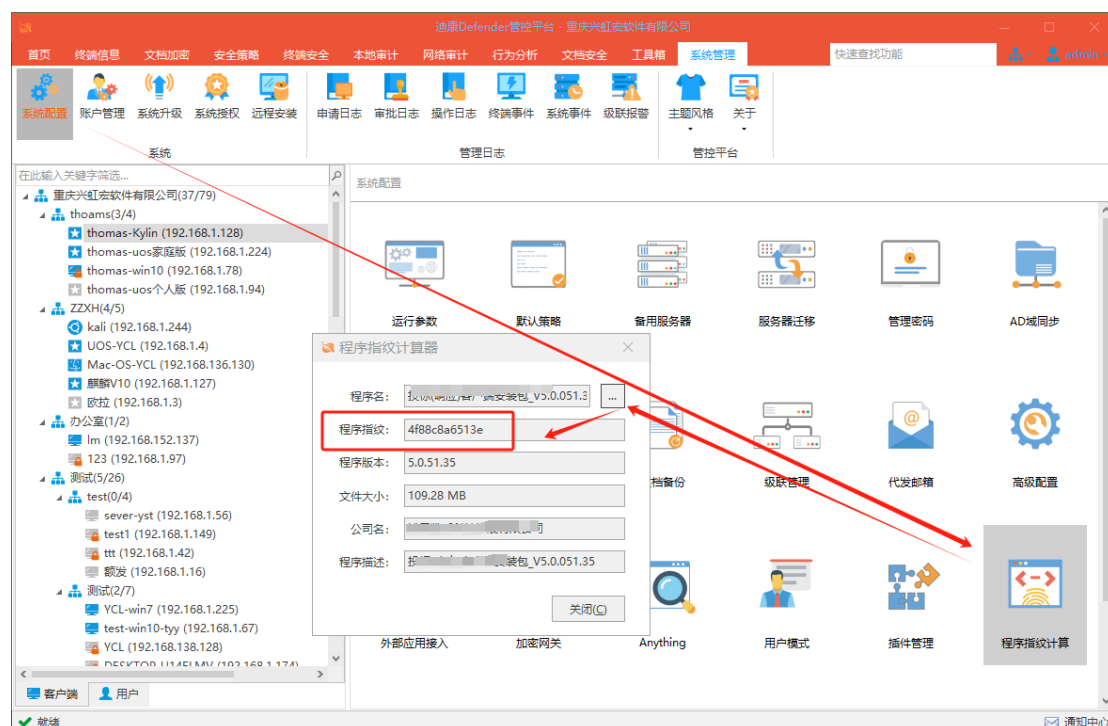
七、 开启禁止安装软件后，企业软件库内的软件提示无法安装

企业软件库安装软件时会校验安装程序与软件管理中上传的软件包的程序指纹是否一致，某些软件安装时会执行解压操作释放进程，若释放的进程与上传时的进程名不一致，无法完成 校验则无法安装。

加白方法：

获取指纹符：

将.exe 的可执行文件导入迪康控制台，通过迪康控制台获取指纹符



添加禁止安装新软件白名单：

将上一步获取到的指纹符添加白名单，并把策略应用给相应的客户端

