

许先生，您好

很高兴与您电话沟通，根据目前的案例情况，我将暂时归档此问题。**案例归档后您会收到调查问卷的邮件，希望可以对我们的服务进行评价。**

**案例总结：**

**案例描述：**

win10 政府版在未入域时可正常调用外设，入域后在未安装 TMS 安全软件的情况下，无法通过网页正常调用外设，外设驱动识别正常，请协助分析问题原因。

**案例进展：**

- 对比入域调用外设失败和未加域成功时，点击“读身份证”按钮后，发现触发问题时浏览器 Console 报错：**SCRIPT0522: SecurityError**，指向 **eloamHidExtend.min.js(268,13)**。后续引入 eloam 厂商一同排查。
- 最新：公积金系统发布新驱动，可以调用外设设备。
- 和用户沟通，可以暂时归档案例。

-----  
贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话：400-818-0055  
电子邮箱：jiawei@cmgos.com

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

**发件人:** Jia Wei

**发送时间:** 2024 年 2 月 29 日 9:42

**收件人:** ICBC 案例通知 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; 'xiaosong@jx.icbc.com.cn' <[xiaosong@jx.icbc.com.cn](mailto:xiaosong@jx.icbc.com.cn)>

**抄送:** ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>; '303642690@qq.com' <[303642690@qq.com](mailto:303642690@qq.com)>

**主题:** 回复: 回复: 【外来邮件，注意核实】 回复: [案例号: CAS-09325-J7D5T3 ] % IP2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生，肖先生，您好

**阶段性案例总结：**

- 对比入域调取外设失败和未加域成功时，点击“读身份证”按钮后，发现触发问题时浏览器 Console 报错：**SCRIPT0522: SecurityError**，指向  
**eloamHidExtend.min.js(268,13)**。后续引入 eloam 厂商一同排查。
- 最新：公积金系统发布新驱动，可以调用外设设备。

-----  
-----  
贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话：400-818-0055  
电子邮箱：jiawei@cmgos.com

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

**发件人:** Jia Wei  
**发送时间:** 2024 年 2 月 23 日 17:14  
**收件人:** ICBC 案例通知 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; 'xiaosong@jx.icbc.com.cn' <[xiaosong@jx.icbc.com.cn](mailto:xiaosong@jx.icbc.com.cn)>  
**抄送:** ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>; '303642690@qq.com' <[303642690@qq.com](mailto:303642690@qq.com)>  
**主题:** 回复: 回复: 【外来邮件，注意核实】回复: [案例号: CAS-09325-J7D5T3 ] % |P2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生，肖先生，您好

在和现场工程师进行沟通、排查后，目前进展如下：

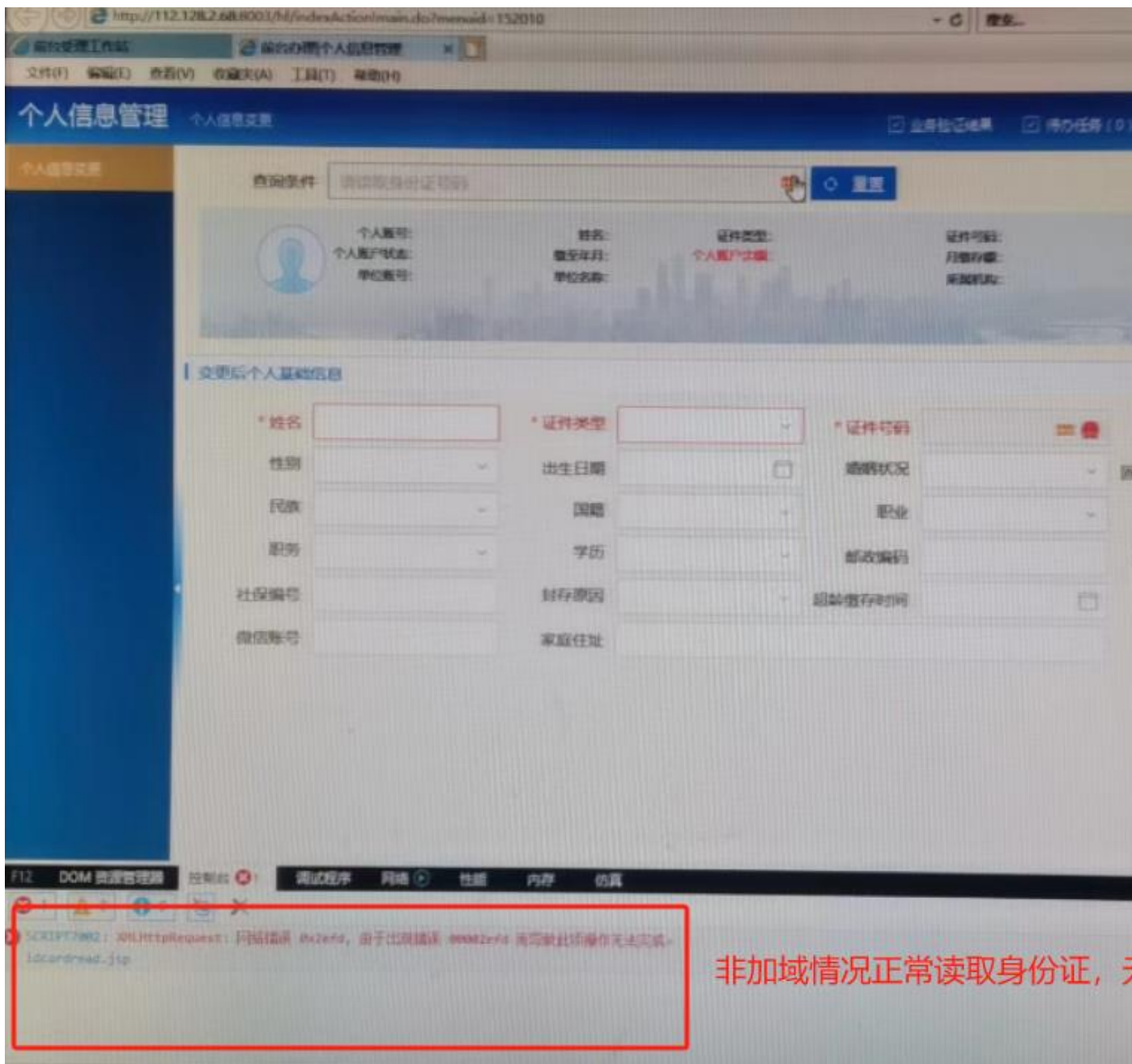
- 目前还未收到 Procmon 和 TSS 日志

- 排查过程中，IE 11 控制台反馈的报错信息中，有 1 条报错在加域复现问题时出现，但未加域正常访问外设的情况下则未出现该报错。
- 由于此 js 文件为厂商研发，涉及设备软硬件内部运行逻辑，建议引入 eloam 厂商排查此报错信息，如果涉及操作系统相关技术咨询，我将持续提供技术支持。
- 报错信息如下：

**SCRIPT5022: SecurityError**

**eloamHidExtend.min.js(268,13)**





贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话: 400-818-0055  
电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

发件人: Jia Wei

发送时间: 2024 年 2 月 21 日 16:37

收件人: ICBC 案例通知 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; 'xiaosong@jx.icbc.com.cn' <[xiaosong@jx.icbc.com.cn](mailto:xiaosong@jx.icbc.com.cn)>

抄送: ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>; '303642690@qq.com' <[303642690@qq.com](mailto:303642690@qq.com)>

主题: 回复: 回复: 【外来邮件, 注意核实】回复: [案例号: CAS-09325-J7D5T3 ] % IP2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生, 肖先生, 您好

为了更快定位问题原因, 除上封邮件的日志, 还需收集如下信息:

1. 打开浏览器调用高拍仪正常过程的视频录像.
2. 出问题情况下, 打开浏览器并尝试调用高拍仪的视频录像.
3. 正常调用高拍仪过程的 Procmon 日志.
4. 出现问题情况下, 打开浏览器调用高拍仪的 procmon 日志.
5. 最后收集正常和问题机器上的 TSS 日志.

### 日志收集:

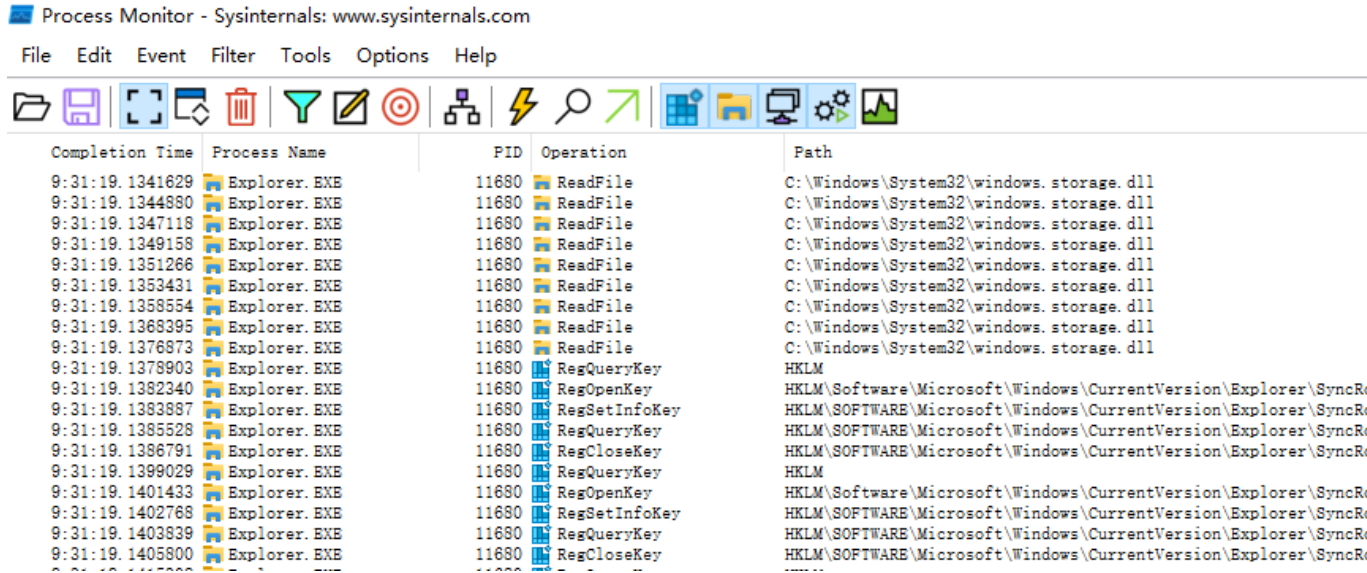
#### 一、Procmon 收集步骤:

=====

- 1) 下载如下链接的 ProcessMonitor 工具

<https://cdue.cmgos.com/download.php?id=655&token=RqIh67w3x7G6pmFjzreeJcoAQ73nHj>  
[fj](#)

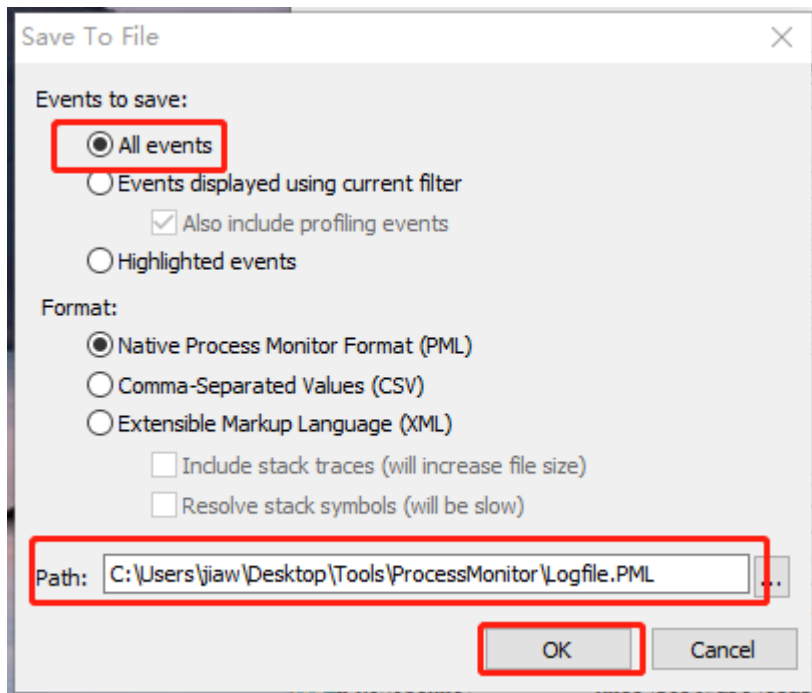
- 2) 在问题计算机和正常机器上, 分别下载解压附件 ProcessMonitor.zip。双击 **Procmon.exe** 运行, 到达此页面, 会有有大量条目出现, 当前已经开始抓取;



- 3) 复现问题（点击系统重装按钮，复现问题）。返回 Process Monitor 窗口，单击 Capture（如下图所示）， 停止抓取



- 4) 点击 File, 点击 Save. 选择 "All events" and "Native Process Monitor Format (PML)" 点击 OK。



压缩并分别将问题日志和正常日志反馈。

## 二、TSS 收集步骤：

=====

1. 从如下网址下载 TSS 工具.

<https://aka.ms/getTSS>


2. 将 **TSS.zip** 解压.
3. 然后以管理员身份打开 PowerShell, 然后执行如下指令收集日志. 如果有 **PowerShell policy** 相关报错, 可以打开以管理员身份运行 **Powershell** 执行 **Set-ExecutionPolicy Bypass** 来允许 PowerShell 脚本执行.

**.\TSS.ps1 -CollectLog DND\_SetupReport**

4. 脚本执行完成后, 日志会生成在 **c:\MS\_DATA** 文件夹下.



This PC ▸ Local Disk (C:) ▸ MS\_DATA

Name	Date modified	Type
 TSS_WIN-A0POQ94ABV2_230816-181027_Log-DND_SetupReport	8/16/2023 6:16 PM	Compressed (zipp...

-----  
-----  
贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话： 400-818-0055  
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

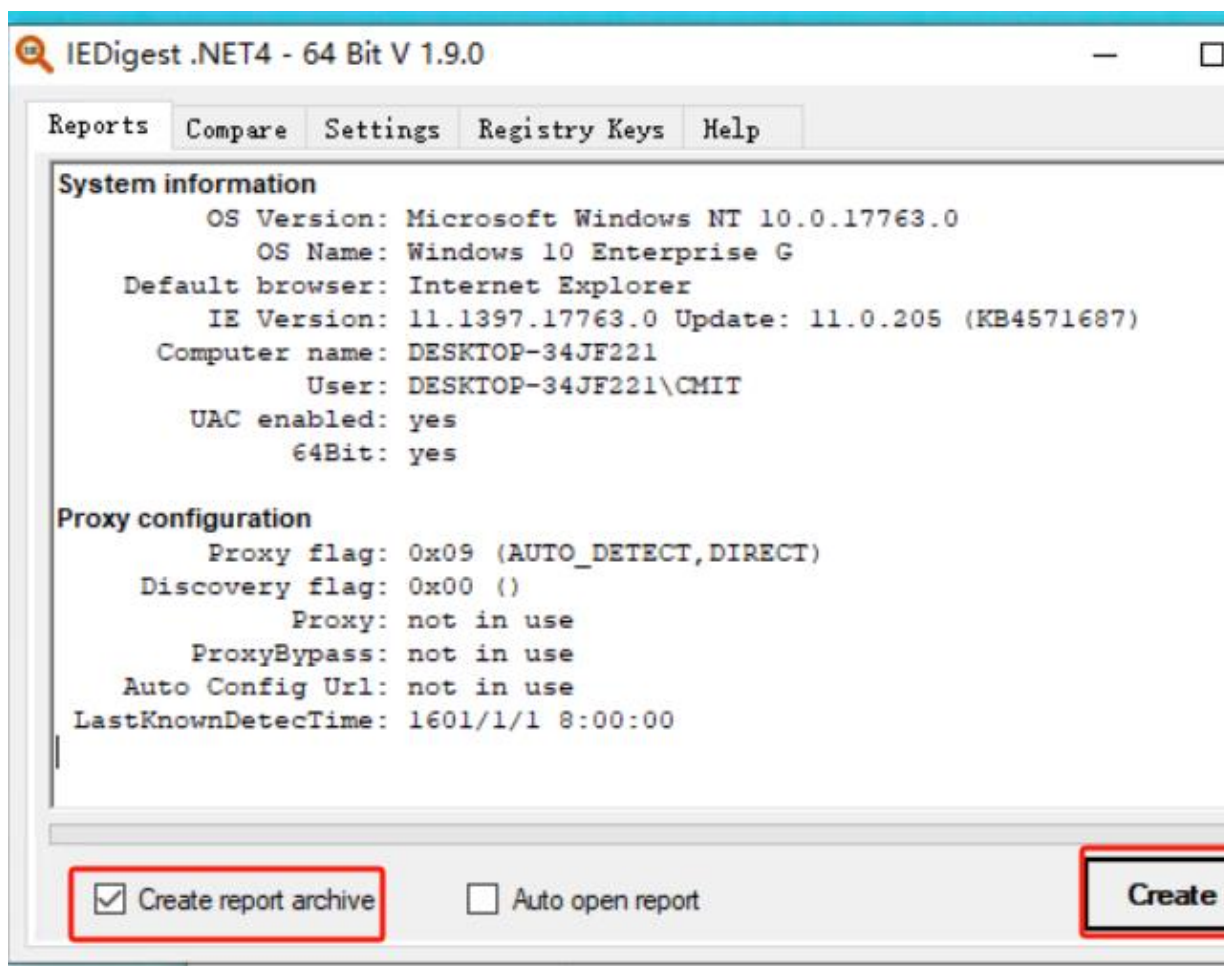
**发件人:** Jia Wei  
**发送时间:** 2024 年 2 月 21 日 11:18  
**收件人:** ICBC 案例通知 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; 'xiaosong@jx.icbc.com.cn' <[xiaosong@jx.icbc.com.cn](mailto:xiaosong@jx.icbc.com.cn)>  
**抄送:** ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>; '303642690@qq.com' <[303642690@qq.com](mailto:303642690@qq.com)>  
**主题:** 回复: 回复: 【外来邮件，注意核实】 回复: [案例号: CAS-09325-J7D5T3 ] %  
|P2||ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生，肖先生，您好

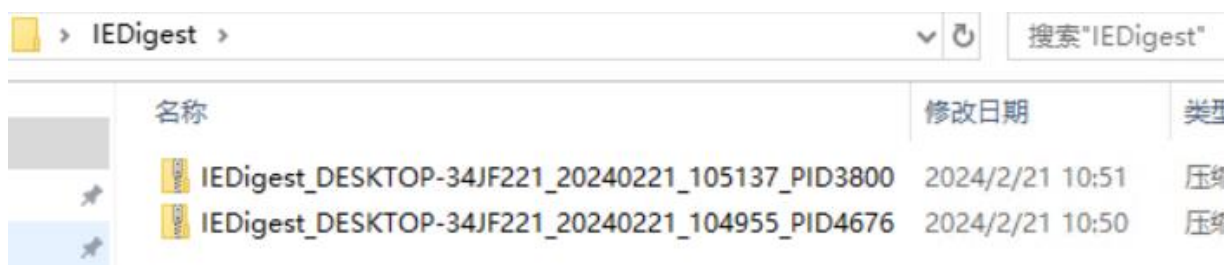
如沟通，请补充收集下面信息：

1. 检查下测试网页是否有识别到高拍仪设备，关于浏览器调用本地设备我们可能无法直接排查，如果厂商那边能提供关于设备识别的相关信息或者本地可以测试设备能否使用也可以给我们
2. IE 11 配置分析。
  - i. 分别在加域前、加域后的 2 台机器上，下载 IE Digest 至桌面，解压后运行 iedigest.exe  
<https://cduecmgos.com/download.php?id=1248&token=HNGnzGIJM85G1sjXUYYRBstAChxmEa2s>
  - ii. 确保“Create report archive”勾选，点击 Create report。

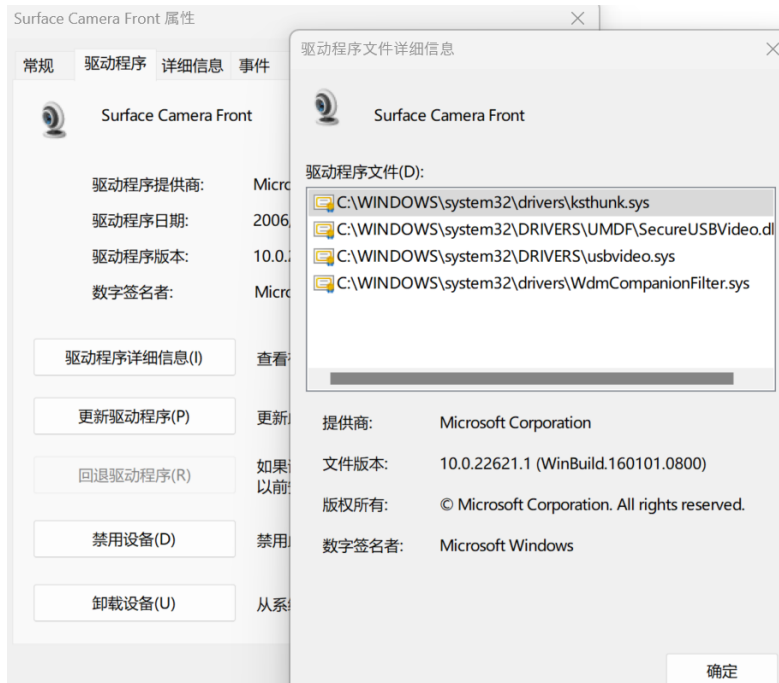




- iii. 之后在桌面找到“IEDigest”文件夹，将其中的 zip 文件反馈（加域前后各一个 zip，共两个）



3. 在设备管理器中将高拍仪设备的驱动程序详细信息和硬件 ID 截图，如果有相应的驱动应用程序名称等相关信息也请提供给我们，谢谢！



贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话： 400-818-0055  
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

发件人: Jia Wei

发送时间: 2023 年 8 月 14 日 17:01

收件人: 'win10 技术支持' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; '303642690@qq.com' <[303642690@qq.com](mailto:303642690@qq.com)>

抄送: '许娇阳' <[xujy2@sdicbc.com.cn](mailto:xujy2@sdicbc.com.cn)>; ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>

主题: 回复: 回复: 【外来邮件, 注意核实】回复: [案例号: CAS-09325-J7D5T3 ] %  
|P2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生, 您好

#### **案例进展及计划:**

得到反馈, 设备厂商暂无法提供进一步支持。只能从操作系统角度尝试排查。收集 Fiddler 日志, 尝试从网页访问角度进行分析。

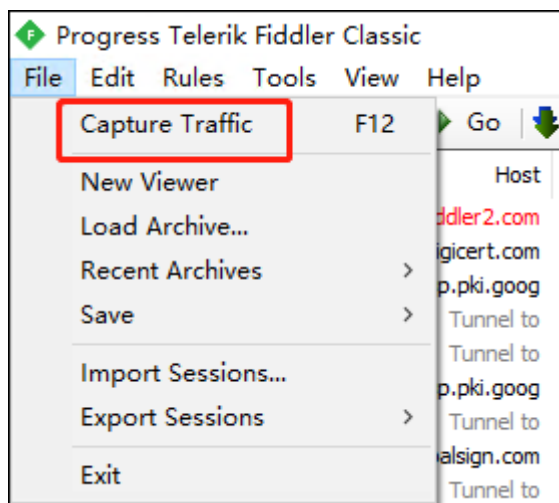
#### **已进行操作:**

- 收集 Procmon 日志, dsp 介入, 卸载后问题依旧。
- 将 IE settings 相关注册表, 回滚至可以正常访问外设的设置。 --- 问题依旧;
- 将 GPO 移除, 导入可以正常访问外设的设置。 ---问题依旧;
- 逐一卸载三方软件。 ---问题依旧;

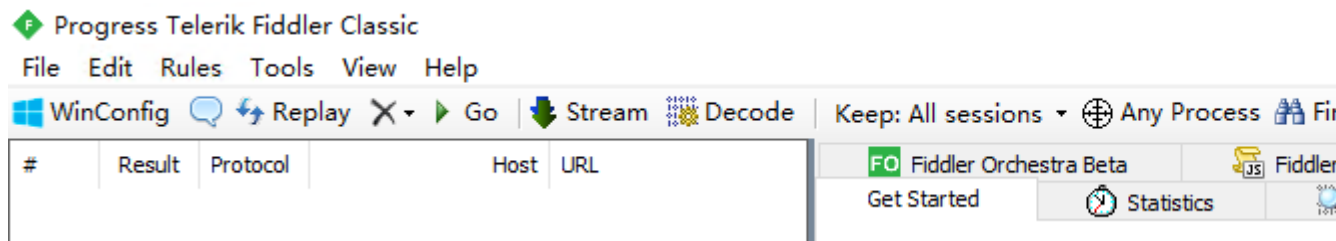
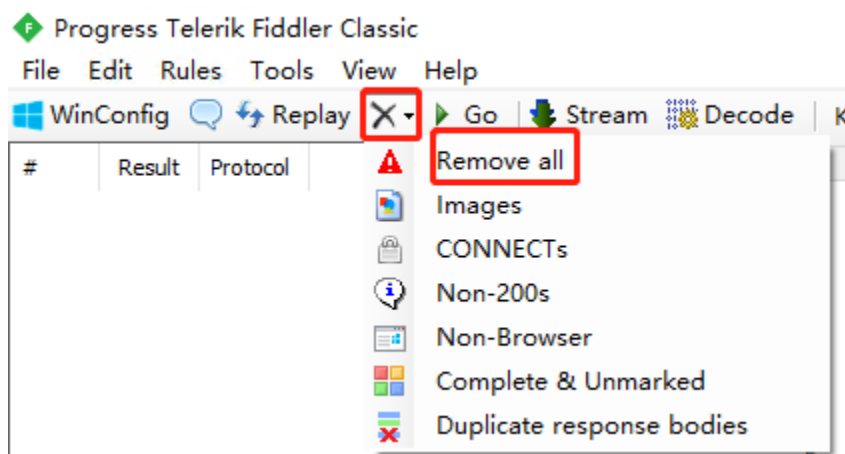
#### **日志收集:**

如下步骤, 需要分别在正常访问外设、访问外设失败过程, 各收集一次。以便对比查看。

- 1) 安装附件 exe 文件后, 打开 **Fiddler classic**
- 2) 进入后有大量条目, **反选 Capture Traffic**, 暂停抓取。

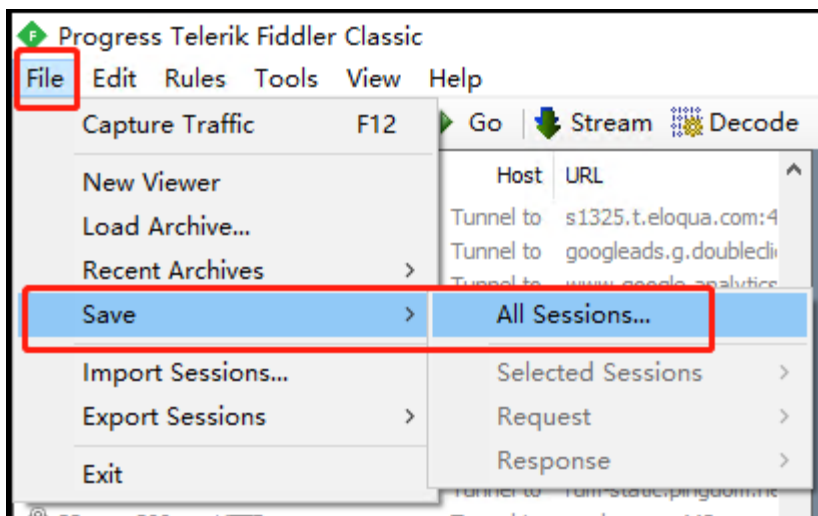


3) 按下图清除所有条目移机 Cache



4) 准备复现场景，回到步骤 2，勾选 Capture Traffic 开始抓取，复现问题。

5) 复现问题完毕，回到 File，先反选 Capture Traffic 停止抓取，再 Save All Sessions 报错日志。



---

贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话： 400-818-0055  
电子邮箱： [jiawei@cmgos.com](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

**发件人:** Jia Wei  
**发送时间:** 2023 年 8 月 1 日 10:47  
**收件人:** 'win10 技术支持' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; '303642690@qq.com' <[303642690@qq.com](mailto:303642690@qq.com)>  
**抄送:** '许娇阳' <[xujy2@sdicbc.com.cn](mailto:xujy2@sdicbc.com.cn)>; ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
**主题:** 回复: 回复: 【外来邮件，注意核实】 回复: [案例号: CAS-09325-J7D5T3 ] % IP2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生，您好

如上封邮件所示，目前的排查思路可以从组策略入手。

可以按照上封邮件内容操作，尝试解决此问题。

---

贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话： 400-818-0055  
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

**发件人:** Jia Wei  
**发送时间:** 2023 年 7 月 21 日 11:23  
**收件人:** 'win10 技术支持' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; '303642690@qq.com' <[303642690@qq.com](mailto:303642690@qq.com)>  
**抄送:** '许娇阳' <[xujy2@sdicbc.com.cn](mailto:xujy2@sdicbc.com.cn)>; ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
**主题:** 回复: 回复: 【外来邮件，注意核实】 回复: [案例号: CAS-09325-J7D5T3 ] % IP2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生，您好

还未收到 IEDigest 日志和 IESettings.vbs 文件，您可以方便时候反馈。

目前的问题现象是：加域前公积金网站可以正常访问高拍仪，加域后无法访问，点击无效。

所以根据加域动作来说，我能想到的大概有 3 方面动作：

- 推送的组策略限制了高拍仪所需组件/功能
- 推送的脚本执行造成了此问题
- 三方软件下发的组策略造成了此问题

此外根据厂商工程师的反馈，如果导入非加域的 IE 设置相关注册表键值都无法解决此问题，我们可以根据上述方面逐一排除

#### 组策略：

思路：非加域正常机器，使用 LGPO 工具备份现有组策略。再加域后移除组策略，导入加域前组策略，测试是否解决此问题。

- 1) 在非加域正常机器，解压 LGPO。并在 C:\根目录创建 gp 文件夹；

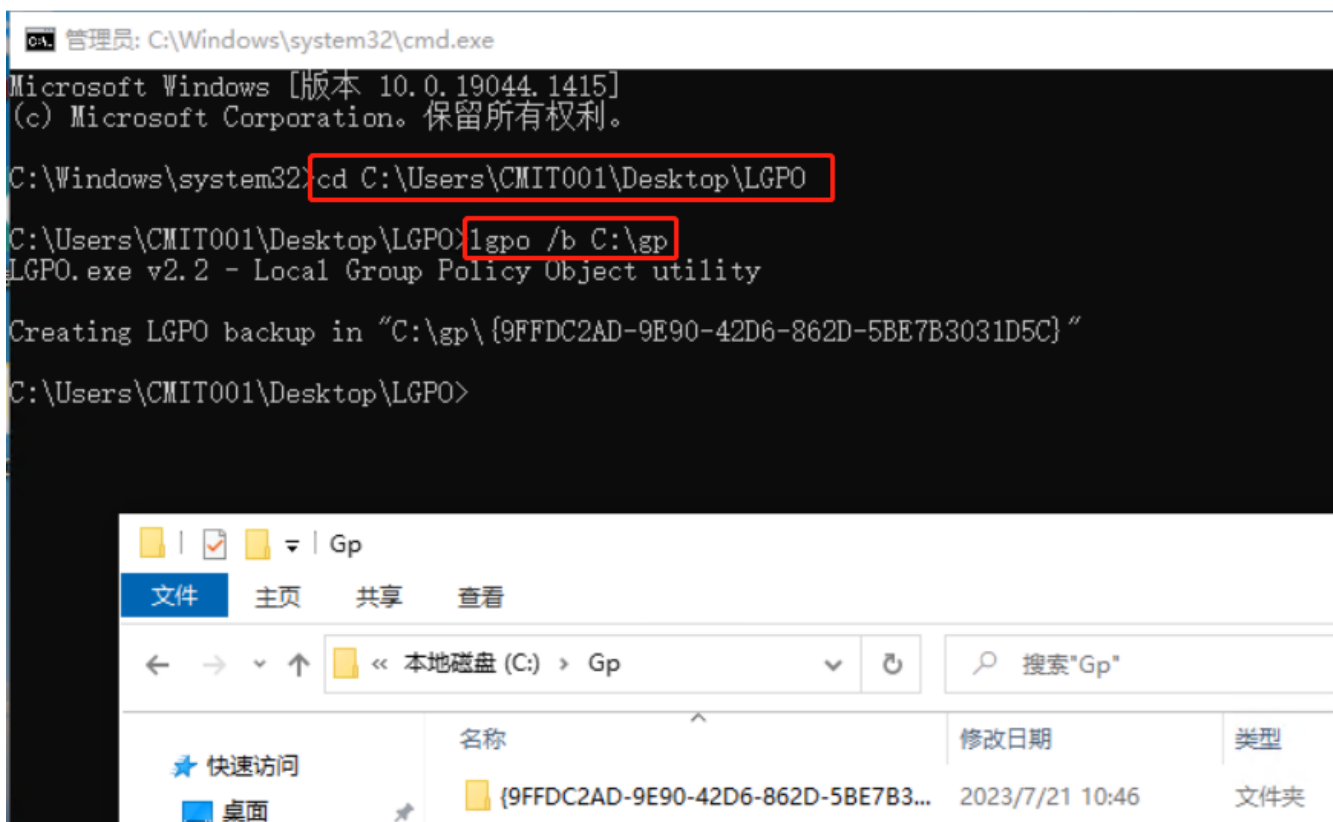
2) 以管理员身份运行命令提示符，依次运行如下命令（黑色斜体部分替换实际 LGPO 路径）

Cd *PATH\LGPO*

Lgpo /b C:\gp

这样就在 C:\gp 文件夹下生成了一个 GUID 为名称的文件，里面就是备份的组策略文件。

备份 gp 文件夹



3) 加域，确认问题复现。以管理员身份运行如下命令（黑色斜体部分替换实际 LGPO 路径）

暂停更新域控策略、移除现有域控策略、恢复加域前组策略。

gpupdate /disable

Cd *PATH\LGPO*

RD /S /Q "%WinDir%\System32\GroupPolicy"

LGPO /g *PATH\gp*



运行完毕后如下图所示，之后快速确认是否可以解决此问题。

```
C:\Users\CMIT001\Desktop\LGPO>RD /S /Q "%WinDir%\System32\GroupPolicy"
C:\Users\CMIT001\Desktop\LGPO>LGPO.exe /g C:\gp
LGPO.exe v2.2 - Local Group Policy Object utility

Created directory for audit policy
Copied C:\gp\{9FFDC2AD-9E90-42D6-862D-5BE7B3031D5C}\DomainSysvol\GPO\Machine\microsoft\
to C:\Windows\system32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv
Clearing existing audit policy
Apply Audit policy from C:\gp\{9FFDC2AD-9E90-42D6-862D-5BE7B3031D5C}\DomainSysvol\GPO\M
\audit.csv
Apply security template: C:\gp\{9FFDC2AD-9E90-42D6-862D-5BE7B3031D5C}\DomainSysvol\GPO\
dit\GptTmpl.inf
Import Machine settings from registry.pol: C:\gp\{9FFDC2AD-9E90-42D6-862D-5BE7B3031D5C}
y.pol
Import User settings from registry.pol: C:\gp\{9FFDC2AD-9E90-42D6-862D-5BE7B3031D5C}\Do
C:\Users\CMIT001\Desktop\LGPO>_
```

-----  
-----  
贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话： 400-818-0055  
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

发件人: Jia Wei  
发送时间: 2023 年 7 月 17 日 15:01  
收件人: 'win10 技术支持' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; '303642690@qq.com' <[303642690@qq.com](mailto:303642690@qq.com)>  
抄送: '许骄阳' <[xujy2@sdicbc.com.cn](mailto:xujy2@sdicbc.com.cn)>; ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
主题: 回复: 回复: 【外来邮件，注意核实】 回复: [案例号: CAS-09325-J7D5T3 ] % IP2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许工，您好

很高兴与您电话沟通，IEDigest 工具下载链接如下：

<https://cdac.cmgos.com/download.php?id=1050&token=5XqNslwpgMHfXgFL2mBC0NjrNdyS>

[AIN](#)

-----  
-----  
贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话: 400-818-0055  
电子邮箱: [jiawei@cmgos.com](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

发件人: Jia Wei  
发送时间: 2023 年 7 月 17 日 11:15  
收件人: 'win10 技术支持' <[win10sup@sdc.icbc.com.cn](mailto:win10sup@sdc.icbc.com.cn)>  
抄送: '许骄阳' <[xujy2@sdc.icbc.com.cn](mailto:xujy2@sdc.icbc.com.cn)>; ICBC\_Notification  
<[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
主题: 回复: 回复: 【外来邮件, 注意核实】 回复: [案例号: CAS-09325-J7D5T3 ] %  
IP2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

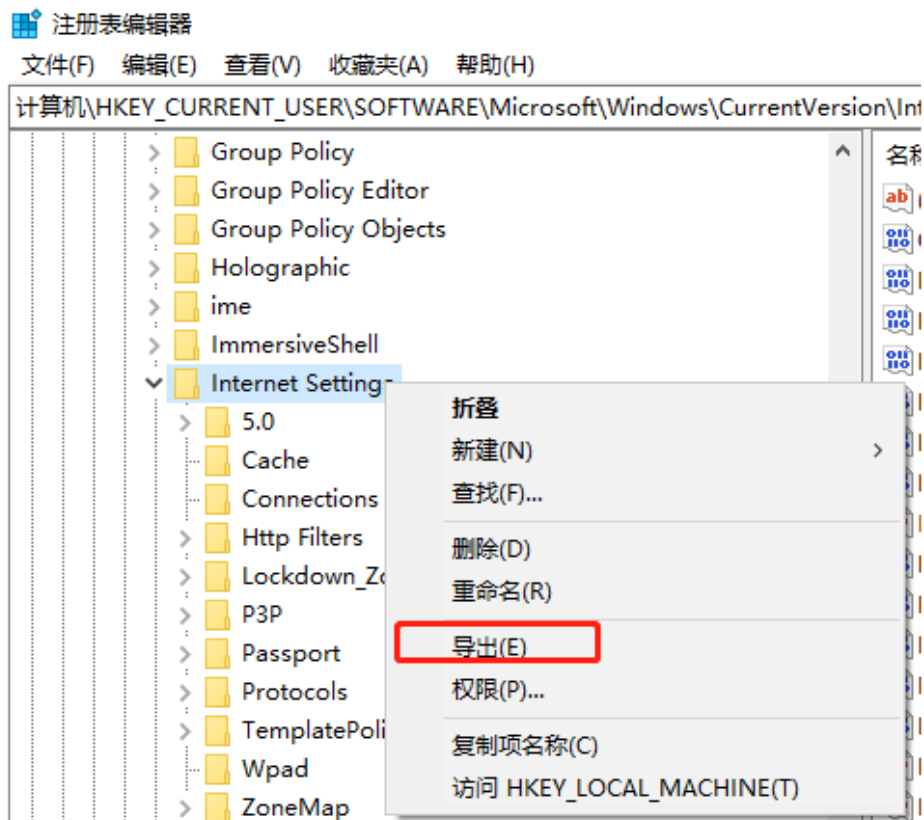
许先生, 您好

目前先对 IE Settings 进行全方面的问题对比测试, 参考如下方式, 进行 IE settings 方面的测试。

**建议操作:**

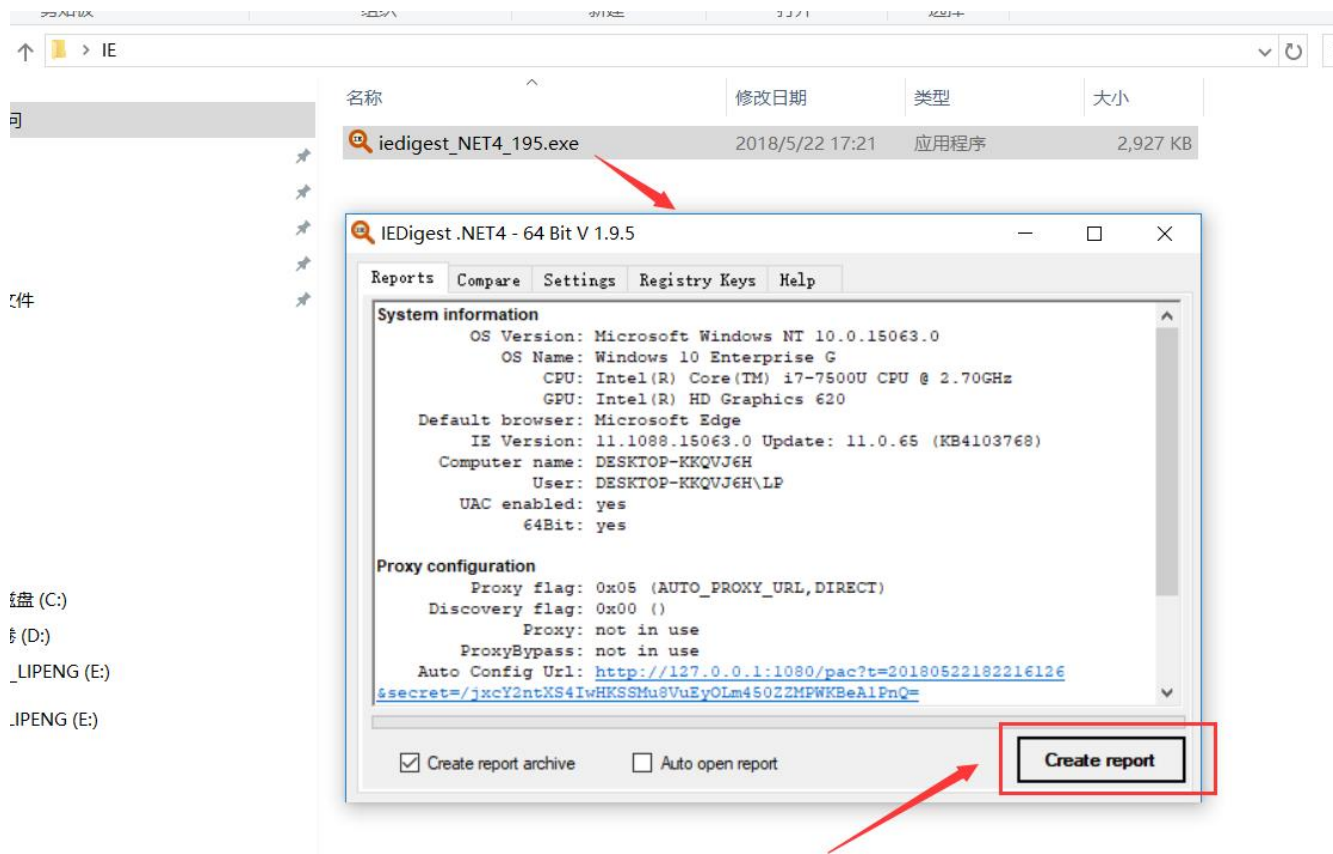
**一、备份注册表信息, 用于覆盖及回滚操作**

- 1) 在非加域可以使用高拍仪的机器上, 同时按下 Windows+R, 运行 regedit, 导航至  
HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
- 2) 右键点击 Internet Settings, 选择导出至本地磁盘其他位置。备份注册表键值, 例如  
123.reg。

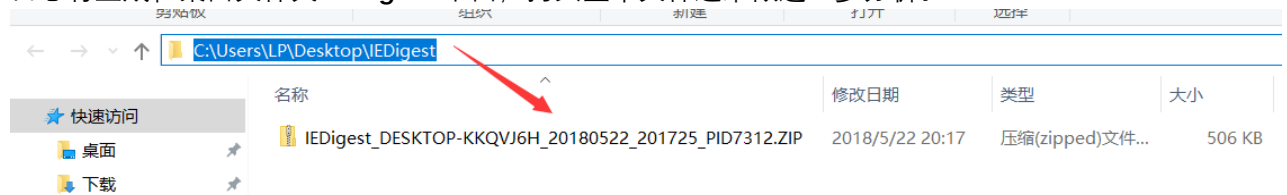


## 二、收集 IEDigest 日志、导入注册表键值对比测试。

- 1) 确认在非加域状态下，公积金网址访问高拍仪正常；
- 2) 使用附件的 IEDigest 工具收集日志；



日志将生成在桌面文件夹“IEDigest”下面，拷贝整个文件过来做进一步分析。



- 3) 加域；确认公积金网址无法访问高拍仪；
- 4) 再使用 IEDigest 工具收集日志。反馈 2) 4) 的日志
- 5) 合并步骤一中备份的 123.reg 文件，确认在当前加域状态下是否可以成功访问。

贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话：400-818-0055  
电子邮箱：jiawei@cmgos.com

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

发件人: Jia Wei

发送时间: 2023 年 7 月 13 日 13:10

收件人: 'win10 技术支持' <[win10sup@sdc.icbc.com.cn](mailto:win10sup@sdc.icbc.com.cn)>

抄送: '许骄阳' <[xujy2@sdc.icbc.com.cn](mailto:xujy2@sdc.icbc.com.cn)>; ICBC\_Notification  
<[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>

主题: 回复: 回复: 【外来邮件, 注意核实】 回复: [案例号: CAS-09325-J7D5T3 ] %  
|P2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生, 您好

### 案例分析:

- 1) 根据提供的《插件和高拍仪的操作手册》-第八步: 浏览器配置, 需要对 Internet Explorer 进行设置; 其中大部分针对 Internet 区域, 而非受信任的站点进行。我整理了需要修改设置和对应的注册表键值。

首先需要启用位于 Internet 区域 (对应路径为

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\)

下:

启用 – 对应注册表 Value 0

2201 ActiveX controls and plug-ins: Automatic prompting for ActiveX controls \*\* ^

1201 ActiveX controls and plug-ins: Initialize and script ActiveX controls not marked  
as safe for scripting

1405 ActiveX controls and plug-ins: Script ActiveX controls marked as safe for  
scripting

2000 ActiveX controls and plug-ins: Binary and script behaviors

1208 ActiveX controls and plug-ins: Allow previously unused ActiveX controls to run without prompt ^

1001 ActiveX controls and plug-ins: Download signed ActiveX controls

1004 ActiveX controls and plug-ins: Download unsigned ActiveX controls

1209 ActiveX controls and plug-ins: Allow Scriptlets

1200 ActiveX controls and plug-ins: Run ActiveX controls and plug-ins

2101 Miscellaneous: Web sites in less privileged web content zone can navigate into this zone \*\*

120B Only allow approved domains to use ActiveX controls without prompt

120A Allow video and animation on a Web page that uses a legacy media player

但根据之前的 Log 来看，部分键值仍为 3，对应禁用

Operation	Path	Detail
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1004	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1201	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\2703	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1201	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\Icon	Type: REG_SZ, 1
RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\MinLevel	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1004	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1201	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\2703	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1201	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\Icon	Type: REG_SZ, 1
RegQueryValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\MinLevel	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1207	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1208	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1208	Type: REG_DWORD
RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\2201	Type: REG_DWORD

其次在受信任站点区域（对应路径为

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\），需要设置如下

禁用 – 对应注册表 Value 3

1409 - Scripting: Enable XSS Filter

此键值应该为 3，但从 Log 来看，此键值 Data = 0 对应已启用。

Completion Time	Process Name	PID	Operation	Path
9:36:00.4218318	IEEXPLORE.EXE	10776	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Intern

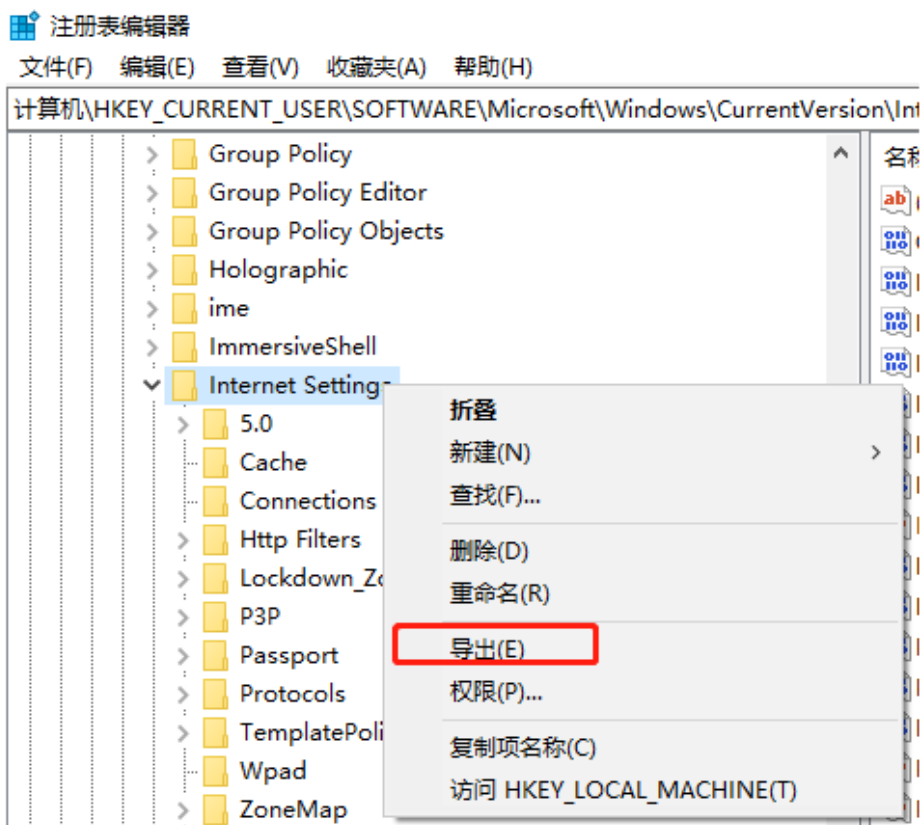
2) 另外，组策略推送了 **IESetting.vbs**，如果方便可以反馈此文件。

**建议操作：**

1) 同时按下 Windows+R，运行 regedit，导航至

HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

2) 右键点击 Internet Settings，选择导出至本地磁盘其他位置。备份注册表键值。



3) 将附件的 Registry 添加后缀.bat，右键以管理员身份运行。

4) 确认问题是否解决。如果未解决，抓取 Procmon 日志。



电子邮箱: [jiawei@cmgos.com](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

**发件人:** Jia Wei

**发送时间:** 2023 年 7 月 12 日 10:42

**收件人:** 'win10 技术支持' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

**抄送:** 许娇阳 <[xujy2@sdicbc.com.cn](mailto:xujy2@sdicbc.com.cn)>; ICBC\_Notification  
<[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>

**主题:** 回复: 回复: 【外来邮件, 注意核实】回复: [案例号: CAS-09325-J7D5T3 ] %  
|P2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生, 您好

根据刚刚电话沟通的结果, 可以将 CMGE 日志收集工具的日志, 以及客户软件安装程序反  
馈。

我将继续跟踪处理此案例。

---

贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话: 400-818-0055  
电子邮箱: [jiawei@cmgos.com](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

**发件人:** win10 技术支持 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

**发送时间:** 2023 年 7 月 11 日 9:48

**收件人:** Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>

**抄送:** 许娇阳 <[xujy2@sdicbc.com.cn](mailto:xujy2@sdicbc.com.cn)>; ICBC\_Notification  
<[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>

**主题:** 回复: 回复: 【外来邮件, 注意核实】回复: [案例号: CAS-09325-J7D5T3 ] %  
|P2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

配置完成后，问题依旧，请协助分析，相关日志已上传。

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心（珠海）

许 翔

系统一部

电话：17606669571

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

---

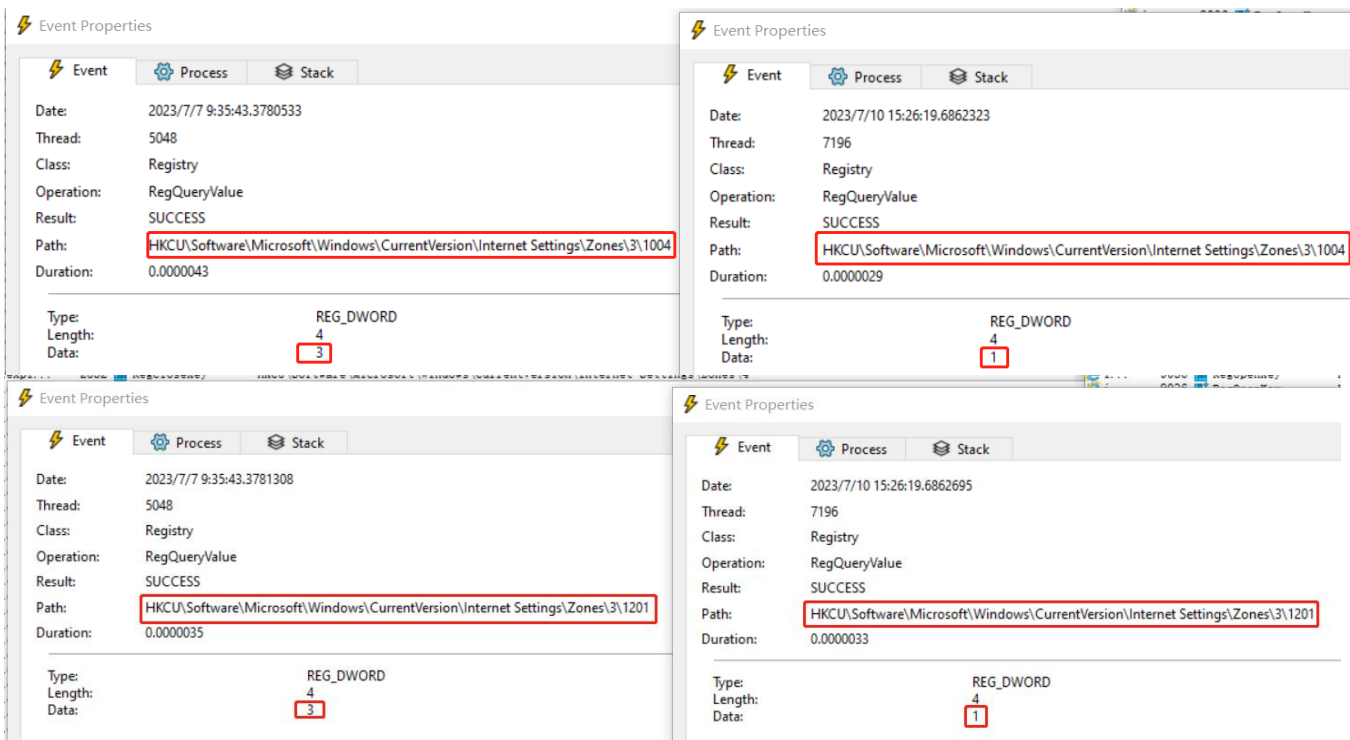
-----原始邮件-----

发件人: "Jia Wei" <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>  
发送时间: 2023-07-10 17:51:38  
收件人: "win10 技术支持" <[win10 技术支持.软件开发中心系统一部@工商银行.icbc](mailto:win10技术支持.软件开发中心系统一部@工商银行.icbc)>  
抄送: "许娇阳" <[许娇阳.软件开发中心系统一部@工商银行.icbc](mailto:许娇阳.软件开发中心系统一部@工商银行.icbc)>, "ICBC\_Notification" <[icbc\\_notification@cmgos.com](mailto:icbc_notification@cmgos.com)>  
主题: 回复: 【外来邮件，注意核实】回复: [案例号: CAS-09325-J7D5T3] % | P2 | ICBC | win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

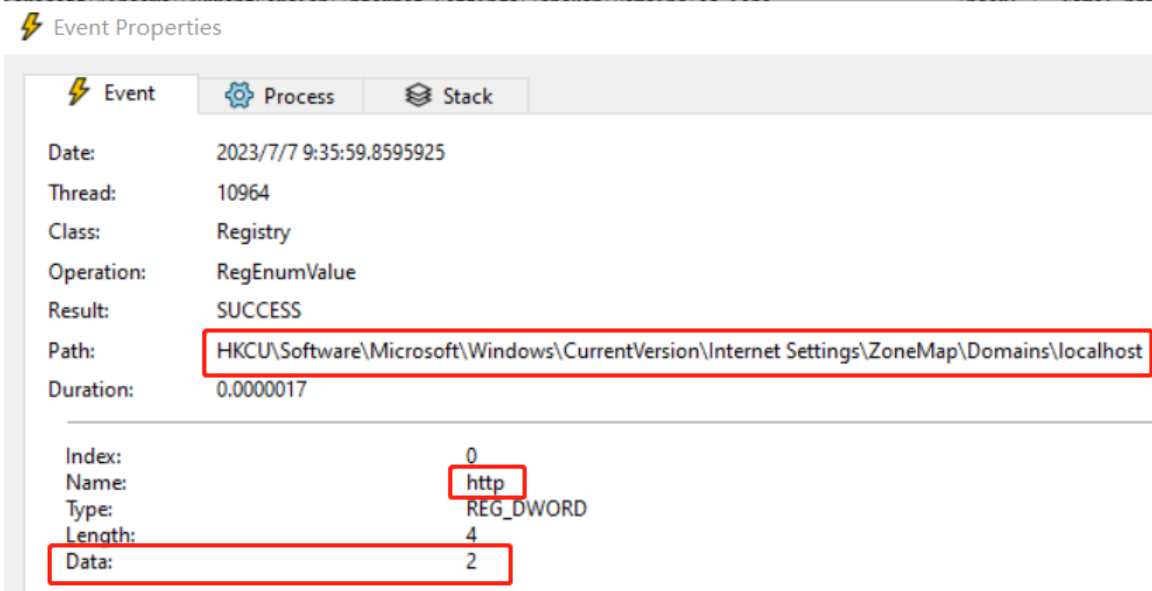
许先生，您好

**案例分析：**

- 由于此问题设计三方厂商的产品，作为操作系统厂商对于三方厂商产品的实际工作原理不甚了解，进一步排查建议引入此设备三方人员一同推进。
- 目前只根据 Procmon 日志来看，eloam-hid.exe 调用了 cmd 执行 cmd /c start <https://localhost:18082/>，最终启动了 IE 浏览器打开网页。
- 所以当前的排查思路可以从 Internet Explorer 的 Internet 选项，安全设置入手。  
从日志来看，加域后确实对于区域的安全设置有所变更，如下是对比的截图。

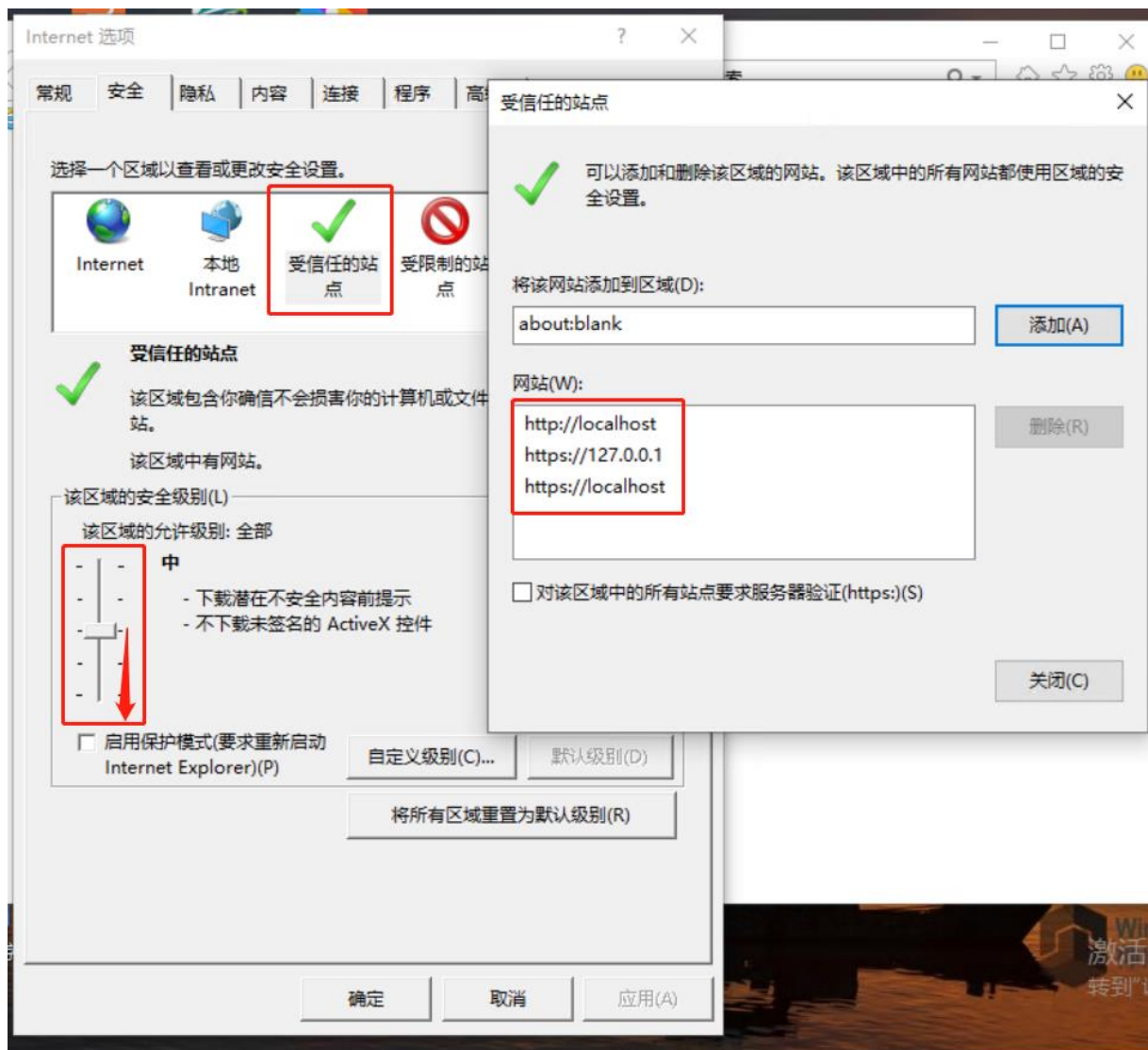


从日志细节看，localhost 的 http 键值为 2，表示已添加 [Http://localhost](http://localhost) 到受信任站点。但没有 https 协议的设置。



### 建议操作：

- 1) 打开 IE 浏览器，在 Internet 设置中，进行如下配置。
- 2) 将 [Https://localhost](https://localhost) 加入受信任站点，同时如允许，将受信任站点的安全级别设置为低。
- 3) 确认是否解决此问题。



贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话： 400-818-0055  
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

发件人: win10 技术支持 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
发送时间: 2023 年 7 月 10 日 15:35  
收件人: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>  
抄送: 许骄阳 <[xujy2@sdicbc.com.cn](mailto:xujy2@sdicbc.com.cn)>; ICBC\_Notification  
<[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
主题: 回复: 【外来邮件, 注意核实】回复: [案例号: CAS-09325-J7D5T3 ] %  
|P2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

已将 dsp 卸载问题依旧, 请协助分析问题原因。

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心(珠海)

许 翔

系统一部

电话: 17606669571

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

---

-----原始邮件-----

发件人: "Jia Wei" <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>  
发送时间: 2023-07-10 09:51:44  
收件人: "win10 技术支持" <[win10 技术支持.软件开发中心系统一部@工商银行.icbc](mailto:win10技术支持.软件开发中心系统一部@工商银行.icbc)>  
抄送: "ICBC\_Notification" <[icbc\\_notification@cmgos.com](mailto:icbc_notification@cmgos.com)>  
主题: 【外来邮件, 注意核实】回复: [案例号: CAS-09325-J7D5T3 ] % |P2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生, 您好

**案例分析:**

从提供的 Procmon 日志来看, 运行"C:\Program Files (x86)\良田-HID\eloam-hid.exe"之后, 启动了 cmd.exe 执行了 cmd /c start <https://localhost:18082/>命令。

从 Process 信息, 目前看有大量的 DSPClient 介入。

根据现有的对比测试情况，请确认加域之后是否有 DSP 策略的下发。如果有建议移除 DSP 或禁用策略，确认问题是否复现。

Event Properties

Event

Process

Stack

Image

Name:

Version:

Path:

Command Line:

PID: 8412

Architecture: 64-bit

Parent PID: 8040

Virtualized: False

Session ID: 1

Integrity:

User:

Auth ID: 00000000:0005aa4e

Started: 2023/7/7 9:35:42

Ended: 2023/7/7 9:35:43

Modules:

Module	Address	Size	Path	Company	Version	Timestamp
vGlog64.dll	0x7fffb62f0000	0x66000	C:\Program Files (x86)\DSPClient\...			2020/11/9 16:3...
vEdsmOfficeExt...	0x7fffb4b80000	0xa3000	C:\Program Files (x86)\DSPClient\...	Beijing VRV Software Co.,Ltd	1.0.0.1	2022/12/23 14:...
EnsecCore64.dll	0x7ffbc1500000	0x79000	C:\Program Files (x86)\DSPClient\...	Beijing VRV Software Co.,Ltd	21, 10, 21, 1	2021/10/21 14:...
MedAdapter64....	0x7ffbc15b0000	0x3b000	C:\Program Files (x86)\DSPClient\...	Beijing VRV Software Co.,Ltd	22, 3, 30, 1	2022/3/31 10:5...
medscreenm64...	0x180000000	0x77000	C:\Program Files (x86)\DSPClient\...	Beijing VRV Software Corporation Limited.	22, 8, 3, 5	2022/8/19 10:4...
MedEoDataCtrl...	0x7fffb5b90000	0xd9000	C:\Program Files (x86)\DSPClient\...	Beijing VRV Software Corporation Limited.	22, 4, 28, 1	2022/4/28 11:5...
cmd.exe	0x7ff740510000	0x65000	C:\Windows\System32\cmd.exe	Microsoft Corporation	10.0.17763.1 (...	2008/5/30 8:32:...
comctl32.dll	0x7ffbcadf0000	0xa9000	C:\Windows\WinSxS\amd64_micr...	Microsoft Corporation	6.10 (WinBuild...	1921/10/6 18:3...
GdiPlus.dll	0x7ffbcdf0000	0x1a4000	C:\Windows\WinSxS\amd64_micr...	Microsoft Corporation	10.0.17763.437...	2037/5/27 8:23:...
winspool.drv	0x7ffbd0e70000	0x8e000	C:\Windows\System32\winspool...	Microsoft Corporation	10.0.17763.197...	1920/5/19 5:51:...

贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话： 400-818-0055  
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

发件人: Jia Wei  
发送时间: 2023 年 7 月 7 日 11:42  
收件人: '许翔' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
抄送: ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>

**主题:** 回复: [案例号: CAS-09325-J7D5T3 ] % |P2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生, 您好

另外请确认此外设设备是否是高拍仪, 如果确认请将如下路径的 log 日志拷贝并反馈。

**C:\Program Files (x86)\良田-HID\gc.log**

-----  
-----  
贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话: 400-818-0055  
电子邮箱: [jiawei@cmgos.com](mailto:jiawei@cmgos.com)

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing  
mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

**发件人:** Jia Wei  
**发送时间:** 2023 年 7 月 7 日 11:36  
**收件人:** 许翔 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>  
**抄送:** ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
**主题:** 回复: [案例号: CAS-09325-J7D5T3 ] % |P2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许先生, 您好

很高兴与您电话沟通, 目前收到了一个问题复现的 Procmon 日志。请按照日志收集部分收集并反馈。

**问题定义:**

win10 政府版在未入域时可正常调用外设, 入域后在未安装 TMS 安全软件的情况下, 无法通过网页正常调用外设, 外设驱动识别正常, 请协助分析问题原因。

**问题范围:**



我们将协助您分析处理上述问题，并对定义的问题给予最大的技术支持。

如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

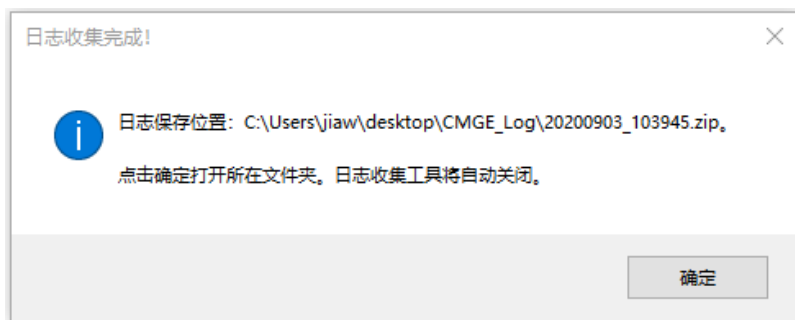
接下来，我们将开始合作解决这个问题。如果您对以上的问题范围界定有任何异议，请尽快告知。如果您有其他任何疑问。也欢迎随时与我联系。

### **日志收集：**

**一、收集正常连接外设过程的 procmon 日志，以便对比分析。**

### **二、工具收集**

1) 在出现问题的计算机上，下载附件zip文件并解压到本地磁盘。双击运行exe文件，同意隐私声明后，按照下图勾选系统日志，组策略信息、网络信息、软件信息，系统进程、更新日志，点击收集。



2) 收集完毕后将在当前用户桌面生产CMGE\_Log。点击确定，将直接打开文件夹并定为压缩文件。

3) 将压缩文件上传。

### 日志上传:

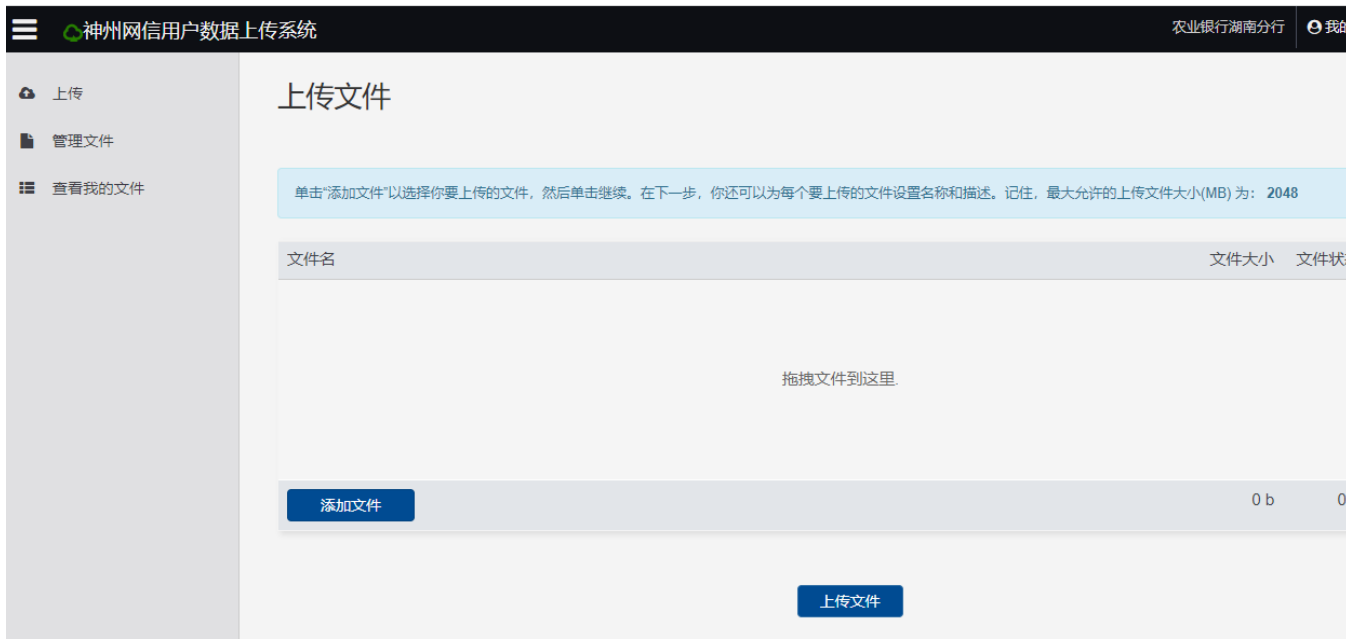
您可以登陆<https://cdac.cmgos.com>，通过数据上传系统上传您所收集的日志信息。

(用户名密码区分大小写)

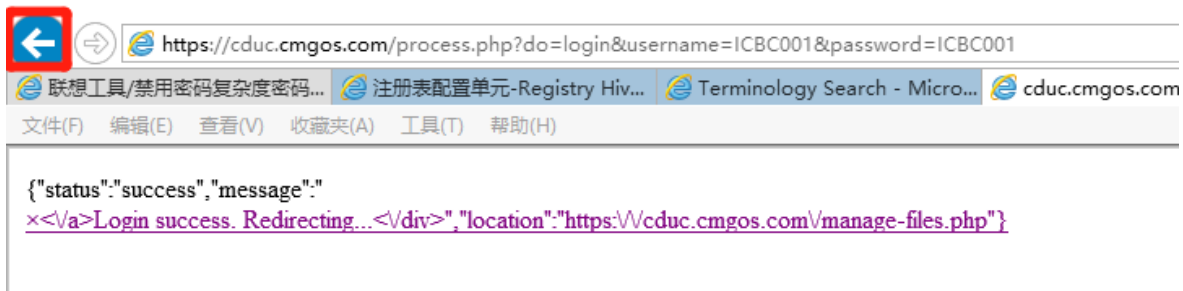
用户名: ICBC001

密码: ICBC001

添加文件后点击上传文件 ,上传完毕后点击保存



注意，如果遇到如下所示页面，点击后退即可看到页面



=====

=====

在向CMIT提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括：

- (1) 神州网信已获得您的明确授权；
- (2) 根据适用法律的要求，神州网信负有披露义务的；
- (3) 司法机关或行政机关基于法定程序要求神州网信提供的；
- (4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。
- (5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

-----  
-----  
贾伟 Jia Wei  
神州网信技术有限公司  
服务支持电话： 400-818-0055  
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.  
11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: [Jiawei@cmgos.com](mailto:Jiawei@cmgos.com) | visit: [www.cmgos.com](http://www.cmgos.com)

---

发件人: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>

发送时间: 2023 年 7 月 7 日 11:17

收件人: 许翔 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

抄送: Jia Wei <[jiawei@cmgos.com](mailto:jiawei@cmgos.com)>

主题: [案例号: CAS-09325-J7D5T3 ] % |P2|ICBC|win10 政府版 1809 入域后无法调用外设问题 % 初次响应 CMIT:0001032

许翔 先生/女士, 您好!

感谢您联系神州网信技术支持中心。我是技术支持工程师 贾伟 。很高兴能有机会协助您解决该问题。您可随时通过邮件回复以及该问题事件号码 CAS-09325-J7D5T3 与我联系。

如果您有任何其他疑问, 请随时与我联系。

此致,

敬礼

---

以上内容是一封有关向神州网信技术有限公司提交技术支持事件的邮件。

如果您希望本次回复能够被自动加入技术支持事件中,您可以选择“全部回复”。

---

—

此邮件信息仅供收件人查阅, 所含任何评论、陈述或数据仅供收件人参考, 若有改动, 恕可能不另行通知。未经中国工商银行书面许可, 请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件, 敬请及时通知发件人, 并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely. The sender and ICBC are not responsible for the loss caused possibly by e-mail.

-----  
-

此邮件信息仅供收件人查阅，所含任何评论、陈述或数据仅供收件人参考，若有改动，恕可能不另行通知。未经中国工商银行书面许可，请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely. The sender and ICBC are not responsible for the loss caused possibly by e-mail.